LAVER'S RESULTS AND LOW-DIMENSIONAL TOPOLOGY

PATRICK DEHORNOY

Dedicated to the memory of Rich Laver

Abstract. In connection with his interest in selfdistributive algebra, Richard Laver established two deep results with potential applications in low-dimensional topology, namely the existence of what is now known as the Laver tables and the well-foundedness of the standard ordering of positive braids. Here we present these results and discuss the way they could be used in topological applications.

Richard Laver established two remarkable results that might lead to significant applications in low-dimensional topology, namely the existence of a series of finite structures satisfying the left-selfdistributive law, now known as the *Laver tables*, and the well-foundedness of the standard ordering of Artin's positive braids. In this text, we shall explain the precise meaning of these results and discuss their (past or future) applications in topology. In one word, the current situation is that, although the depth of Laver's results is not questionable, few topological applications have been found. However, the example of braid groups orderability shows that, once initial obstructions are solved, topological applications of algebraic results involving selfdistributivity can be found; the situation with Laver tables is presumably similar, and the only reason explaining why so few applications are known is that no serious attempt has been made so far, mainly because the results themselves remain widely unknown in the topology community.

Therefore this text is more a program than a report on existing results. Our aim is to provide a self-contained and accessible introduction to the subject, hopefully helping the algebraic and topological communities to better communicate. Most of the results mentioned below have already appeared in literature, a number of them even belonging to the folklore of their domain (whereas ignored outside of it). However, at least the observations about cocycles for Laver tables mentioned in Subsection 1.3 (and established in another paper) are new.

Very naturally, the text comprises two sections, one devoted to Laver tables, and one devoted to the well-foundedness of the braid ordering. It should be noted that the above two topics (Laver tables, well-foundedness of the braid ordering) do not exhaust Laver's contributions to selfdistributive algebra and, from there, to potential topological applications: in particular, Laver constructed powerful tools for investigating free LD-structures, leading to applications of their own [68, 69, 70]. However, connections with topology are less obvious in these cases and we shall not develop them here (see the other articles in this volume).

1991 *Mathematics Subject Classification.* 57M25, 03E55, 03F30, 06F15, 20F10, 20F36.

Key words and phrases. Laver table, selfdistributivity, large cardinal, rack, quandle, link invariant, rack cohomology, R-matrix, set-theoretic Yang–Baxter equation, birack, braid ordering, well-order, unprovability statements, conjugacy problem.

Acknowledgments

The author wishes to thank the specialists of knot theory and quantum groups who open-mindedly welcomed his questions and made a number of suggestions, in particular Nicolás Andruskiewitsch, Scott Carter, Mohamed Elhamdadi, Christian Kassel, Victoria Lebed, Józef Przytycki, Marc Rosso.

1. Laver tables

The left-selfdistributivity law is the algebraic law (LD) $x(yz) = (xy)(xz)$, which is obeyed among others by the conjugacy operation of any group. Its connection with low-dimensional topology as an algebraic distillation of Reidemeister move of type III has been recognized more than thirty years ago [59, 77], and its investigation led in particular to the discovery of the orderability of Artin's braid groups [22, 23]. Every new example of a structure obeying the LD-law is potentially promising for topological applications. First described in 1995, the Laver tables are a family of such finite structures. Easily accessible to computer experiments but quite different from the standard examples, they are fundamental in several respects and using them in topology is one of the most exciting programs one could reasonably propose.

The section comprises four subsections: after introducing the Laver tables in Subsection 1.1, we successively discuss four approaches known to provide applications of selfidistributivity, namely diagram colourings (Subsection 1.2), homology and cohomology (Subsection 1.3) and, finally, R-matrices and the Yang–Baxter equation (Subsection 1.4); in each case, we first introduce the general context and then discuss the specific case of Laver tables. To save some space, we deliberately omitted virtual knots [63] here, although the latter provide a natural framework for extending many existing results and might therefore appear as natural candidates for using Laver tables.

1.1. **Laver's result.**

In the rest of this text, an algebraic structure $(S, *)$ made of a set equipped with a binary operation that obeys the LD-law will be called an *LD-system*, a neutral and easily understandable term inspired by Bruck's classical textbook [9]. The names "LD-groupoid" and "LD-algebra" have also been used in the algebra community (conflicting with other standard meanings for "groupoid" and "algebra"), whereas "shelf" was sporadically used in the topology community for the right-counterpart of an LD-system, that is, a binary system that obeys the right-selfdistributivity law (RD) $(xy)z = (xz)(yz)$.

Most of the classically known LD-systems are connected with conjugacy in a group. In particular, not much was known before the 1990's about finite monogenerated LD-systems, that is, those that are generated by a single element. Richard Laver changed this situation radically in 1995—thus answering by anticipation the question candidly raised twenty years after in [84, Problem 9].

Theorem 1.1 (Laver [70]). (i) *For every $N \geqslant 1$, there exists a unique binary operation $*$ on $\{1, ..., N\}$ that, for all p, q, satisfies*

$$p * 1 = p + 1 \bmod N, \tag{1.1}$$

$$p * (q * 1) = (p * q) * (p * 1). \tag{1.2}$$

Then $(\{1, ..., N\}, *)$ is an LD-system if and only if N is a power of 2.

(ii) *Let A_n be the LD-system of size 2^n so obtained. Then, for all n and $p \leqslant 2^n$, there exists a (unique) integer 2^r satisfying*

$$p * 1 < p * 2 < \cdots < p * 2^r = 2^n,$$

and the subsequent values $p * q$ then repeat periodically. The number 2^r is called the period *of p, written $\pi_n(p)$; one has $\pi_n(2^n - 1) = 1$ and $\pi_n(2^n) = 2^n$.*

(iii) *The LD-system A_n admits the presentation $\langle 1 \mid 1_{[2^n]} = 1 \rangle$, where $x_{[k]}$ stands for $(...((x*x)*x)...)*x$ with x repeated k times.*

(iv) *For $n \geqslant 1$, the map $\mathrm{pr}_n : x \mapsto x \bmod 2^{n-1}$ defines a surjective homomorphism from A_n to A_{n-1} and, for every $p \leqslant 2^n$, one has either $\pi_n(p) = \pi_{n-1}(\mathrm{pr}_n(p))$ or $\pi_n(p) = 2\pi_{n-1}(\mathrm{pr}_n(p))$.*

(v) *If Axiom* I3*—see below—is true, the period $\pi_n(1)$ tends to ∞ with n, the relation $\pi_n(1) \geqslant \pi_n(2)$ holds for every n, and, letting A_∞ be the limit of the inverse system $(A_n, \mathrm{pr}_n)_n$, the sub-LD-system of A_∞ generated by $(1, 1, ...)$ is free.*

The LD-system A_n is now known as the *nth Laver table.* Due to their explicit definition, it is easy to effectively compute the first Laver tables, see Table 1.

The way Richard Laver discovered the tables is remarkable, and, together with the orderability of braid groups, it is arguably one of the most interesting applications of large cardinals ideas in algebra [24].

In recent Set Theory, large cardinal axioms play an important rôle as natural axioms that can be added to the basic Zermelo-Fraenkel system to enhance its logical power. A number of such axioms state the existence of certain elementary embeddings, that is, of injective maps that preserve every notion that is first-order definable from the membership relation. One of the most simple such statements, Axiom I3, asserts the existence of a (nontrivial, that is, non-bijective) elementary embedding from a limit rank V_λ to itself [89, 60]. The point here is that, if such an object exists, then the family $\mathcal{E}_\lambda$ of all such elementary embeddings of V_λ to itself equipped with the binary operation $j[k] := \bigcup_{\alpha<\lambda} j(k{\restriction}V_\alpha)$ is an LD-system, that is, the relation $i[j[k]] = i[j][i[k]]$ holds. It has been known since the 1980's that the algebraic structures $(\mathcal{E}_\lambda, [\,])$ have nontrivial properties [20]. Investigating them since the time of [67], Laver was naturally led to introducing their quotients obtained by cutting the graphs of the elementary embeddings at some level. Laver proved that, for every n, cutting at the level of what is called the 2^nth critical ordinal yields a finite quotient with 2^n elements and that the latter enjoys the properties listed in Theorem 1.1. What is remarkable here is that, once the definition of Theorem 1.1(i) has been isolated, the existence of the tables and the basic properties listed in (i)–(iv) can be established directly, without appealing to elementary embeddings and, therefore, they do not require any large cardinal assumption. By contrast, for the properties listed in (v), no direct combinatorial proof has been found so far and, therefore, one cannot assert them without assuming the (unprovable) existence of an elementary embedding of the needed type, which is precisely the (strong) large cardinal axiom I3. We refer to Chapters X, XII, and XIII of [26] for details.

The algebraic investigation of Laver tables was pursued in two directions. The first one is the study of general (finite) LD-systems, which proved to be an intricate question. As shown by A. Drápal in [35, 36, 37], the global result is that Laver tables are the fundamental objects when one considers finite LD-systems with one generator: every such LD-system can be obtained from Laver tables by means of various transformations, see [26, Section X.2] for precise statements, and also the

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

A_4	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	12	14	16	2	12	14	16	2	12	14	16	2	12	14	16
2	3	12	15	16	3	12	15	16	3	12	15	16	3	12	15	16
3	4	8	12	16	4	8	12	16	4	8	12	16	4	8	12	16
4	5	6	7	8	13	14	15	16	5	6	7	8	13	14	15	16
5	6	8	14	16	6	8	14	16	6	8	14	16	6	8	14	16
6	7	8	15	16	7	8	15	16	7	8	15	16	7	8	15	16
7	8	16	8	16	8	16	8	16	8	16	8	16	8	16	8	16
8	9	10	11	12	13	14	15	16	9	10	11	12	13	14	15	16
9	10	12	14	16	10	12	14	16	10	12	14	16	10	12	14	16
10	11	12	15	16	11	12	15	16	11	12	15	16	11	12	15	16
11	12	16	12	16	12	16	12	16	12	16	12	16	12	16	12	16
12	13	14	15	16	13	14	15	16	13	14	15	16	13	14	15	16
13	14	16	14	16	14	16	14	16	14	16	14	16	14	16	14	16
14	15	16	15	16	15	16	15	16	15	16	15	16	15	16	15	16
15	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
16	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Table 1. The first five Laver tables; we read for instance the values $\pi_0(1) = 1$, $\pi_1(1) = \pi_2(1) = 2$; $\pi_3(1) = \pi_4(1) = 4$: the periods of the first rows make a non-decreasing sequence; the tables make an inverse system under projection mod 2^n: for instance, taking mod 8 the four values that occur in the first row of A_4, namely $2, 12, 14, 16$, yields $2, 4, 6, 8$, which are the 4 values that occur in the first row of A_3; taking the latter mod 4 then gives $2, 4$ repeated twice, hence the two values that occur in the first row of A_2, *etc.*

recent preprint [88], which offers a simplified description in a restricted situation. Summarizing, we can say that the Laver tables play, in the world of selfdistributivity, the same rôle as the one played by the cyclic groups $\mathbb{Z}/p\mathbb{Z}$ in the world of associativity.

The second direction of research was to try to discard the large cardinal assumption in Theorem 1.1(v)—or, contrariwise, to prove that it is necessary. So far, only partial results have been obtained. In the direction of eliminating the axiom, A. Drápal established in [38, 39, 40] the first three steps of a program which, if completed, would show that $\pi_n(1)$ tends to infinity with n. The combinatorial complexity increases so fast that the problem was then abandoned. In the other direction, it was proved by R. Dougherty and T. Jech [34] that $\pi_n(1)$ tends to infinity (if it does) at least as slow as the functional inverse of the Ackermann function, implying that its divergence cannot be proved in Primitive Recursive Arithmetic. This however says nothing for Peano Arithmetic nor, *a fortiori* for the Zermelo–Fraenkel system. Note that, in contradistinction with the properties of free LD-systems, in particular the irreflexivity property of [68] and [21], that were first proved using Axiom I3 and subsequently without it, the properties of the LD-systems $\mathcal{E}_\lambda$ used to establish that $\pi_n(1)$ tends to infinity are not trivial from a set-theoretical point of view, relying on a deep result by J. Steel about extenders. This might explain why discarding the large cardinal axiom is more difficult here, see [30] for details.

1.2. **The diagram colouring approach.** We now turn to possible applications of the Laver tables in low-dimensional topology, starting here with the principle of using selfdistributive structures to colour the strands of link or braid diagrams and its known implementations: in this subsections as in the next ones, we first recall the general principle (thus mentioning elements that are mostly standard in the topology community) and then consider the specific case of Laver tables.

As a general preliminary remark, we would like to insist on the fact that, according to Theorem 1.1, Laver tables are closely connected with free LD-systems, so, in some sense, with the most general LD-systems. By contrast, all racks and quandles that have been used so far in topology (see Definition 1.4 below) are, by very definition, quite far from being free LD-systems: for instance, every rack (here in its left-selfdistributive version) satisfies the law $(x{*}x){*}y = x{*}y$ and its operation is closely connected with the conjugacy operation of a group. This is not at all the case with general LD-systems, and with Laver tables in particular: in a sense, this is bad news as it may suggest that none of the existing tools will extend, but, in another sense, this is good news as this suggests that any possible application of the Laver tables has good chances to be really new—as was the application of free LD-systems to braid orderability twenty years ago.

The general principle. In order to investigate embedded 1-dimensional objects like knots, links, braids, one usually starts with diagrams similar to those of Figure 1, which are seen as plane projections of curves embedded in $\mathbb{R}^3$, and the generic question is to recognize whether two diagrams represent ambient isotopic curves, that is, whether there exists a continuous deformation of the ambient space that takes the curves projecting to the first diagram to the curve projecting to the second diagram.

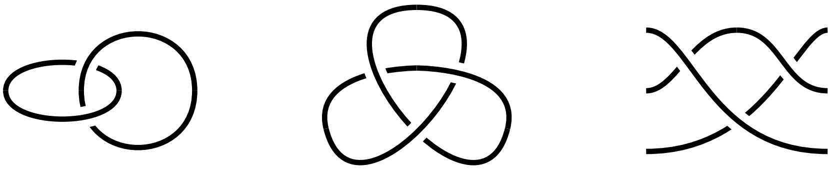


FIGURE 1. Three diagrams, respectively representing the Hopf link (two circles embedded in $\mathbb{R}^3$), the trefoil knot (one embedded circle), and Garside's fundamental braid Δ_3.

A classical result—see for instance [5], [12], or [62]—asserts that two diagrams represent ambient isotopic links if and only if they can be transformed into one another by means of the three types of Reidemeister moves displayed in Figure 2.

The idea of strand colouring is then natural: assuming that an auxiliary set S (the "colours") has been fixed, we attach to each arc in the considered diagram a

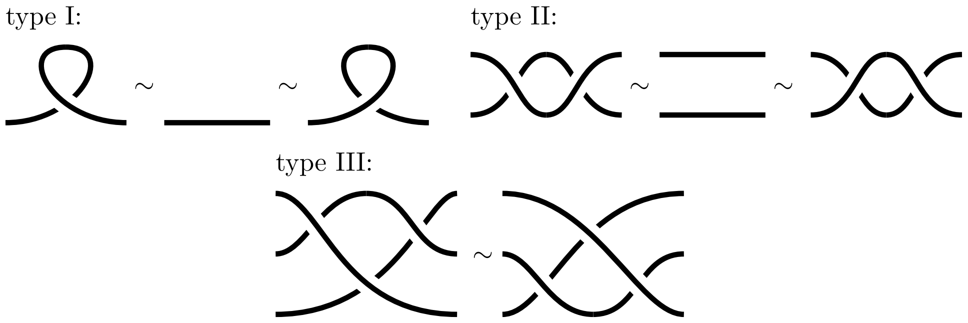
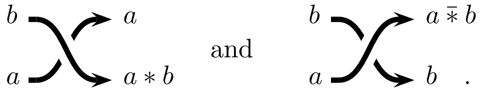


FIGURE 2. Reidemeister moves: two diagrams represent ambient isotopic figures if and only if they can be transformed into one another using a finite sequence of such moves.

label from S, with the aim of extracting information about the isotopy class of the considered diagram. If the colours do not change when two strands cross, the only piece of information that can be extracted is the number of connected components in the case of a (closed) link diagram, or the permutation associated with the braid in the case of an (open) braid diagram. Things become more interesting when colours are allowed to change at crossings. The simplest case is when the strands are oriented and, when two strands cross, only the colour of the top arc may change and its new colour only depends on the colours of the two arcs involved in the crossing and of the orientation of the latter. This amounts to assuming that the set of colours S is equipped with two binary operations $*, \bar{*}$ and the colours obey the rules

(1.3)



Now, in order to possibly extract information about the isotopy class of a diagram, we have to request that the colours do not change when an isotopy is performed or, more exactly, that an admissible colouring is mapped to (another) admissible colouring with the same output. Both in the case of closed diagrams (knots and links) and in the case of open diagrams (braids), this amounts to requiring that, when a Reidemeister move is performed and some input colours are applied to the (oriented) strands, then the output colours are not changed. This immediately translates into algebraic constraints for the operations $*$ and $\bar{*}$.

Lemma 1.2 (Joyce [59]). *Assume that $*$ and $\bar{*}$ are binary operations on S. Then $(S, *, \bar{*})$-colourings are invariant under Reidemeister moves if and only if $(S, *, \bar{*})$ obeys the following laws:*

(1.4) *type I:* $x * x = x \,\bar{*}\, x = x;$

(1.5) *type II:* $x * (x \,\bar{*}\, y) = x \,\bar{*}\, (x * y) = y;$

(1.6) *type III:* $x *' (y *'' z) = (x *' y) *'' (x *' z)$ *for* $*', *''$ *ranging in* $\{*, \bar{*}\}$.

The proof is given in Figure 3.

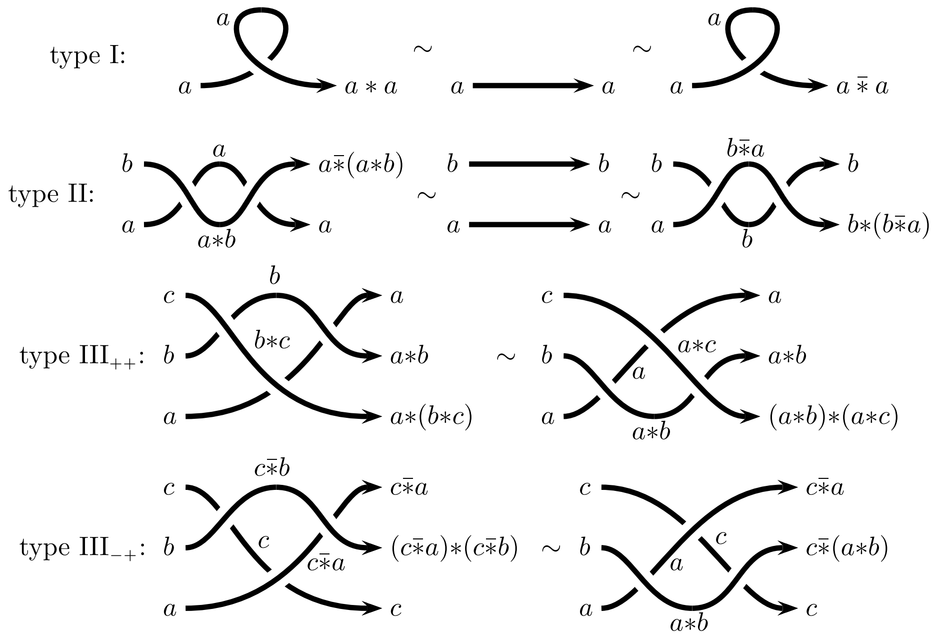


FIGURE 3. Translation of invariance under Reidemeister moves into algebraic laws for the colourings: in the case of Reidemeister III, four orientations are possible, of which only two are displayed; the other two are similar and correspond to the last two combinations of $*$ and $\bar{*}$.

One is thus led to considering the structures involving two binary operations obeying the laws listed in (1.4)–(1.6). An easy observation is that, in such structures, each operation determines the other and that the four laws of (1.6) reduce to a single law.

Lemma 1.3. *A structure* $(S, *, \bar{*})$ *obeys* (1.5) *if and only if the left-translations of* $(S, *)$ *are bijective and, for all* a, b *in* S*, one has*

(1.7) $$a \mathbin{\bar{*}} b = \textit{the unique element } c \textit{ of } S \textit{ satisfying } a * c = b.$$

In this case, the laws of (1.4) *(resp.* (1.6)*) are satisfied if and only if* $(S, *)$ *obeys*

(1.8) $$x * x = x$$

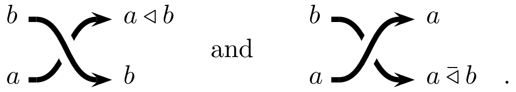
(1.9) $$(\textit{resp. } x * (y * z) = (x * y) * (x * z)).$$

We skip the (easy) verification, which can be found for instance in [31]. It is then natural to introduce a terminology for those LD-systems that satisfy the additional laws of Lemma 1.2.

Definition 1.4. [44, 59] An LD-system $(S, *)$ in which all left-translations are bijective—or, equivalently, a structure $(S, *, \bar{*})$ where (1.5) and (1.6) are obeyed—is called a *rack*. An idempotent rack, that is, a rack satisfying (1.8), is called a *quandle*.

Remark 1.5. Various names appear for the above structures in literature. For instance, racks are called *automorphic sets* in the early source [8], whereas the terms *LD-quasigroup* and *LDI-quasigroups* would be coherent with the standards the algebra community for rack and quandle respectively. More importantly, the most common convention in the topology community is to appeal to the opposite operations, namely to define colourings by the rules

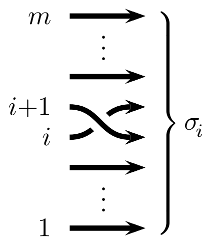
(1.10)



The effect of these conventions is to replace left-selfdistributivity with its right counterpart (RD) $(x \triangleleft y) \triangleleft z = (x \triangleleft z) \triangleleft (y \triangleleft z)$ everywhere and, of course, to consider right-translations in the definition of a rack. Because of our specific interest in the Laver tables here, we shall stick to (1.3) and the law (LD) here. To avoid ambiguity, we use $*$ and $\bar{*}$ as a generic notation for LD-operations, thus keeping $\triangleleft$ and $\bar{\triangleleft}$ for RD-operations. Of course, the transpose $\widetilde{A}_n$ of the Laver table A_n is an RD-system with 2^n elements.

Using colourings: case of braids. Using diagram colourings takes different forms according to whether the considered diagram is open (braid diagram) or closed (link diagram). We begin with the case of braids.

An *m-strand geometric braid* is a family of m open curves embedded in $\mathbb{R}^2 \times [0,1]$ such that the family of initial points is $\{(0,i,0) \mid i = 1,...,m\}$, the family of final points is $\{(0,i,1) \mid i = 1,...,m\}$, and, for every t, the intersection with the plane $z = t$ consists of m points exactly. A *braid* is an isotopy class of geometric braids, referring here to isotopies of $\mathbb{R}^2 \times [0,1]$ that leave the planes $\mathbb{R}^2 \times \{0\}$ and $\mathbb{R}^2 \times \{1\}$ fixed. Projecting a geometric braid on the plane $x = 0$ gives a diagram like the one on the right of Figure 1: the specificity is that there exists a fixed orientation so that the diagrams consists of m arcs going from the line $x = 0$ to the line $x = 1$ in such a way that the x coordinate keeps increasing (no U-turn).



Concatenating m strand geometric braids induces (after rescaling) a well-defined product on m strand braids, which turns to provide a group structure as, by Reidemeister moves of type II, the concatenation of a geometric braid and its image in a vertical mirror is isotopic to the trivial braid, a collection of horizontal segments. Calling σ_i the (class of the geometric) braid that projects as shown on the right, one easily shows that the group B_m of all m-strand braids is generated by $\sigma_1, ..., \sigma_{m-1}$.

It was then proved by E. Artin in [3, 4] that the group B_m admits the presentation

$$\left\langle \sigma_1, ..., \sigma_{n-1} \;\middle|\; \begin{array}{lll} \sigma_i\sigma_j = \sigma_j\sigma_i & \text{for} & |i-j| \geqslant 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{for} & |i-j| = 1 \end{array} \right\rangle, \tag{1.11}$$

and, by F.A. Garside in [50], that the submonoid B_m^+ of B_m generated by $\sigma_1, ..., \sigma_{m-1}$ admits, as a monoid, the presentation (1.11). The elements of the monoid B_m^+ are called *positive* m-strand braids. By definition, they can be represented by braid diagrams in which all crossings have the same orientation.

Using a fixed structure $(S, *, \bar{*})$ to colour the strands of an S-strand braid diagram using the rules (1.3) provides a map from S^m to itself, namely the map that associates the sequence of output colours to the sequence of input colours. By Lemma 1.2, this map is isotopy-invariant whenever $(S, *)$ is a quandle. Actually, due to the definition of braids with U-turns forbidden, Reidemeister moves of type I are impossible, and it is sufficient to use racks that need not be quandles. Similarly, when one considers positive braids, Reidemeister moves of type II are impossible, and using general LD-systems becomes possible. As, by very definition, colourings are compatible with the product of braids, Lemma 1.2 takes the form:

Lemma 1.6 (Brieskorn [8]). (i) *Assume that* $(S, *)$ *is a rack. Then putting*

$$(a_1, \dots, a_m) \bullet \sigma_i = (a_1, \dots, a_{i-1}, a_i * a_{i+1}, a_i, a_{i+2}, \dots, a_m), \tag{1.12}$$

$$(a_1, \dots, a_m) \bullet \sigma_i^{-1} = (a_1, \dots, a_{i-1}, a_{i+1}, a_i \mathbin{\bar{*}} a_{i+1}, a_{i+2}, \dots, a_m) \tag{1.13}$$

defines an action (on the right) of the group B_m *on* S^m.

(ii) *Assume that* $(S, *)$ *is an LD-system. Then* (1.12) *defines an action of the monoid* B_m^+ *on* S^m.

The action of Lemma 1.6 is called the *Hurwitz action.* Using classical examples of racks then leads to no less classical examples of braid invariants. For instance, considering $\mathbb{Z}$ equipped with the operation $x * y = y + 1$ leads to the augmentation homomorphism from B_m to $(\mathbb{Z}, +)$, whereas considering a $\mathbb{Z}[t, t^{-1}]$-module equipped with the binary operations $x * y = (1 - t)x + ty$ leads to a linear representation of B_m into $\mathrm{GL}_n(\mathbb{Z}[t, t^{-1}])$, the (unreduced) *Burau representation* of B_m. Similarly, considering a rank m free group F_m equipped with the conjugacy operation $x * y = xyx^{-1}$ leads to a (faithful) representation of B_m in $\mathrm{Aut}(F_m)$, the *Artin representation.*

Using colourings: case of links and knots. An (oriented) *m-component geometric link* is a family of m disjoint closed curves embedded in $\mathbb{R}^3$. A *link* is an isotopy class of geometric links, referring here to isotopies of $\mathbb{R}^3$. Knots are links with one component. Projecting geometric links to a plane keeping track of the orientation of crossings and avoiding triple points and tangencies yields a link diagram. As already said, two diagrams represent the same link if and only if they can be transformed into each other by means of Reidemeister moves.

At least two different approaches have been developed in order to use selfdistributive structures to construct link invariants via the colouring approach. Developed by D. Joyce [59] and S. Matveev [77], the first one consists in attaching to every diagram a specific quandle that will capture the topology of the link it represents: assuming that the considered link diagram is the closure $\widehat{D}$ of an m-strand braid diagram D (see Figure 4), one uses m letters $a_1, \dots, a_m$ to colour the input ends of the braid diagram, one propagates the colours throughout the diagram resulting in m output colours $t_1, \dots, t_m$ which are formal combinations of $a_1, \dots, a_m$ by means of two formal operations $*, \bar{*}$, and one defines the *fundamental quandle* Q_D to be the quandle that admits the presentation $\langle a_1, \dots, a_m \mid t_1 = a_1, \dots, t_m = a_m \rangle$. The quandle laws imply that Q_D only depends on the isotopy class of $\widehat{D}$, and it captures almost all topological information about the link represented by D as it is a complete invariant of the isotopy type up to a mirror symmetry. In practice, determining the fundamental quandle effectively is possible only in simple particular cases [80], so one tends to consider more simple structures, typically quotients of the fundamental quandle like the Alexander quandle from which the Alexander polynomial can be read [45, 46].

The second approach consists, as in the case of braids, in fixing one auxiliary quandle (the same for all diagrams) and using it to define topological invariants. Here applications are so numerous that we can only be extremely sketchy and refer

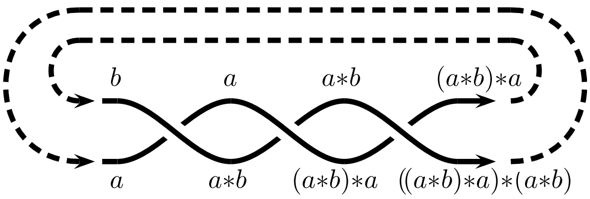


FIGURE 4. A link diagram for the trefoil knot of Figure 1 that is the closure (dashed lines) of a braid diagram, here σ_1^3; the fundamental quandle of the knot is the quandle whose presentation is obtained by equating the labels on the left- and right-ends, here $\langle a, b \mid ((a{*}b){*}a){*}(a{*}b) = a, (a{*}b){*}a = b\rangle$, which is also $\langle a, b \mid b{*}(a{*}b) = a, (a{*}b){*}a = b\rangle$, or, more symmetrically, $\langle a, b, c \mid a{*}b = c, b{*}c = a, c{*}a = b\rangle$. By projecting the fundamental quandle to a group, that is, interpreting $*$ as a conjugacy operation, one obtains the Wirtinger presentation of the fundamental group of the complement of the knot, here the group $\langle a, b \mid aba = bab\rangle$ in which we recognize B_3.

for instance to the survey [18] for a better account and a more complete bibliography. Typically, if S is a finite quandle, one can count how many S-colourings exist. More precisely, the value of the *quandle counting* invariant for a link L is defined to be the number of homomorphisms from the fundamental quandle Q_L to S. It is shown in [53, 51] that the counting invariants associated with certain explicit family of quandles lead to classical link invariants like the linking number or the Alexander polynomial.

The case of Laver tables. Laver tables are very far from all racks and quandles that have been mentioned above—and, much more generally, from those that have been used so far. By the way, Laver tables are LD-systems, but they are *not* racks nor *a fortiori* quandles: as asserted in Theorem 1.1(iii), the period of $2^n - 1$ in A_n is 1, meaning that the row of $2^n - 1$ is constant (with value 2^n) and, for $n \geqslant 1$, the associated left-translations is very far from bijective. So, the only direct application is the existence of an Hurwitz action for positive braids:

Lemma 1.7. *For every n, putting*

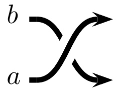
$$(a_1, ..., a_m) \bullet \sigma_i = (a_1, ..., a_{i-1}, a_i * a_{i+1}, a_i, a_{i+2}, ..., a_m) \tag{1.14}$$

defines an action of the monoid B_m^+ on A_n^m.

The problem now is the failure of the laws (1.4) and (1.5), which respectively correspond to Reidemeister moves of types I and II. As for Reidemeister moves of type I, we know that the problem vanishes if we restrict to braids; in the case of links, forgetting type I amounts to restricting to what is called *regular isotopy*, corresponding to considering framed links in which, in addition to the strands, a distinguished orthogonal direction is fixed at each point. The overall conclusion is that the failure of (1.4) alone does not discard topological applications. By the way, a number of recent works consist in extending to general racks some results first established in the particular case of quandles, see for instance [78, 19, 79].

The failure of (1.5) is a more serious obstruction since it *a priori* discards the existence of an Hurwitz action for arbitrary braids. However, it turns out that, at least in good cases, the problem can be solved. So assume that $(S, *)$ is an LD-system. We do not assume that $(S, *)$ is a rack, but we assume for a while that

$(S, *)$ is left-cancellative, that is, the left-translations of $*$ are injective. Then using for the negative crossings the colouring rule



the unique c satisfying $a * c = b$, if such one exists

enables one to define a *partial* Hurwitz action, in the sense that $\vec{a} \bullet w$ need not be defined for every sequence $\vec{a}$ in S^m and every m-strand braid word w: not all sequences of initial colours can be propagated throughout the braid diagram. Then the point is the following (absolutely nontrivial) result:

Lemma 1.8. [23] *Assume that $(S, *)$ is a left-cancellative LD-system.*

(i) *For all m-strand braid words $w_1, ..., w_p$, there exists at least one sequence $\vec{a}$ in S^m such that $\vec{a} \bullet w_i$ is defined for every i.*

(ii) *If w, w' are equivalent m-strand braid words, and $\vec{a}$ is a sequence in S^m such that both $\vec{a} \bullet w$ and $\vec{a} \bullet w'$ are defined, then the latter sequences are equal.*

In other words, although $(S, *)$ is not assumed to be a rack, one obtains an action that is partial but still enjoys good invariance properties. Applying this approach in the case when $(S, *)$ is a free LD-system directly led to the orderability of the group B_m in [23]: free LD-systems are orderable, in the sense that there exists a linear ordering satisfying $a < a * b$ for all a, b, and using the associated colourings naturally leads to ordering braids: a braid β is declared smaller than another braid β' if, for some/any sequence $\vec{a}$ such that both $\vec{a} \bullet \beta$ and $\vec{a} \bullet \beta'$ are defined, the sequence $\vec{a} \bullet \beta$ is smaller than the sequence $\vec{a} \bullet \beta'$ with respect to the lexicographical ordering on S^m.

Laver tables are not left-cancellative, hence they are not directly eligible for Lemma 1.8 and further tricks will have to be developed in order to use them for colourings. A natural but probably too naive approach could be to use fractionary decompositions of braids: every m-strand braid β can be expressed as a quotient $\beta_1^{-1}\beta_2$ where β_1 and β_2 are positive m-strand braids, and the decomposition is unique if one requires in addition that β_1 and β_2 admit no common left-divisor in the monoid B_m^+. Whenever $(S, *)$ is an LD-system, the sequences $\vec{a} \bullet \beta_1$ and $\vec{a} \bullet \beta_2$ are defined for every sequence $\vec{a}$ in S^m and, therefore, the pair $(\vec{a} \bullet \beta_1, \vec{a} \bullet \beta_2)$, which depends only on $\vec{a}$ and β, could be used as a (sort of) colouring for β, see Figure 5 for an example. Alternatively, every braid in $B_m \setminus B_m^+$ admits a unique expression as $\Delta_m^{-d}\beta_0$ where Δ_m is Garside's fundamental m-strand braid, d is a positive integer and β_0 is a positive braid that is not left-divisible by Δ_m in B_m^+, and one could use the pair $(\vec{a} \bullet \Delta_m^d, \vec{a} \bullet \beta_0)$ as another colouring for β.

The failure of left-cancellativity for each of the LD-systems A_n implies that we may have $\vec{a} \bullet \beta_1 = \vec{b} \bullet \beta_1$ with $\vec{a} \neq \vec{b}$ and, from there, with $\vec{a} \bullet \beta_2 \neq \vec{b} \bullet \beta_2$. However, an important positive point is that, by Laver's Theorem 1.1 and at least if Axiom I3 is true, (a subsystem of) the inverse limit A_∞ of the LD-systems A_n is a free LD-system. So, A_n-colourings can be viewed as finite approximations of free LD-system-colourings. Hence the left-cancellativity of free LD-systems might imply a good asymptotic behaviour for A_n-colourings. This is probably worth exploring.

Another (related) direction of research would be to use the approach of R.L. Rubinsztein in [85], based on the introduction of a notion of topological quandle. Laver tables are finite, discrete structures, and they are *a priori* not relevant for such a topological approach. However, the limit A_∞ of the inverse system (A_n, pr_n)

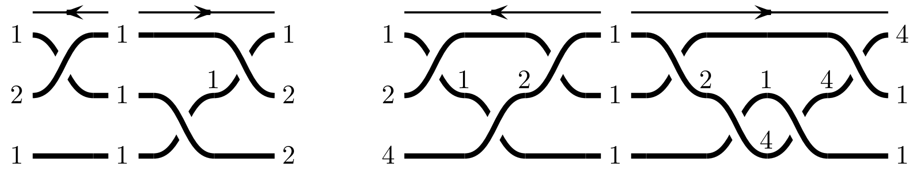


FIGURE 5. Two tentative colourings of the 3-strand braid $\sigma_1\sigma_2\sigma_1^{-1}$ using the Laver table A_2: on the left, we use the decomposition of the braid as an irreducible fraction, namely $\sigma_2^{-1}\sigma_1\sigma_2$, on the right, we use its decomposition with a denominator that is a power of Garside's fundamental braid, namely $\Delta_3^{-1}\sigma_2\sigma_1^2\sigma_2$; in both cases, one propagates the colours from the middle.

consists of all 2-adic integers, and this limit is therefore equipped with a natural valuation, hence with an ultrametric topology. In particular, at least if Axiom I3 is satisfied, the substructure of A_∞ generated by $(1, 1, ...)$ is a free LD-system: the latter is not a rack, but it is close to be one in that all left-translations are one-to-one. Thus investigating the counterpart of the space of colourings $J_Q(L)$, a link invariant defined in [85], seems to be a natural and promising approach.

1.3. **The (co)-homology approach.** Owing to the difficulty of computing the fundamental quandle of a link, it is natural to try to obtain partial information by developing a convenient homology theory, viewed as a way to define sort of linear approximations. Initiated by R. Fenn, C. Rourke, B. Sanderson from 1990 [43, 45] and developed by S. Carter, M. Elhamdadi, M. Saito, and their collaborators in [14, 15, 16, 17], this approach proved to be extremely fruitful, as explained in [43, 18].

The general principle. A comprehensive survey can be found in [18], and we shall just present here the very first steps. As we consider left-selfdistributivity here, it is coherent to use a symmetric version of the construction as developed in [14] or (for the case of a general LD-system) [82]. The starting observation is that several ways of associating chain complexes to an LD-system exist—and even more exist when one starts with a *multi-LD-system*, that is, a set equipped with several mutually distributive operations [83].

Lemma 1.9. *Assume that $(S, *)$ is an LD-system. For $k \geqslant 1$, let $C_k(S)$ be a free $\mathbb{Z}$-module based on S^k, and put $C_0(S) = \mathbb{Z}$. For $1 \leqslant i \leqslant k$, define $\mathbb{Z}$-linear maps $d^*_{k,i}, d^0_{k,i} : C_k(S) \to C_{k-1}(S)$ by*

$$d^*_{k,i}(x_1, ..., x_k) = (x_1, ..., x_{i-1}, \widehat{x_i}, x_i * x_{i+1}, ..., x_i * x_k),$$
$$d^0_{k,i}(x_1, ..., x_k) = (x_1, ..., x_{i-1}, \widehat{x_i}, x_{i+1}, ..., x_k).$$

Put $\partial^*_k := \sum_{i=1}^k (-1)^{i-1} d^*_{k,i}$, and $\partial^0_k := \sum_{i=1}^k (-1)^{i-1} d^0_{k,i}$. Then, for every $\mathbb{Z}$-linear combination ∂_k of ∂^*_k and ∂^0_k, we have $\partial_{k-1} \circ \partial_k = 0$ for every k.

Proof (sketch). A direct computation shows that, for all $1 \leqslant j < i \leqslant k$ and for every choice of $\diamond$ and $\star$ in $\{*, 0\}$, the relation $d^\diamond_{k-1,j} \circ d^\star_{k,i} = d^\star_{k-1,i-1} \circ d^\diamond_{k,j}$ is satisfied. From there, one deduces

$$\partial^*_{k-1} \circ \partial^*_k = \partial^0_{k-1} \circ \partial^0_k = \partial^*_{k-1} \circ \partial^0_k + \partial^0_{k-1} \circ \partial^*_k = 0, \tag{1.15}$$

and the result easily follows. The point in this computation is that, when say $d^*_{k-1} d^*_k(x_1, ..., x_{k+1})$ is expanded into a sum of $(k-1)k$ terms, then, for all $i < j$, there appear exactly two terms in which x_i and x_j do not appear on the right:

$$(-1)^{i+j+2}(x_1, ..., x_{i-1}, \widehat{x_i}, x_i * x_{i+1}, ..., x_i * x_{j-1}, \widehat{x_j},\\ x_i * (x_j * x_{j+1}), ..., x_i * (x_j * x_{k+1})),$$

which corresponds to omitting the jth entry first and then the ith one, and

$$(-1)^{i+j+1}(x_1, ..., x_{i-1}, \widehat{x_i}, x_i * x_{i+1}, ..., x_i * x_{j-1}, \widehat{x_j},\\ (x_i * x_j) * (x_i * x_{j+1}), ..., x_i * (x_i * x_{j+1}), ..., x_i * x_{k+1})),$$

which corresponds to omitting the ith entry first and then the $j-1$st one. The left-selfdistributivity law is then exactly the condition needed to ensure that the above two tuples coincide, so their cumulated contribution vanishes. □

So Lemma 1.9 says that, for every linear combination ∂_k of ∂_k^* and ∂_k^0, the sequence $(C_k(S), \partial_k)_k$ is a chain complex—actually (1.15) says that $(C_k(S), \partial_k^*, \partial_k^0)_k$ is what is called a chain bicomplex—leading to a derived notion of homology and, dually, of cohomology. It is standard to consider two particular linear combinations, namely ∂_k^* itself, and $\partial_k^* - \partial_k^0$.

Definition 1.10. Assume that $(S, *)$ is an LD-system.

(i) For $k \geqslant 1$, put $\partial_k^{\mathrm{R}} = \partial_k^* - \partial_k^0$. Then the chain complex $(C_k(S), \partial_k^{\mathrm{R}})_k$ is called the *rack complex* of $(S, *)$, and its homology is called the *rack homology* of $(S, *)$, denoted by $(H_k^{\mathrm{R}}(S))_k$.

(ii) For every abelian group G, define $C^k(S; G)$ to be $\mathrm{Hom}_{\mathbb{Z}}(C_k(S); G)$ and let ∂_{R}^k be the differential on $C^k(S; G)$ induced by ∂_k^{R}. The cohomology of the cochain complex $(C^k(S; G), \partial_{\mathrm{R}}^k)_k$ is called the G-valued *rack cohomology* of $(S, *)$, denoted by $(H_{\mathrm{R}}^k(S; G))_k$. The image of $\partial_{\mathrm{R}}^{k-1}$ (*resp.* the kernel of ∂_{R}^k) is denoted by $B_{\mathrm{R}}^k(S; G)$ (*resp.* $Z_{\mathrm{R}}^k(S; G)$) and its elements are called G-valued *k-coboundaries* (*resp. k-cocycles*).

(iii) The *one-term distributive homology* and *cohomology* of $(S, *)$ are obtained by replacing ∂_k^{R} with ∂_k^* everywhere.

In the distributive world, the one-term distributive complex can be seen as the analogue of the bar complex for associative algebras, whereas the rack complex is an analogue of the Hochschild complex. This was pointed out in [82] and explained in the context of a unifying braided homology theory in [74].

It turns out that, in view of topological applications, the rack (co)homology is more suitable than the one-term distributive (co)homology. More specifically, the rack 2-cocycles directly lead to interesting invariants. It follows from the explicit definitions of Lemma 1.9 that a map $\phi : S \times S \to G$ defines a (rack) 2-cocycle if and only if it obeys the rule

$$\phi(x, z) + \phi(x * y, x * z) = \phi(y, z) + \phi(x, y * z). \tag{1.16}$$

Then the general principle that makes 2-cocycles valuable here is the possibility of using them in the context of diagram colourings so as to obtain invariants.

Lemma 1.11. [18] (i) *Assume that $(S, *)$ is an LD-system, G is an abelian group, and $\phi : S \times S \to G$ is a G-valued 2-cocycle for $(S, *)$. For D a positive m-strand braid diagram and $\vec{a}$ in S^m, define $\widehat{\phi}_D(\vec{a}) = \sum_i \phi(a_i, b_i)$ where a_i, b_i are the input colours at the ith crossing of D when D is coloured from $\vec{a}$. Then $\widehat{\phi}_D$ is invariant under Reidemeister moves of type III.*

(ii) *If $(S, *)$ is a rack and a negative crossing contributes $-\phi(a, b)$ when the output colours are a, b, then $\widehat{\phi}_D$ is defined for every braid diagram and it is invariant under Reidemeister moves of type II and III.*

(iii) *If $(S, *)$ is a quandle and ϕ satisfies the rule $\phi(x, x) = 0$, then $\widehat{\phi}_D$ is defined for every link diagram and it is invariant under Reidemeister moves of type I–III.*

Proof. The argument for (i) is given in Figure 6. For (ii), concatenating two opposite crossings leads to a contribution of the form $\phi(a, b) - \phi(a, b)$. Finally, for (iii), adding a loop results in an additional contribution of the form $\pm\phi(a, a)$, hence 0 under the additional assumption. □

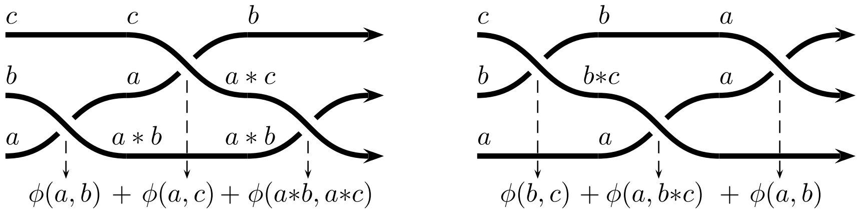

c
c
b
b
a
$a * c$
a
$a * b$
$a * b$
$\phi(a, b) + \phi(a, c) + \phi(a{*}b, a{*}c)$
c
b
a
b
$b{*}c$
a
a
a
$\phi(b, c) + \phi(a, b{*}c) + \phi(a, b)$

FIGURE 6. Using a 2-cocycle to construct a braid invariant: one associates with every braid diagram the sum of the values of the cocycle at the successive crossings labelled by means of the reference LD-system; the cocycle rule of (1.16) is exactly what is needed to guarantee invariance with respect to Reidemeister moves of type III.

Rack 3-cocycles also proved to lead to interesting topological applications, but here we shall only refer to the survey [18] where a complete discussion can be found.

The case of the Laver tables. The Laver tables are directly eligible for the above constructions, and there is no problem for defining the associated homology and cohomology groups. The cases of one-term and rack homologies are rather different, the latter turning out to be much richer than the former.

So, let us first briefly consider the one-term homology of Laver tables. As is the case of many monogenerated LD-systems (that is, LD-systems generated by a single element), the groups $H^*_k(A_n)$ are trivial:

Proposition 1.12. *For every n, the chain complex $(C_k(A_n), \partial^*_k)_k$ is acyclic, and the resulting homology groups $H^*_k(A_n)$ are trivial.*

Proof. We follow the method of [82, Proposition 6.5] and give two different arguments. First define $\theta_k : C_k(A_n) \to C_{k+1}(A_n)$ for $k \geqslant -1$ by $\theta_{-1}(1) = -(2^n)$ and $\theta_k(x_1, ..., x_{k+1}) = -(2^n, x_1, ..., x_k)$. Using the fact that $2^n * x = x$ holds for every x in A_n, we obtain

$$\begin{aligned}\theta_k\partial^*_k(x_1, ..., x_{k+1}) &= \sum_{i=1}^{k+1}(-1)^i(2^n, x_1, ..., x_{x_1}, \widehat{x_i}, x_i{*}x_{i+1}, ..., x_i{*}x_{k+1}),\\ \theta_{k+1}\partial^*_{k+1}(x_1, ..., x_{k+1}) &= (x_1, ..., x_k)\\ &\quad + \sum_{i=1}^{k+1}(-1)^{i+1}(2^n, x_1, ..., x_{x_1}, \widehat{x_i}, x_i{*}x_{i+1}, ..., x_i{*}x_{k+1}),\end{aligned}$$

whence $\theta_k\partial^*_k + \partial^*_{k+1}\theta_{k+1} = \mathrm{id}$. Hence θ_k is a contracting homotopy for $(C_k(A_n), \partial^*_k)$, and the homology of the complex must be trivial.

Putting $\theta'_{-1}(1) = (2^n)$ and $\theta'_k(x_1, ..., x_{k+1}) = (-1)^{k+1}(x_1, ..., x_k, 2^n)$, one checks that θ'_* is an alternative contracting homotopy for $(C_k(A_n), \partial^*_k)$ now using the fact that $x * 2^n = 2^n$ holds for every x in A_n. □

Rack (co)homology of Laver tables is much more interesting. Due to our specific interest in topological applications, and owing to Lemma 1.11, we only consider rack 2-cocycles. Without loss of generality, we also restrict to $\mathbb{Z}$-valued cocycles. Thus, we are interested in maps $\phi : \{1, ..., 2^n\} \times \{1, ..., 2^n\} \to \mathbb{Z}$ that obey (1.16). It turns out that such 2-cocycles can be described very precisely in terms of the values that appear in the columns of the tables A_n. Here we shall mention the main result only, and refer to [33] for more details and proofs.

Proposition 1.13. [33] *For every n, the $\mathbb{Z}$-valued 2-cocycles for A_n make a free $\mathbb{Z}$-module of rank 2^n, with a basis consisting of coboundaries defined for $1 \leqslant q < 2^n$ by*

$$\psi_{q,n}(x, y) = \begin{cases} 1 & \textit{if } q \textit{ appears in the column of } y \textit{ in } A_n \textit{ but not in that of } x * y, \\ 0 & \textit{otherwise,} \end{cases}$$

completed with the constant cocycle with value 1.

A complete enumeration in the case of the 8-element table A_3 is displayed in Table 2.

$\psi_{1,3}$	1	2	3	4	5	6	7	8
1	1	·	·	·	·	·	·	·
2	1	·	·	·	·	·	·	·
3	1	·	·	·	·	·	·	·
4	1	·	·	·	·	·	·	·
5	1	·	·	·	·	·	·	·
6	1	·	·	·	·	·	·	·
7	1	·	·	·	·	·	·	·
8	·	·	·	·	·	·	·	·

$\psi_{2,3}$	1	2	3	4	5	6	7	8
1	·	1	·	·	·	·	·	·
2	1	1	·	·	1	·	·	·
3	1	1	·	·	1	·	·	·
4	·	1	·	·	·	·	·	·
5	1	1	·	·	1	·	·	·
6	1	1	·	·	1	·	·	·
7	1	1	·	·	1	·	·	·
8	·	·	·	·	·	·	·	·

$\psi_{3,3}$	1	2	3	4	5	6	7	8
1	1	·	1	·	1	·	·	·
2	·	·	1	·	·	·	·	·
3	1	·	1	·	1	·	·	·
4	·	·	1	·	·	·	·	·
5	1	·	1	·	1	·	·	·
6	1	·	1	·	1	·	·	·
7	1	·	1	·	1	·	·	·
8	·	·	·	·	·	·	·	·

$\psi_{4,3}$	1	2	3	4	5	6	7	8
1	·	·	·	1	·	·	·	·
2	·	·	·	1	·	·	·	·
3	·	1	·	1	·	1	·	·
4	·	·	·	1	·	·	·	·
5	·	1	·	1	·	1	·	·
6	·	1	·	1	·	1	·	·
7	1	1	1	1	1	1	1	·
8	·	·	·	·	·	·	·	·

$\psi_{5,3}$	1	2	3	4	5	6	7	8
1	1	·	·	·	1	·	·	·
2	1	·	·	·	1	·	·	·
3	1	·	·	·	1	·	·	·
4	·	·	·	·	·	·	·	·
5	1	·	·	·	1	·	·	·
6	1	·	·	·	1	·	·	·
7	1	·	·	·	1	·	·	·
8	·	·	·	·	·	·	·	·

$\psi_{6,3}$	1	2	3	4	5	6	7	8
1	·	1	·	·	·	1	·	·
2	·	1	·	·	·	1	·	·
3	1	1	1	·	1	1	1	·
4	·	·	·	·	·	·	·	·
5	·	1	·	·	·	1	·	·
6	·	1	·	·	·	1	·	·
7	1	1	1	·	1	1	1	·
8	·	·	·	·	·	·	·	·

$\psi_{7,3}$	1	2	3	4	5	6	7	8
1	1	·	1	·	1	·	1	·
2	·	·	·	·	·	·	·	·
3	1	·	1	·	1	·	1	·
4	·	·	·	·	·	·	·	·
5	1	·	1	·	1	·	1	·
6	·	·	·	·	·	·	·	·
7	1	·	1	·	1	·	1	·
8	·	·	·	·	·	·	·	·

TABLE 2. A basis of $B^2_{\mathrm{R}}(A_3)$ consisting of the seven $\{0, 1\}$-valued 2-cocycles $\psi_{q,3}$ with $1 \leqslant q \leqslant 7$. To make reading easier, the zeroes are indicated with "-". Completing with the constant cocycle with value 1, we obtain a basis of $Z^2_{\mathrm{R}}(A_3)$.

The proof of Proposition 1.13 is not trivial, and it relies on the combinatorial properties of right-division in Laver tables. Two-cocycles capture a lot of information about Laver tables: for instance, one can directly recover from the cocycle $\psi_{2^{n-1},n}$ all periods in A_n, hence, in a sense, the most critical combinatorial parameters.

Rack 3-cocycles can also be analyzed for Laver tables. They involve functions of three variables and the 2-cocycle condition (1.16) is replaced with the 3-cocycle condition

$$\begin{aligned}\phi(x*y, x*z, x*t)+&\phi(x,y,z*t)+\phi(x,z,t)\\ &= \phi(x,y*z,y*t)+\phi(y,z,t)+\phi(x,y,t).\end{aligned} \tag{1.17}$$

It turns out that 3-cocycles on A_n make a free $\mathbb{Z}$-module of rank $2^{2n}-2^n+1$, and an explicit basis can again be described [33].

At the moment, the question of using the above results to extract topological information about not necessarily positive braids and possibly links, remains open, as does the question of a topologically interpreting these possible invariants. However, we note that having an explicit basis of 2-cocycles made of $\mathbb{N}$-valued functions seems especially promising in view of combinatorial interpretations, typically for counting arguments. We shall not go further here, but, clearly, the conclusion of this section should be that the (co)homological approach is promising in terms of possible topological applications for Laver tables.

1.4. **The approach of the Yang–Baxter equation.** Another context in which selfdistributive structures are involved is that of the (Quantum) Yang–Baxter equation (YBE or QYBE) and its connections with quantum groups and R-matrices, whence indirectly with topology and knot invariants.

The general principle. We start from the (non-parametric form of) the (quantum) Yang–Baxter equation, or, rather, of the equivalent braid equation.

Definition 1.14. If V is a vector space, an element R of $\mathrm{GL}(V\otimes V)$ is called a *solution of the Yang–Baxter equation* (YBE), or an *R-matrix*, if we have

$$(R\otimes\mathrm{id})(\mathrm{id}\otimes R)(R\otimes\mathrm{id}) = (\mathrm{id}\otimes R)(R\otimes\mathrm{id})(\mathrm{id}\otimes R). \tag{1.18}$$

If one writes R^{ij} for the automorphism of $V^{\otimes 3}$ that corresponds to R acting on the ith and jth coordinates, the YBE becomes

$$R^{12}R^{23}R^{12} = R^{23}R^{12}R^{23}, \tag{1.19}$$

directly reminiscent of the braid relation (1.11)—with the notation of (1.19), the original Yang–Baxter equation is $R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12}$; it transforms into the "braid form" (1.19) when R is replaced by ΠR, where Π is the switch operator that exchanges x and y [58].

For instance, if A is $\mathbb{C}[q,q^{-1}]$ and V is $A\times A$ with standard basis (e_1,e_2), then the automorphism of $V\otimes V$ defined in the basis $(e_1\otimes e_1,\, e_1\otimes e_2,\, e_2\otimes e_1,\, e_2\otimes e_2)$ by the matrix $q^{-1/2}\begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&q-q^{-1}&0\\0&0&0&1\end{pmatrix}$ satisfies (1.18), that is, it is a solution of YBE. This solution is connected with the basic representation of the quantum group $U_q(\mathfrak{sl}(2))$ and the Jones polynomial [61].

Among the (many) solutions of the Yang–Baxter equation, we consider here those solutions R that preserve some fixed basis S of the considered vector space V. Then the restriction of R to $S\times S$ yields a bijection ρ of $S\times S$ to itself that satisfies

$$\rho^{12}\rho^{23}\rho^{12} = \rho^{23}\rho^{12}\rho^{23}, \tag{1.20}$$

and, conversely, every bijection of $S\times S$ into itself that satisfies (1.20) induces a solution of YBE that maps $S^{\otimes 2}$ into itself. Such solutions of YBE are called *set-theoretic* because they are entirely determined by their action on the basis.

Definition 1.15. A *set-theoretic solution of YBE* is a pair (S,ρ) where S is a set and ρ is a bijection of $S\times S$ into itself that satisfies (1.20). In this case, we denote by $\rho_1(x,y)$ and $\rho_2(x,y)$ the first and the second entry of $\rho(x,y)$. A set-theoretic solution (S,ρ) of YBE is called *nondegenerate* if, for every a in S, the left-translation $y\mapsto\rho_1(a,y)$ is one-to-one and the right-translation $x\mapsto\rho_2(x,a)$ are one-to-one.

A set-theoretic solution ρ of YBE can then be characterized in terms of algebraic laws obeyed by the associated maps ρ_1 and ρ_2 viewed as binary operation on the reference set S.

Lemma 1.16. *Assume that (S,ρ) is a set-theoretic solution of YBE. For a,b in S, write $a\rceil b$ for $\rho_1(a,b)$ and $a\lceil b$ for $\rho_2(a,b)$. Then the operations $\rceil$ and $\lceil$ obey the laws*

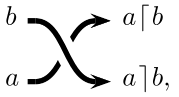
$$(x\rceil y)\rceil((x\lceil y)\rceil z)=x\rceil(y\rceil z),\tag{1.21}$$

$$(x\rceil y)\lceil((x\lceil y)\rceil z)=(x\lceil(y\rceil z))\rceil(y\lceil z),\tag{1.22}$$

$$(x\lceil y)\lceil z=(x\lceil(y\rceil z))\lceil(y\lceil z).\tag{1.23}$$

Conversely, if $\rceil$ and $\lceil$ are binary operations on S that satisfy (1.21)–(1.23) *and ρ is the map of $S\times S$ to itself defined by $\rho(a,b)=(a\rceil b,a\lceil b)$, then (S,ρ) is a set-theoretic solution of YBE. In the above context, (S,ρ) is nondegenerate if and only if left-translations of $\rceil$ and the right-translations of $\lceil$ are one-to-one.*

Proof. We may appeal to braid colourings, using colours from S and the rule

(1.24) 

that is, the extension of (1.3) in which both crossing strands may change colours. Then saying that ρ satisfies (1.20) amounts to saying that, for every choice of the input colours, the output colours of the diagrams $\sigma_1\sigma_2\sigma_1$ and $\sigma_2\sigma_1\sigma_2$ coincide. We read on Figure 7 that this happens exactly when the operation $\lceil$ and $\rceil$ obey the laws of (1.21)–(1.23). The other verifications are then straightforward. □

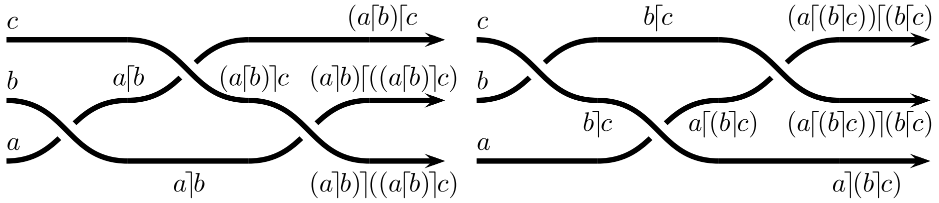

c
$(a\lceil b)\lceil c$
b
$a\lceil b$
$(a\lceil b)\rceil c$
$(a\rceil b)\lceil((a\lceil b)\rceil c)$
a
$a\rceil b$
$(a\rceil b)\rceil((a\lceil b)\rceil c)$
c
$b\lceil c$
$(a\lceil(b\rceil c))\lceil(b\lceil c)$
b
$b\rceil c$
$a\lceil(b\rceil c)$
$(a\lceil(b\rceil c))\rceil(b\lceil c)$
a
$a\rceil(b\rceil c)$

FIGURE 7. Colouring braids using the rule (1.24) is invariant under braid relations if and only if the birack laws (1.21)–(1.23) are obeyed.

The following terminology is then natural:

Definition 1.17. A *birack* is a system $(S,\rceil,\lceil)$ consisting of a set S equipped with two binary operations $\rceil$ and $\lceil$ that satisfy (1.21)–(1.23) and such that the left-translations of $\rceil$ and the right-translations of $\lceil$ are one-to-one.

So Lemma 1.16 says that a set-theoretic solution of the YBE, that is, a set-theoretic R-matrix, is one and the same thing as a birack. Let us mention here the beautiful result of Rump [86] who observed that inverting the operations of a birack enables one to replace biracks and the rather complicated laws (1.21)–(1.23) with equivalent structures made of a set equipped with a binary operation obeying the unique more simple law $(x * y) * (x * z) = (y * x) * (y * z)$, see [32, Chapter XII].

Returning to selfdistributive structures, we immediately obtain the following simple connection:

Lemma 1.18. *Assume that $*$ is a binary operation on a set S. For a, b in S, define $a *_0 b = a$. Then $(S, *, *_0)$ is a birack if and only if $(S, *)$ is a rack.*

The verification has already been done, as this essentially amounts to checking that what remains from (1.21)–(1.23) when the operation $\lceil$ is the trivial operation $*_0$ is the fact that the operation $*$ obeys the left-selfdistributivity law: this corresponds to specializing (1.24) into (1.3), that is, using Figure 3 (case of type III_{++}) instead of Figure 7. In terms of R-matrices, we deduce the following result, which appears in [41] and belongs to folklore:

Proposition 1.19. *Assume that $(S, *)$ is a (finite) rack. Let V be a $\mathbb{C}$-vector space based on a copy $(e_a)_{a \in S}$ of S. Then the endomorphism of $V^{\otimes 2}$ defined by $R(e_a, e_b) = (e_{a*b}, e_a)$ is a (set-theoretic) solution of YBE.*

By definition, a solution of YBE is an automorphism of the considered space: in the context of Proposition 1.19, the endomorphism R is invertible if and only if the map $(a, b) \mapsto (a * b, a)$ is a bijection of $S \times S$, that is, if the left-translations associated with $*$ are bijective. This is the place where the assumption that $(S, *)$ is a rack, and not only a general LD-system, is used.

1.4.1. *The case of the Laver tables.* When we consider the Laver tables, they are indeed finite LD-systems, but they are not racks (except in the trivial case of A_0): in the table of A_n, the row of $2^n - 1$ is constant, hence very far from being bijective. The rest of the construction works, so one naturally obtains is a "pseudo-solution" of YBE, defined to be an endomorphism that satisfies (1.19) but need not be invertible. For instance, the pseudo-R-matrix associated with the Laver table A_1 corresponds to the (non-invertible) matrix $\begin{pmatrix} 0&0&1&0 \\ 0&0&0&0 \\ 1&1&0&0 \\ 0&0&0&1 \end{pmatrix}$, whereas that associated with A_2 is $\begin{pmatrix} 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0 \\ 1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&1&0&1&0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \end{pmatrix}$. In general, the pseudo-R-matrix associated with the Laver table A_n is a square matrix of size 2^{2n} that contains 2^n entries equal to 1. The obvious question is whether such "non-invertible R-matrices" can be of any use, typically in connection with the theory of Hopf algebras. In particular, one can wonder whether q-deformations of such matrices might exist and be useful. As in Subsection 1.2, many results originally established using quandles have been subsequently extended to arbitrary racks [2]. Also, racks proved to play a fundamental rôle in the classification of finite-dimensional pointed Hopf algebras [1]. The question of whether one could go one step further and work with more general LD-systems, specifically with Laver tables, remains open.

2. The well-foundedness of the braid ordering

The second result by Laver we shall mention here involves Artin's braid groups and their ordering(s). Braid groups were proved to be orderable, that is, to admit a left-invariant linear ordering, in 1992 [22, 23], by an ordering that proved both to be canonical, in the sense that many different approaches converge to the same notion, and to have rich combinatorial properties [29]. Using his approach to selfdistributivity via recursive normal forms, Rich Laver proved in 1995 what is probably the deepest result known so far about this braid ordering, namely that its restriction to the monoid of positive braids is a well-ordering. At the moment, this mainly led to applications of logical flavour, but the result inspires several promising ideas for further work.

This section contains four subsections. First, the braid ordering, Laver's result, and its direct consequences are described in Subsection 2.1. Subsequent refinements are mentioned in Subsection 2.2. Next, applications to unprovability statements are stated in Subsection 2.3. Finally, we discuss more hypothetic applications involving the Conjugacy Problem of braids and, possibly, the Markov equivalence relation, in Subsection 2.4.

2.1. **The well-ordering of positive braids.** We recall from Subsection 1.2 that the n-strand braid group, that is, the group of isotopy classes of n-strand braid diagrams, is denoted by B_n. The group B_n admits a more or less canonical family of generators ('the Artin generators') $\sigma_1, ..., \sigma_{n-1}$ in terms of which B_n admits the presentation (1.11). Thus every n-strand braid is represented by various words in the alphabet $\{\sigma_1^{\pm 1}, ..., \sigma_{n-1}^{\pm 1}\}$, naturally called *$n$-strand braid words*, two such braid words representing the same braid if and only if they can be transformed into one another using the relations of (1.11) and the free group relations $\sigma_i \sigma_i^{-1} = \sigma_i^{-1} \sigma_i = 1$.

Definition 2.1. [23] (i) A braid word w is called *σ_i-positive* if it contains the letter σ_i but neither the letter σ_i^{-1} nor any letter $\sigma_j^{\pm 1}$ with $j < i$.

(ii) For β, β' in B_n, say that $\beta <_D \beta'$ holds if, among the various braid words that represent $\beta^{-1}\beta'$, at least one is σ_i-positive for some i.

In other words, $\beta <_D \beta'$ holds if the quotient-braid $\beta^{-1}\beta'$ admits an expression in which the generator σ_i with least index occurs positively only. For instance, consider $\beta = \sigma_1$ and $\beta' = \sigma_2\sigma_1$. Then the quotient $\beta^{-1}\beta'$ is $\sigma_1^{-1}\sigma_2\sigma_1$, so the braid word $\sigma_1^{-1}\sigma_2\sigma_1$ is one expression of this quotient, and it is neither σ_1-positive nor σ_2-positive. Now another expression of the same quotient-braid is $\sigma_2\sigma_1\sigma_2^{-1}$, which is a σ_1-positive braid word. Therefore $\sigma_1 <_D \sigma_2\sigma_1$ is declared to be true.

Proposition 2.2. [22, 23] *For every n, the relation $<_D$ is a linear ordering on the group B_n and it is left-invariant, that is, $\beta <_D \beta'$ implies $\gamma\beta <_D \gamma\beta'$ for every γ.*

The braid order $<_D$ will be referred to here as the *D-ordering* of braids ('Dehornoy ordering'). There is no need to mention a braid index here, as one shows that the D-ordering on B_{n-1} is the restriction of the D-ordering on B_n when B_{n-1} is embedded in B_n by adding an nth strand on the top of the diagrams. Going to the limit yields a left-invariant ordering on the limit group B_∞. Note that, for $n = 2$, the group B_n is the free group generated by σ_1, so it is isomorphic to the additive group of integers and the associated D-ordering corresponds to the usual ordering of integers via $p \mapsto \sigma_1^p$.

For $n \geqslant 3$, the D-ordering of n-strand braids is not right-invariant, and it is actually easy to show that no left-invariant ordering of B_n may be right-invariant. However, Laver proved

Theorem 2.3 (Laver, [71]). *For all β in B_n and i in $\{1, ..., n-1\}$, the relation $\beta <_D \sigma_i \beta$ is satisfied.*

In other words, whereas $\gamma <_D \gamma'$ does not imply $\gamma\beta <_D \gamma'\beta$ in general, $1 <_D \sigma_i$ does imply $1\beta <_D \sigma_i\beta$ for every braid β. Laver's proof of Theorem 2.3 relies on colouring braids (in the sense of Subsection 1.2) using elements of free LD-systems and developing a fine combinatorial analysis of the latter structures by means of normal forms of their elements introduced by tricky recursive definitions—a quite delicate argument actually.

Let us say that a word w is a *subword* of another word w' if w' can be obtained from w by inserting letters, not necessarily in adjacent positions. Then Theorem 2.3 directly implies that the D-ordering has what is usually called the Subword Property:

Corollary 2.4 (Laver, [71]). *If β, β' are braids and some braid word representing β is a subword of some braid word representing β, then $\beta \leqslant_D \beta'$ holds.*

Proof. For an induction, it is sufficient to show that the conjunction of $\beta = \beta_1\beta_2$ and $\beta' = \beta_1\sigma_i\beta_2$ implies $\beta <_D \beta'$. Now Theorem 2.3 implies $\beta_2 <_D \sigma_i\beta_2$, whence $\beta_1\beta_2 <_D \beta_1\sigma_i\beta_2$ since $<_D$ is invariant under left-multiplication. □

The Subword Property directly implies that every conjugate β' of a positive braid, that is, every braid of the form $\gamma^{-1}\beta\gamma$ with $\beta \in B_n^+$, satisfies $\beta' >_D 1$, since we can write $\gamma^{-1}\beta\gamma >_D \gamma^{-1}\gamma = 1$. It follows in turn that $\beta >_D 1$ is true for every *quasipositive* braid β, the latter being defined as a braid that can be expressed as a product of conjugates of positive braids [81].

Using the Subword Property in a more tricky way, one shows the following property that involves a sort of shifted conjugacy.

Corollary 2.5. [25, Lemma 3.5] *Let* sh *be the shift endomorphism of B_∞ that maps σ_i to σ_{i+1} for every i. Then, for every braid β, one has $\mathrm{sh}(\beta)\,\sigma_1 >_D \beta$.*

However, the most promising consequence of Laver's result is that some fragments of the D-ordering are well-orderings, that is, every nonempty subset must have a smallest element.

Corollary 2.6 (Laver, [71]). *For every n, the restriction of the D-ordering to B_n^+ is a well-ordering.*

Proof. By a celebrated result of Higman [52], an infinite set of words over a finite alphabet necessarily contains two elements w, w' such that w is a subword of w'. Let $\beta_1, \beta_2, ...$ be an infinite sequence of braids in B_n^+. Our aim is to prove that this sequence is not strictly decreasing. For each p, choose a positive braid word w_p representing β_p. There are only finitely many n-strand braid words of a given length, so, for each p, there exists $p' > p$ such that $w_{p'}$ is at least as long as w_p.

So, inductively, we can extract a subsequence $w_{p_1}, w_{p_2}, \ldots$ in which the lengths are non-decreasing. If the set $\{w_{p_1}, w_{p_2}, \ldots\}$ is finite, there exist k, k' such that w_{p_k} and $w_{p_{k'}}$ are equal, and then we have $\beta_{p_k} = \beta_{p_{k'}}$. Otherwise, by Higman's result, there exist k, k' such that w_{p_k} is a subword of $w_{p_{k'}}$, and, by construction, we must have $p_k \leqslant p_{k'}$. By Corollary 2.4, this implies $\beta_{p_k} \leqslant_D \beta_{p_{k'}}$ in B_n^+. So, in any case, the sequence $\beta_1, \beta_2, \ldots$ is not strictly decreasing. □

The well-order property established by Laver for B_n^+ is a strong statement. As a general matter of fact, the D-ordering on B_n is an intricate relation for $n \geqslant 3$: it is not Archimedean (there exist β, β' such that $\beta^p <_D \beta'$ holds for every p), it is not Conradian (there exist β, β' such that $\beta' \beta^p <_D \beta$ holds for every p), it has infinite ascending and descending sequences, *etc.* By contrast, Laver's result shows that forgetting about non-positive braids yields a very simple ordering, in particular one where the position of an element can be specified using just an ordinal, see Figure 8.

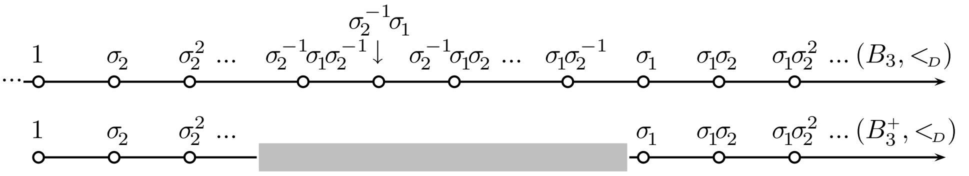

1
σ_2
σ_2^2 ...
$\sigma_2^{-1}\sigma_1\sigma_2^{-1}$
$\sigma_2^{-1}\sigma_1$ ↓
$\sigma_2^{-1}\sigma_1\sigma_2$ ...
$\sigma_1\sigma_2^{-1}$
σ_1
$\sigma_1\sigma_2$
$\sigma_1\sigma_2^2$ ... $(B_3, <_D)$
1
σ_2
σ_2^2 ...
σ_1
$\sigma_1\sigma_2$
$\sigma_1\sigma_2^2$ ... $(B_3^+, <_D)$

FIGURE 8. Restricting to positive braids changes the ordering: for instance, in $(B_3^+, <_D)$, the braid σ_1 is the limit of σ_2^p, whereas, in $(B_3, <_D)$, it is an isolated point with immediate predecessor $\sigma_1\sigma_2^{-1}$; the grey part in B_3 includes infinitely many braids, such as $\sigma_2^{-1}\sigma_1$ and its neighbours—and much more—but none of them lies in B_3^+.

Among the standard consequences of the well-order property, we deduce

Corollary 2.7. *Every nonempty subset of B_n^+ is either cofinal or it has a least upper bound inside $(B_n^+, <_D)$.*

Indeed, for X included in B_n^+, unless X is unbounded in B_n^+, the set of all upper bounds of X is nonempty, hence it admits a least element.

Before turning to further results, let us conclude this subsection with a conjecture of R. Laver that involves braids and extends his well-order result. We saw in Lemma 1.7 and Lemma 1.8 that, whenever $(S, *)$ is a left-cancellative LD-system, one can define a partial Hurwitz action of B_n on S^n. For every sequence $\vec{a}$ in S^n, we can then consider the family

$$D_S(\vec{a}) = \{\beta \in B_n \mid \vec{a} \bullet \beta \text{ is defined}\}.$$

As the action of positive braids is always defined, we always have $B_n^+ \subseteq D_S(\vec{a})$. In some cases [66], the family $D_S(\vec{a})$ reduces to B_n^+ and, therefore, Corollary 2.6 says that the restriction of the D-ordering to this family $D_{B_\infty}(1, \ldots, 1)$ is a well-order.

Conjecture 2.8 (Laver, private communication)**.** *If $(S, *)$ is a free LD-system, the restriction of the D-ordering to every family of the form $D_S(\vec{a})$ is a well-order.*

The conjecture remains open when $\vec{a}$ has length 3 and more. As noted by R. Laver, the above braid formulation is equivalent to a formulation involving free LD-systems only, and connected with the results of [72] and [73]. Let us also mention a similar conjecture where free LD-systems are replaced with the (left-cancellative) LD-system $(B_\infty, *)$ where $*$ is the shifted conjugacy operation

$$\beta * \gamma = \beta \cdot \mathrm{sh}(\gamma) \cdot \sigma_1 \cdot \mathrm{sh}(\beta)^{-1}, \tag{2.1}$$

with sh the endomorphism that maps σ_i to σ_{i+1} for every i. This conjecture is also open so far.

2.2. **Further refinements.** We now report about some subsequent results, mainly by S. Burckel, J. Fromentin, and the author, that made the description of the braid well-order more precise than the original abstract argument of R. Laver.

The restriction of the D-ordering to the monoid B_∞^+ of positive braids on an unbounded number of strands is not a well-ordering since it contains the descending sequence $\sigma_1 >_D \sigma_2 >_D \cdots$. However, it is easy, and technically convenient, to reverse the role of left and right in braid diagrams and to obtain a well-ordering on B_∞^+.

Definition 2.9. For $n \geqslant 2$, let ϕ_n be the automorphism of the group B_n (‘*flip* automorphism’) that maps σ_i to σ_{n-i} for every i. For β, β' in B_n, we write $\beta <_D^\phi \beta'$ for $\phi_n(\beta) <_D \phi_n(\beta')$. The relation $<_D^\phi$ is called the *flipped D-ordering* on B_n.

It is straightforward to check that the relation $<_D^\phi$ is a left-invariant linear ordering on B_n, and that it is independent of n in that, for β, β' in B_n, the relation $\beta <_D^\phi \beta'$ holds in B_n if and only if it holds in $B_{n'}$ for any $n' \geqslant n$. When compared with the D-ordering, the flipped D-ordering amounts to exchanging left and right: $\beta <_D^\phi \beta'$ holds if and only if the quotient-braid $\beta^{-1}\beta'$ admits an expression in which the generator σ_i with *largest* index occurs positively only. In particular, we have $\sigma_1 <_D^\phi \sigma_2 <_D^\phi \cdots$. The benefit of considering $<_D^\phi$ instead of $<_D$ is to give an improved picture of the way the monoids B_n^+ embed into one another, see Figure 9. Indeed, one shows:

Proposition 2.10. [29, Proposition II.2.10] *The restriction of the flipped D-ordering of B_∞ to B_∞^+ is a well-ordering and, for every n, the set B_n^+ is the initial segment of $(B_\infty^+, <_D^\phi)$ determined by σ_n, that is, we have $B_n^+ = \{\beta \in B_\infty^+ \mid \beta <_D^\phi \sigma_n\}$.*

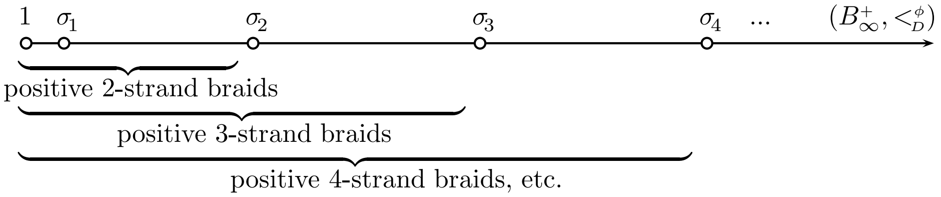


FIGURE 9. The well-ordered set $(B_\infty^+, <_D^\phi)$: an increasing union of end-extensions, in which B_n^+ is the initial segment determined by σ_n.

Laver's proof that the restriction of the D-ordering to positive braids is a well-ordering is indirect, and it remains ineffective in that it does not specifies the order type of $(B_n^+, <_D)$ or $(B_\infty^+, <_D^\phi)$. These natural questions have been solved.

Proposition 2.11 (Burckel, [10])**.** *For every n, the order type of $(B_n^+, <_D)$ is $\omega^{\omega^{n-2}}$.*

Proposition 2.11 also implies that the order type of $(B_n^+, <_D^\phi)$ is $\omega^{\omega^{n-2}}$ and, therefore, that of $(B_\infty^+, <_D)$ is ω^{ω^ω}, the upper bound of $\omega^{\omega^{n-2}}$ when n goes to infinity.

Burckel's result relies on an intricate inductive argument, which assigns to every n-strand braid word a finite rooted tree with uniform height $n-2$, so that, for β, β' in B_n^+, the relation $\beta <_D \beta'$ holds if and only if the `ShortLex`-minimal tree representing β is `ShortLex`-smaller than the `ShortLex`-minimal tree representing β', where a height m rooted tree is considered to be a finite sequence of height $m-1$ rooted trees, and a height m rooted tree $(T_1, ..., T_\ell)$ is declared `ShortLex`-smaller than another height m rooted tree $T' = (T'_1, ..., T'_{\ell'})$, if $\ell < \ell'$ holds, or if $\ell = \ell'$ holds and there exists i such that $T_j = T'_j$ holds for $j < i$ and T_i is `ShortLex`-smaller than T'_i.

In Burckel's approach, the `ShortLex`-minimal tree representing a braid β appears as the terminal point of a recursive reduction process and it is not easily determined. The situation was made simpler when the simple connection between $(B_n^+, <_D)$ and $(B_{n-1}^+, <_D)$ stated in Proposition 2.12 below was found, leading to considering the ordering of B_n^+ as an iterated extension of the ordering of B_2^+, that is, of the standard ordering of natural numbers.

If β, β' are positive braids, one says that β *right-divides* β' if there exists a positive braid γ satisfying $\beta' = \gamma\beta$. Garside's theory of braids [50] implies that every braid in B_n admits a unique maximal right-divisor lying in B_{n-1}, namely the least common left-multiple of all right-divisors of β lying in B_{n-1}. Iterating the result, one obtains a decomposition of every positive n-strand braid in terms of a sequence of positive $(n-1)$-strand braids. The result is then that, in terms of such decompositions, the flipped D-ordering on B_n^+ is the `ShortLex`-extension of the flipped D-ordering on B_{n-1}^+.

Proposition 2.12. [28] *For $n \geqslant 3$ and β in B_n^+, define the ϕ_n-splitting of β to the (unique) sequence $(\beta_p, ..., \beta_1)$ in B_{n-1}^+ such that, for each r, the braid β_r is the maximal right-divisor of γ_{r-1} that lies in B_{n-1}^+, where γ_r is inductively defined by $\beta = \gamma_r\beta_r$ starting from $\beta_0 = 1$. Then, for β, β' in B_n^+ with ϕ_n-splittings $(\beta_p, ..., \beta_1)$ and $(\beta'_{p'}, ..., \beta'_1)$, the relation $\beta <_D^\phi \beta'$ holds if and only if $(\beta_p, ..., \beta_1)$ is smaller than $(\beta'_{p'}, ..., \beta'_1)$ for the* `ShortLex`*-extension of $(B_{n-1}^+, <_D^\phi)$.*

Saying that $(\beta_p, ..., \beta_1)$ is the ϕ_n-splitting of a braid β means that one has

$$\beta = \phi_n^{p-1}(\beta_p) \cdot ... \cdot \phi_n(\beta_2) \cdot \beta_1, \tag{2.2}$$

and σ_1 is the only generator σ_i that right-divides $\phi_n^{n-r}(\beta_p) \cdots \phi_n(\beta_{r+1})\,\beta_r$ for each r. By iterating the decomposition process, one eventually obtains for every positive braid β an expression in terms of shifted powers of σ_1, that is, a distinguished expression by a braid word, called the *alternating normal form* of β.

As the right-divisibility relation of braids can be tested in linear time, the ϕ_n-splitting of a positive braid can be computed in quadratic time and Proposition 2.12 implies that, for every n, the orderings $<_D^\phi$ and $<_D$ of B_n can be recognized in quadratic time.

One of the nice consequences of Laver's well-ordering result is that every positive braid can be characterized by a unique parameter, namely the ordinal that describes its rank in the well-order $(B_\infty^+, <_D^\phi)$: for instance, the rank of the trivial braid 1 is 0, that of σ_1, the immediate successor of 1, is 1 and, for $i \geqslant 2$, the rank of σ_i is the length of the initial segment determined by σ_i, which is B_i^+ by Proposition 2.10, hence this rank is $\omega^{\omega^{i-1}}$ by Proposition 2.11. It is then natural to ask for a complete explicit description of the rank function. The latter is *not* an algebraic homomorphism with respect to the ordinal sum: in general, the rank of $\beta_1\beta_2$ is not the sum of the ranks of β_1 and β_2. This happens to be true when β_2 is σ_1, which has rank 1 but, for instance, the rank of $\sigma_1\sigma_2$ turns out to be ω^2, which is not $1+\omega$ (that is, ω) although the rank of σ_2 is ω. The problem essentially amounts to recognizing which braid words are alternating normal; in the case of 3-strand braids, the answer is simple:

Proposition 2.13. [28, Proposition 6.7] *Put $\varepsilon_1 = 0$, $\varepsilon_2 = 1$, and $\varepsilon_r = 2$ for $r \geqslant 3$. Then every braid in B_3^+ admits a unique expression $\sigma_{\mathrm{parity}(p)}^{e_p} \cdots \sigma_2^{e_2}\sigma_1^{e_1}$ with $e_p \geqslant 1$, and $e_r \geqslant \varepsilon_r$ for $r < p$; its rank in $(B_3^+, <_D^\phi)$ is then*

$$\omega^{p-1} \cdot e_p + \sum_{p>r\geqslant 1} \omega^{r-1} \cdot (e_r - \varepsilon_r). \tag{2.3}$$

For instance, the alternating normal form of Garside's fundamental braid Δ_3 is $\sigma_1\sigma_2\sigma_1$, as the latter word satisfies the defining inequalities of Proposition 2.13, contrary to $\sigma_2\sigma_1\sigma_2$, that is, $\sigma_2^1\sigma_1^1\sigma_2^1\sigma_1^0$, in which the third exponent from the right, namely 1, is smaller than the minimal legal value $\varepsilon_3 = 2$. So, in this case, the sequence $(e_p, ..., e_1)$ is $(1, 1, 1)$, and, applying (2.3), we deduce that the rank of Δ_3 in $(B_3^+, <_D^\phi)$—hence in $(B_\infty^+, <_D^\phi)$ as well—is $\omega^2 + 1$.

In the general case, only partial results are known: for instance, it is shown in [28] that the family of all alternating normal n-strand braid words is recognized by a finite state automaton and, in [11], S. Burckel describes a recursive procedure for determining the rank in B_n^+.

We conclude with extensions of the previous results involving other submonoids of the braid groups. It turns out that the argument used to establish that the restriction of the D-ordering to the monoid B_n^+ is a well-ordering works for other submonoids:

Corollary 2.14. *Assume that M is a submonoid of B_∞ that is generated by finitely many elements, each of which is a conjugate of some generator σ_i. Then the restriction of the D-ordering to M is a well-order.*

Proof. The argument is the same as for Corollary 2.6: assuming that M is generated by $\beta_1, ..., \beta_p$, it suffices to show that the Subword Property is valid for the words in the alphabet $\{\beta_1, ..., \beta_p\}$ and, for this, it is enough to show that $\beta <_D \beta_k\beta$ holds for every positive braid β. Now, assuming $\beta_k = \gamma^{-1}\sigma_i\gamma$, Theorem 2.3 gives $\gamma\beta <_D \sigma_i\gamma\beta$, whence $\beta <_D \gamma^{-1}\sigma_i\gamma\beta$, for every β. □

The hypothesis that the monoid M is finitely generated is crucial in Corollary 2.14. For instance, the descending sequence $\sigma_1 >_D \sigma_2 >_D ...$ witnesses that the submonoid B_∞^+ of B_∞ is not well-ordered by the D-ordering. Such phenomena already occur inside B_3: for instance, the submonoid of B_3 generated by all conjugates $\sigma_2^{-p}\sigma_1\sigma_2^p$ of σ_1—and, more generally, the submonoid of all quasipositive n-strand braids—contains the infinite descending sequence $\sigma_1 >_D \sigma_2^{-1}\sigma_1\sigma_2 >_D \sigma_2^{-2}\sigma_1\sigma_2^2 >_D \cdots$.

A typical example of a monoid eligible for Corollary 2.14 is the *dual braid monoid* B_n^{+*}, which is the submonoid of B_n generated by the $\binom{n}{2}$ braids of the form $\sigma_i \cdots \sigma_j\sigma_{j-1}^{-1} \cdots \sigma_i^{-1}$, the 'band' or 'Birman–Ko–Lee' generators [6]. J. Fromentin showed in [48] that the order type of $(B_n^{+*}, <_D^\phi)$ is $\omega^{\omega^{n-2}}$, using a characterization of the restriction of the (flipped) D-ordering to B_n^{+*} in terms of a normal from ('rotating normal form') that is analogous to the alternating normal form of Proposition 2.12 but involves an order n automorphism analogous to a rotation instead of the order 2 automorphism ϕ_n that is analogous to a symmetry [49]. At the technical level, the properties of the rotating normal form are often nicer than those of the alternating normal form.

Another indirect outcome of Laver's result is the investigation of the well-foundedness of alternative braid orderings. There exists an uncountable family of left-invariant linear orderings on the braid group B_n [29, Chapter XIV]. Most of them do not induce well-orderings on the braid monoid B_n, but at least all the orderings stemming from the hyperbolic geometry approach suggested by W. Thurston and investigated in [87] do, and it was recently shown that the associated order type is again $\omega^{\omega^{n-2}}$ [56, 57].

2.3. **Applications to unprovability statements.** The order type of the well-ordering on B_n^+, namely $\omega^{\omega^{n-2}}$, is a (relatively) large ordinal: although not extremely large in the hierarchy of countable ordinals, it is large enough to give rise to nontrivial unprovability statements. The principle is that, although the well-order property forbids that infinite descending sequences exist, there exist nevertheless finite descending sequences that are so long that their existence cannot be proved in weak logical systems.

It is well-known that there exist strong limitations about the sentences possibly provable in a given formal system, starting with Gödel's famous theorems implying that certain arithmetic sentences cannot be proved in the first-order Peano system. However, the Gödel sentences have a strong logical flavour and they remain quite remote from the sentences usually considered by mainstream mathematicians. It is therefore natural to look for further sentences that are unprovable in the Peano system, or in other formal systems, and, at the same time, involve objects and properties that are both simple and natural. Typical results in this direction involve finite combinatorics, well-quasiorders, and the Ramsey Theory [7, 47, 90].

We shall mention some results along this line of research that involve the D-ordering of braids. Here we shall restrict to the case of 3-strand braids and refer to [13] for details and extensions. In order to construct a long sequence of braids, we start with an arbitrary braid in B_3^+ and then repeat some transformation until, if ever, the trivial braid is obtained. Here, the transformation at step t will consist in removing one crossing, but, in all cases but one, introducing t new crossings. It is reminiscent of Kirby–Paris' Hydra Game [64], with Hercules chopping off one head of the Hydra and the Hydra sprouting t new heads. The paradoxical result is that, contrary to what examples suggest, one always reaches the trivial braid after finitely many steps.

Definition 2.15. For β is a nontrivial positive 3-strand braid, and t a positive integer, define $\beta\{t\}$ to be the braid represented by the following diagram: in the alternating normal diagram of β, we remove one crossing in the critical block, defined to be the rightmost block whose size is not the minimal legal one, and add t crossings in the next block, if it exists, that is, if the critical block is not the final block of σ_1. The $\mathcal{G}_3$*-sequence from* β is defined by $\beta_0 = \beta$ and $\beta_t = \beta_{t-1}\{t\}$ for $t \geqslant 1$; it stops when the trivial braid 1 is possibly obtained.

It is easy to check that the $\mathcal{G}_3$-sequence from $\sigma_2^2\sigma_1^2$ has length 14: it consists of $\sigma_2^2\sigma_1^2$, $\sigma_2^2\sigma_1$, σ_2^2, $\sigma_2\sigma_1^3$, $\sigma_2\sigma_1^2$, $\sigma_2\sigma_1$, σ_2, σ_1^7, σ_1^6, σ_1^5, σ_1^4, σ_1^3, σ_1^2, σ_1, and finally 1.

Similarly, the $\mathcal{G}_3$-sequence from Δ_3 has length 30. Not all examples are so easy: starting from $\sigma_1^2\sigma_2^2\sigma_1^2$, a braid with six crossings only, one does reach the trivial braid, but after $90,159,953,477,630$ steps.

Proposition 2.16 (Carlucci, D., Weiermann [13])**.** (i) *For every braid β in B_3^+, the $\mathcal{G}_3$-sequence from β is finite, that is, there exists a finite number t for which $\beta_t = 1$ holds.*

(ii) *The statement of* (i) *is an arithmetic statement that cannot be proved from the axioms of the system* $\mathsf{I}\Sigma_1$.

Although braids are not natural numbers, one can encode braids and their basic operations using natural numbers and the usual arithmetic operations. Therefore, it makes sense to speak of braid properties that can be proved from a certain system of arithmetical axioms: by this we mean that some reasonable encoding of braids by natural numbers has been fixed once for all and we consider the arithmetic counterpart of the braid property we have in mind.

The standard first-order Peano axiomatization of arithmetic PA consists of basic axioms involving addition and multiplication, plus the induction scheme, which asserts that, for each first-order formula $\Phi(x)$ involving $+, \times$ and $<$, the conjunction of $\Phi(0)$ and $\forall n(\Phi(n) \Rightarrow \Phi(n{+}1))$ implies $\forall n(\Phi(n))$. Then $\mathsf{I}\Sigma_k$ is the subsystem of PA in which the induction principle is restricted to formulas of the form $\exists x_1 \forall x_2 \exists x_3 \cdots Q x_k(\Psi)$, where Q is $\exists$ or $\forall$ according to the parity of k and Ψ is a formula that only contains bounded quantifications $\forall x{<}y$ and $\exists x{<}y$.

Proof of Proposition 2.16 (sketch). For (i), one shows that every $\mathcal{G}_3$-sequence is descending with respect to $<_D^\phi$, and the result then follows from Laver's well-order result (Corollary 2.6). For (ii), in order to prove that a certain sentence Φ is not provable from the axioms of $\mathsf{I}\Sigma_1$, it is sufficient to establish that, from Φ, and using arguments that can be formalized in $\mathsf{I}\Sigma_1$, one can prove the existence of a function that grows as fast as the Ackermann function. Now, if $T(\beta)$ denotes the length of the $\mathcal{G}_3$-sequence from β, then the function $p \mapsto T(\Delta_3^p)$ actually grows as fast as the Ackermann function. □

The $\mathsf{I}\Sigma_1$-unprovability result of Proposition 2.16 is directly connected with the order type ω^ω of the well-ordering on B_3^+. Similarly, the order type ω^{ω^ω} of the well-ordering on B_∞^+ induces a connection with the stronger system $\mathsf{I}\Sigma_2$: in [13] a certain notion of $\mathcal{G}_\infty$-sequence in B_∞^+ is defined so that, as can be expected, the analog of Proposition 2.16 is established, namely every $\mathcal{G}_\infty$-sequence is finite but that result cannot be proved from $\mathsf{I}\Sigma_2$. As the order-type of $(B_\infty^+, <_D^\phi)$ is larger than that of $(B_3^+, <_D^\phi)$, the $\mathcal{G}_\infty$-sequences can be made longer than the $\mathcal{G}_3$-sequences, so proving their finiteness is more difficult and requires a stronger logical context.

Further results involve the transition between provability and unprovability, which turns out to happen at a level that can be described precisely. To this end, one considers the length of descending sequences of braids that admit some bounded Garside complexity. Let Δ_3 be the positive 3-strand braid $\sigma_1\sigma_2\sigma_1$. Garside [50] showed that every braid in B_3^+ right-divides some power Δ_3^d. Define the *degree* $\deg\beta$ of a braid β to be the least integer d such that β right-divides Δ_3^d. Then, for f a fixed function on the integers, we consider (the length of) the descending sequences $(\beta_0, ..., \beta_N)$ in $(B_3^+, <_D^\phi)$ satisfying $\deg\beta_t \leqslant d + f(t)$ for every t, that is, the descending sequences whose complexity is, in a sense, bounded by f. If f is constant, the number of braids β satisfying $\deg\beta \leqslant d + f(t)$ is finite, so the length of a sequence as above is certainly bounded. One can show using König's Lemma that, for every function f, the length of a sequence as above is bounded by some constant (depending on d). The question is whether this can be proved in the system $\mathsf{I}\Sigma_1$, and the result is that there exists a quick transition phase between $\mathsf{I}\Sigma_1$-provability and $\mathsf{I}\Sigma_1$-unprovability. Indeed, using Ack_r for the functions defined by the double recursion rules: $\mathrm{Ack}_0(x) = x + 1$, $\mathrm{Ack}_r(0) = \mathrm{Ack}_{r-1}(1)$, and $\mathrm{Ack}_r(x + 1) = \mathrm{Ack}_{r-1}(\mathrm{Ack}_r(x))$ for $r \geqslant 1$ and Ack for the diagonal function defined by $\mathrm{Ack}(x) = \mathrm{Ack}_x(x)$ ('Ackermann function'), and using f^{-1} for the functional inverse of f, we have

Proposition 2.17. [13] *Denote by WO_f the statement:*

"For every d, there exists N such that every descending sequence $(\beta_0, \beta_1, ...)$ in $(B_3^+, <_D^\phi)$ satisfying $\deg \beta_t \leqslant d + f(t)$ for every t has length at most N."

Put $f_r(x) = \lfloor \sqrt[\mathrm{Ack}_r^{-1}(x)]{x} \rfloor$ for $r \geqslant 0$, and $f(x) = \lfloor \sqrt[\mathrm{Ack}^{-1}(x)]{x} \rfloor$. Then, for every r, the principle WO_{f_r} is provable in $\mathsf{I}\Sigma_1$, but WO_f is not provable in $\mathsf{I}\Sigma_1$.

The functions involved in Proposition 2.17 all are of the form $x \mapsto \sqrt[g(x)]{x}$ where g is a very slowly increasing function. The proof is a—rather sophisticated—mixture of combinatorial methods and specific results about the number of 3-strand braids satisfying some order and degree constraints.

It is likely that a similar result involving B_∞^+ and $\mathsf{I}\Sigma_2$ could be established, but this was not made in [13].

2.4. **Braid conjugacy.** We conclude with applications of the well-order property of a different nature, namely those where the order is used to provide distinguished elements. As we shall see, not much is known so far, but the approach leads at the least to testable conjectures.

As a preliminary remark, let us mention that connections are known between the position of a braid β in the D-ordering, typically the unique interval $[\Delta_n^{2k}, \Delta_n^{2k+1})$ it belongs to (the parameter k is then called the *D-floor* of β), and various topological parameters associated with the link that is the closure of β [75, 76, 54, 55], see [31], but we shall not give details here as these results do not involve the well-order property.

By very definition, the well-order property asserts that every nonempty subset of B_∞^+ contains a $<_D^\phi$-minimal element, and that every nonempty subset of B_n^+ contains a $<_D$-minimal element. In this way, one obtains a natural way to distinguish an element in a family of positive braids. As the D-ordering of braids appears as canonical in that many different approaches lead to the same ordering, one may expect that the elements so identified enjoy good properties.

The Conjugacy Problem for the group B_n, namely the question of algorithmically recognizing whether two braids are conjugated, is one of the main algorithmic questions involving braids. The question was shown to be decidable by F.A. Garside [50] but, in spite of many efforts, the best methods known so far in the case of 5 strands and more have an exponential complexity with respect of the length of the input braid words—which led to proposing braid groups and conjugacy as a cryptographic platform [65, 27].

Because of the specific properties of Garside's fundamental braid Δ_n, every braid of B_n can be expressed as $\Delta_n^{-d}\beta$ with β in B_n^+, and any two braids are conjugated if and only if they are positively conjugated, that is, conjugated via a positive braid.

It follows that, in order to solve the Conjugacy Problem of B_n, it is enough to solve the Conjugacy Problem of the monoid B_n^+. Now, the well-order property implies

Lemma 2.18. *For every braid β in B_n^+, the intersection of the conjugacy class of β with B_n^+ contains a unique $<_D$-minimal element $\mu_n(\beta)$.*

Being able to algorithmically compute the function μ_n would provide an immediate solution for the Conjugacy Problem of B_n^+, since β is conjugated to β' if and only if $\mu_n(\beta)$ and $\mu_n(\beta')$ are equal. So the question is to compute the function μ_n.

At the moment, the question remains open but, at least in the case of 3-strand braids, the simple connection between the (flipped) D-ordering and the alternating normal form of Proposition 2.13 makes it realistic to explicitly compute the function μ_3. To this end, the obvious approach is to investigate the analog of the cycling and decycling operations of [42] with the Garside normal form replaced by the alternating normal form (or the rotating normal form), that is, the operations corresponding to $(\beta_p, ..., \beta_1) \mapsto (\beta_1, \beta_p, ..., \beta_2)$ and $(\beta_p, ..., \beta_1) \mapsto (\beta_{p-1}, ..., \beta_1, \beta_p)$.

β	1	σ_1	σ_1^2	$\cdots$	σ_2	$\sigma_2\sigma_1$	$\sigma_2\sigma_1^2$	$\cdots$	σ_2^2	$\sigma_2^2\sigma_1$	$\sigma_2^2\sigma_1^2$	$\cdots$
$\mathrm{rk}(\beta)$	0	1	2		ω	$\omega{+}1$	$\omega{+}2$		$\omega{\cdot}2$	$\omega{\cdot}2{+}1$	$\omega{\cdot}2{+}2$	
$\mu_3(\beta)$	↻	↻	↻		σ_1	↻	↻		σ_1^2	$\sigma_2\sigma_1^2$	↻	

β	$\cdots$	σ_2^3	$\sigma_2^3\sigma_1$	$\sigma_2^3\sigma_1^2$	$\cdots$	$\sigma_1\sigma_2$	$\sigma_1\sigma_2\sigma_1$	$\sigma_1\sigma_2\sigma_1^2$	$\cdots$
$\mathrm{rk}(\beta)$		$\omega{\cdot}3$	$\omega{\cdot}3{+}1$	$\omega{\cdot}3{+}2$		ω^2	$\omega^2{+}1$	$\omega^2{+}2$	
$\mu_3(\beta)$		σ_1^2	$\sigma_2\sigma_1^3$	$\sigma_2^2\sigma_1^3$		$\sigma_2\sigma_1$	$\sigma_2\sigma_1^2$	$\sigma_2\sigma_1^3$	

β	$\cdots$	$\sigma_1\sigma_2^2$	$\sigma_1\sigma_2^2\sigma_1$	$\sigma_1\sigma_2^2\sigma_1^2$	$\cdots$	$\sigma_1^2\sigma_2$	$\sigma_1^2\sigma_2\sigma_1$	$\sigma_1^2\sigma_2\sigma_1^2$	$\cdots$
$\mathrm{rk}(\beta)$		$\omega^2{+}\omega$	$\omega^2{+}\omega{+}1$	$\omega^2{+}\omega{+}2$		$\omega^2{\cdot}2$	$\omega^2{\cdot}2{+}1$	$\omega^2{\cdot}2{+}2$	
$\mu_3(\beta)$		$\sigma_2\sigma_1^2$	$\sigma_2^2\sigma_1^2$	$\sigma_2^2\sigma_1^3$		$\sigma_2\sigma_1^2$	$\sigma_2\sigma_1^3$	$\sigma_2\sigma_1^4$	

β	$\cdots$	$\sigma_1^2\sigma_2^2$	$\sigma_1^2\sigma_2^2\sigma_1$	$\sigma_1^2\sigma_2^2\sigma_1^2$	$\cdots$	$\sigma_1^2\sigma_2^3$	$\sigma_1^2\sigma_2^3\sigma_1$	$\cdots$
$\mathrm{rk}(\beta)$		$\omega^2{\cdot}2{+}\omega$	$\omega^2{\cdot}2{+}\omega{+}1$	$\omega^2{\cdot}2{+}\omega{+}2$		$\omega^2{\cdot}2{+}\omega{\cdot}2$	$\omega^2{\cdot}2{+}\omega{\cdot}2{+}1$	
$\mu_3(\beta)$		$\sigma_2^2\sigma_1^2$	$\sigma_2^2\sigma_1^3$	$\sigma_2^2\sigma_1^4$		$\sigma_2^2\sigma_1^3$	$\sigma_2^3\sigma_1^3$	

β	$\cdots$	$\sigma_1^2\sigma_2^4$	$\sigma_1^2\sigma_2^4\sigma_1$	$\sigma_1^2\sigma_2^4\sigma_1^2$	$\cdots$	$\sigma_1^3\sigma_2$	$\sigma_1^3\sigma_2\sigma_1$	$\cdots$
$\mathrm{rk}(\beta)$		$\omega^2{\cdot}2{+}\omega{\cdot}3$	$\omega^2{\cdot}2{+}\omega{\cdot}3{+}1$	$\omega^2{\cdot}2{+}\omega{\cdot}3{+}2$		$\omega^2{\cdot}3$	$\omega^2{\cdot}3{+}1$	
$\mu_3(\beta)$		$\sigma_2^2\sigma_1^4$	$\sigma_2^3\sigma_1^4$	$\sigma_2^4\sigma_1^4$		$\sigma_2\sigma_1^3$	$\sigma_2\sigma_1^4$	

β	$\cdots$	$\sigma_1^3\sigma_2^2$	$\sigma_1^3\sigma_2^2\sigma_1$	$\cdots$	$\sigma_2\sigma_1^2\sigma_2$	$\sigma_2\sigma_1^2\sigma_2\sigma_1$	$\sigma_2\sigma_1^2\sigma_2\sigma_1^2$	$\cdots$
$\mathrm{rk}(\beta)$		$\omega^2{\cdot}3{+}\omega$	$\omega^2{\cdot}3{+}\omega{+}1$		ω^3	$\omega^3{+}1$	$\omega^3{+}2$	
$\mu_3(\beta)$		$\sigma_2^2\sigma_1^3$	$\sigma_2^2\sigma_1^4$		$\sigma_2^2\sigma_1^2$	$\sigma_2\sigma_1^4$	↻	

TABLE 3. A few values of the function μ_3 on B_3^+: here the braids are enumerated in $<_D^\phi$-increasing order, specified using their alternating normal form, and accompanied with their ordinal rank in the well-order; the symbol ↻ indicates the fixed points of μ_3, that is, the braids that are minimal in their conjugacy class.

Some values of the function μ_3 are listed in Table 3; these values should suggest both that μ_3 is nontrivial but also that it obeys simple rules. For instance, a typical rule suggested by the computer experiments is the following formula (an n-strand version is easy to guess):

Conjecture 2.19 (D., Fromentin, Gebhardt, [31]). *For every β in B_3^+, one has*

$$\mu_3(\beta\Delta_3^2) = \sigma_1\sigma_2^2\sigma_1 \cdot \mu_3(\beta) \cdot \sigma_1^2.$$

It is reasonable to expect that an investigation of cycling and decycling for the alternating normal form would lead to a solution of that specific conjecture and, more generally, lead to the practical computation of the function μ_3 on B_3^+, and subsequently of the function μ_n on B_n^+.

If this program can be fulfilled, it would then become foreseeable to investigate similar questions for analogous functions in which the conjugacy relation is replaced with the Markov equivalence relation, that is, the equivalence relation on B_∞, or rather on $\bigcup_n B_n \times \{n\}$, generated by conjugacy together with the Markov transformation $(\beta, n) \sim (\beta\sigma_n^{\pm 1}, n+1)$. It is well-known [5] that the closures of two braid diagrams represent the same link if and only if the braids are Markov-equivalent; moreover, at the expense of taking into account a power of the braid Δ_n^2, one can always reduce to the case of positive braids. So, should the above approach turn out to be possible, one would associate with every link L a unique distinguished braid, namely the $(B_\infty^+, <_D^\phi)$-smallest positive braid in the equivalence class of the braids that represent L—or, equivalently, the unique ordinal that is the rank of this distinguished braid in the well-order. Of course, the problem here is not the existence of the smallest braid or the ordinal (which is guaranteed by Laver's result), but its practical computability.

Remark 2.20. In the case of Markov-equivalence, the braid index and the braid length are not preserved, so an equivalence class is in general infinite and Laver's result is essential to ensure the existence of a smallest representative. However, in the case of conjugacy, the braid index and the length (of positive braids) are preserved, so the considered equivalence classes are finite: in this case, the existence of a smallest element is guaranteed for every linear ordering of braids, and Laver's result is important for a motivation, but it is not needed to ensure the existence of the function μ_n. As we cannot expect to solve the Conjugacy Problem for free, this suggests that the investigation of μ_n may still require significant technical efforts.

References

[1] N. Andruskiewitsch & M. Graña, *From racks to pointed Hopf algebras*, Adv. in Math. **178** (2003) 177–243.

[2] N. Andruskiewitsch, F. Fantino, G. García, L. Vendramin, *On Nichols algebras associated to simple racks*, Contemp. Math. **537** (2011) 31–56.

[3] E. Artin, *Theorie der Zopfe*, Abh. Math. Sem. Univ. Hamburg **4** (1925) 47–72.

[4] E. Artin, *Theory of Braids*, Ann. of Math. **48** (1947) 101–126.

[5] J. Birman, *Braids, Links, and Mapping Class Groups*, Annals of Math. Studies **82** Princeton Univ. Press (1975).

[6] J. Birman, K.H. Ko, & S.J. Lee, *A new approach to the word problem in the braid groups*, Advances in Math. **139-2** (1998) 322-353.

[7] A. Bovykin, *Brief introduction to unprovability*, Logic Colloquium 2006, S. Cooper, H. Geuvers, A. Pillay, J. Väänänen eds., Lecture Notes in Logic, Cambridge University Press (2009) pp. 38–64.

[8] E. Brieskorn, *Automorphic sets and braids and singularities*, Braids, Contemporary Maths AMS **78** (1988) 45–117.

[9] R. H. Bruck, *A survey of binary systems*, Springer-Verlag (1966).

[10] S. Burckel, *The wellordering on positive braids*, J. Pure Appl. Algebra **120-1** (1997) 1–17.

[11] S. Burckel, *Computation of the ordinal of braids*, Order **16** (1999) 291–304.

[12] G. Burde & H. Zieschang, *Knots*, de Gruyter, Berlin (1985).

[13] L. Carlucci, P. Dehornoy, & A. Weiermann, *Unprovability statements involving braids*, Proc. London Math. Soc. **2011** (102) 159–192.

[14] J.S. Carter, D. Jelsovsky, S. Kamada, & M. Saito, *Computation of quandle cocycle invariants of knotted curves and surfaces*, Adv. Math. **157** (2001) 36–94.

[15] J.S. Carter, M. Elhamdadi, & M. Saito, *Twisted quandle homology theory and cocycle knot invariants*, Algebra Geom. Topol. **2** (2002) 95–135.

[16] J.S. Carter, M. Elhamdadi, & M. Saito, *Homology theory for the set-theoretic Yang-Baxter equation and knot invariants from generalizations of quandles*, Fund. Math. **184** (2004) 31–54.

[17] J.S. Carter, S. Kamada, & M. Saito, *Geometric interpretations of quandle homology*, J. Knot Th. Ramific. **10** (2001) 345–386.

[18] S. Carter, *A survey of quandle ideas*, in: Introductory lectures on Knot Theory, Kauffmann and al. eds, Series on Knots and Everything vol. 46, World Scientific (2012), pages 22–53.

[19] W. Chang & S. Nelson, *Rack shadows and their invariants*, J. Knot Theory Ramifications **20** (2011) 1259–1269.

[20] P. Dehornoy, Π^1_1*-complete families of elementary sequences*, Ann. P. Appl. Logic **38** (1988) 257–287.

[21] P. Dehornoy, *Preuve de la conjecture d'irréflexivité pour les structures distributives libres*, C. R. Acad. Sci. Paris **314** (1992) 333–336.

[22] P. Dehornoy, *Deux propriétés des groupes de tresses*, C. R. Acad. Sci. Paris **315** (1992) 633–638.

[23] P. Dehornoy, *Braid groups and left distributive operations*, Trans. Amer. Math. Soc. **345-1** (1994) 115–151.

[24] P. Dehornoy, *Another use of set theory*, Bull. Symb. Logic **2-4** (1996) 379–391.

[25] P. Dehornoy, *Strange questions about braids*, J. Knot Th. and its Ramifications **8-5** (1999) 589–620.

[26] P. Dehornoy, *Braids and Self-Distributivity*, Progress in Math. vol. 192, Birkhäuser, (2000).

[27] P. Dehornoy, *Braid-based cryptography*, Contemp. Math. **360** (2004) 5–33.

[28] P. Dehornoy, *Alternating normal forms for braids and locally Garside monoids*, J. Pure Appl. Algebra **212-11** (2008) 2416–2439.

[29] P. Dehornoy, with I. Dynnikov, D. Rolfsen, B. Wiest, *Ordering Braids*, Mathematical Surveys and Monographs vol. 148, Amer. Math. Soc. (2008).

[30] P. Dehornoy, *Elementary embeddings and algebra*, Handbook of Set Theory, vol. 2 (Foreman, Kanamori, Eds.), Springer, pp. 737–774 (2010)

[31] P. Dehornoy, *Braid Order, Sets, and Knots*, in: Introductory lectures on Knot Theory, Kauffmann and al. eds, Series on Knots and Everything vol. 46, World Scientific (2012), pages 77–96.

[32] P. Dehornoy, with F. Digne, E. Godelle, J. Michel, *Foundations of Garside Theory*, Submitted manuscript, arXiv:1309.0796, http://www.math.unicaen.fr/∼garside/Garside.pdf.

[33] P. Dehornoy & V. Lebed, *Two- and three-cocycles for Laver tables*, Preprint, arXiv:1401.2335.

[34] R. Dougherty & T. Jech, *Finite left-distributive algebras and embedding algebras*, Advances in Math. **130** (1997) 201–241.

[35] A. Drápal, *On the semigroup structure of cyclic left-distributive algebras*, Semigroup Forum **51** (1995) 23–30.

[36] A. Drápal, *Finite left distributive algebras with one generator*, J. Pure Appl. Algebra **121** (1997) 233–251.

[37] A. Drápal, *Finite left distributive groupoids with one generator*, Int. J. Algebra & Computation **7** (1997) 723–748.

[38] A. Drápal, *Homomorphisms of primitive left distributive groupoids*, Comm. in Algebra **22** (1994) 2579–2592.

[39] A. Drápal, *Persistency of cyclic left distributive algebras*, J. Pure Appl. Algebra **105** (1995) 137–165.

[40] A. Drápal, *The third level of homomorphisms in finite cyclic left-distributive algebras*, Unpublished preprint (1996).

[41] V.G. Drinfeld, *On some unsolved problems in quantum group theory*, in: Quantum Groups (Leningrad, 1990), Lecture Notes in Mathematics, Vol. 1510, Springer, Berlin, 1992, pp. 18.

[42] E.A. Elrifai & H.R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford **45-2** (1994) 479–497.

[43] R. Fenn, *Tackling the trefoils*, J. Knot Theory Ramifications **21** (2012) 1240004-1–20.

[44] R. Fenn & C. Rourke, *Racks and links in codimension 2*, J. of Knot Th. Ramific. **1-4** (1992) 343–406;

[45] R. Fenn, C. Rourke, & B. Sanderson, *James bundles*, Proc. London Math. Soc. **89** (2004) 217240.

[46] R. Fenn, C. Rourke, & B. Sanderson, *The rack space*, Trans. Amer. Math. Soc. **359** (2007) 701740.

[47] H. Friedman, *Long finite sequences*, J. Combin. Th. A **95** (2001) 102–144.

[48] J. Fromentin, *The well ordering on dual braid monoids*, J. Knot Th. Ramifications **19** (2010) 631–654.

[49] J. Fromentin, *Every braid admits a short sigma-definite expression*, J. Europ. Math. Soc. **13** (2011) 1591–1631.

[50] F. A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20** No.78 (1969) 235–254.

[51] N. Harrell & S. Nelson, *Quandles and linking number*, J. Knot Theory Ramifications **16** (2007) 12831293.

[52] G. Higman, *Ordering by divisibility in abstract algebras*, Proc. London Math. Soc. **2** (1952) 326-336

[53] A. Inoue, *Homomorphisms of knot quandles to Alexander quandles*, J. Knot Th. Ramific. **10** (2001) 813–822.

[54] T. Ito, *Braid ordering and the geometry of closed braids*, Geom. Topol. **15** (2011) 473–498.

[55] T. Ito, *Braid ordering and knot genus*, J. Knot Th. Ramif. **20** (2011) 1311–1323.

[56] T. Ito, *On finite Thurston-type orderings of braid groups*, Groups, Complexity Cryptol. **2** (2010) 123—155.

[57] T. Ito, *Finite Thurston type orderings on dual braid monoids*, J. Knot Th. Ramif. **20** (2011) 995–1019.

[58] M. Jimbo, *Introduction to the Yang–Baxter equation*, Int. J. of Modern Physics A **4** (1989) 3759–3777.

[59] D. Joyce, *A classifying invariant of knots: the knot quandle*, J. of Pure and Appl. Algebra **23** (1982) 37–65;

[60] A. Kanamori, *The Higher Infinite*, Springer-Verlag (1994).

[61] C. Kassel, *Quantum Groups*, Springer-Verlag (1995).

[62] L. Kauffman, *On knots*, Annals of Math. Studies 115, Princeton Univ. Press (1987).

[63] L. Kauffman, *Virtual knots theory*, Europ. J. of Combinatorics **99** (20) 663–691.

[64] L. Kirby & J. Paris, *Accessible independence results for Peano Arithmetic*, Bull. London Math. Soc. **14** (1982) 285–293.

[65] K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang, & C. Park, *New public-key cryptosystem using braid groups*, Crypto 2000; Springer Lect. Notes in Comput. Sci., 1880 (2000) 166–184.

[66] D. Larue, *Left-distributive and left-distributive idempotent algebras*, Ph D Thesis, University of Colorado, Boulder (1994).

[67] R. Laver, *Elementary embeddings of a rank into itself*, Abstracts Amer. Math. Soc. **7** (1986) 6.

[68] R. Laver, *The left distributive law and the freeness of an algebra of elementary embeddings*, Advances in Math. **91-2** (1992) 209–231.

[69] R. Laver, *A division algorithm for the free left distributive algebra*, Oikkonen & *al.* eds, Logic Colloquium '90, Lect. Notes Logic **2** (1993) 155–162.

[70] R. Laver, *On the algebra of elementary embeddings of a rank into itself*, Advances in Math. **110** (1995) 334–346.

[71] R. Laver, *Braid group actions on left distributive structures and well-orderings in the braid group*, J. Pure Appl. Algebra **108-1** (1996) 81–98.

[72] R. Laver & S. Miller, *Left-divisors in the free one-generated LD-algebra*, J. Pure and Appl. Algebra **215** (2010) 276–282.

[73] R. Laver & S. Miller, *The free one-generated left distributive algebra: basics and a simplified proof of the division algorithm*, Central Europ. J. of Math. **11** (2013) 2150–2175.

[74] V. Lebed, *Homologies of algebraic structures via braidings and quantum shuffles*, J. Algebra **391** (2013) 152–192.

[75] A. Malyutin, *Twist number of (closed) braids*, St. Peterburg Math. J. **16** (2005) 791–813.

[76] A. Malyutin & N. Netsvetaev, *Dehornoy's ordering on the braid group and braid moves*, St. Peterburg Math. J. **15** (2004) 437–448.

[77] S.V. Matveev, *Distributive groupoids in knot theory*, Math. Sbornik **119, 1-2** (1982) 73–83.

[78] S. Nelson, *Link invariants from finite racks*, arXiv:0808.0029.

[79] S. Nelson & R. Wieghard, *Link invariants from finite Coxeter racks*, J. Knot Theory Ramifications **20** (2011) 1247–1257.

[80] M. Niebrzydowski & J.H. Przytycki, *The quandle of the trefoil as the Dehn quandle of the torus*, Osaka J. Math. **46** (2009) 645–659.

[81] S. Orevkov, *Strong positivity in the right-invariant order on a braid group and quasipositivity*, Mat. Zametki **68** (2000) 692–698 (Russian); English translation in *Math. Notes* **68** (2000), no. 5-6, 588-593.

[82] J. Przytycki, *Distributivity versus associativity in the homology theory of algebraic structures*, Demonstratio Math. **44** (2011) 823-869.

[83] J. Przytycki & K. Putyra, *Homology of distributive lattices*, Journal of homotopy and related structures **8** (2013) 35–65.

[84] J. Przytycki & A. Sikora, *Distributive products and their homology*, Comm. in Algebra **42(4)** (2014) to appear, arXiv:1105.3700.

[85] R.L. Rubinsztein, *Topological quandles and invariants of links*, J. Knot Theory Ramifications **16** (2007) 789–808.

[86] W. Rump, *A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation*, Advances in Math. **193** (2005) 40–55.

[87] H. Short & B. Wiest, *Orderings of mapping class groups after Thurston*, Ens. Math. **46** (2000) 279–312.

[88] M. Smedberg, *A dense family of well-behaved monogenerated LD groupoids*, Archive for Mathematical Logic **52** (2013) 377-402.

[89] R. Solovay, W. Reinhardt & A. Kanamori, *Strong axioms of infinity and elementary embeddings*, Ann. Math. Logic **13** (1978) 73–116.

[90] A. Weiermann, *Analytic combinatorics, proof-theoretic ordinals, and phase transitions for independence results*, Ann. Pure Appl. Logic **136** (2005) 189–218.

Laboratoire de Mathématiques Nicolas Oresme, UMR 6139 CNRS, Université de Caen
BP 5186, 14032 Caen Cedex, France

Current address: Laboratoire Preuves, Programmes, Systèmes, UMR 7126 CNRS, Université Paris-Diderot Case 7014, 75205 Paris Cedex 13, France

E-mail address: dehornoy@math.unicaen.fr

URL: //www.math.unicaen.fr/∼dehornoy