ON STRUCTURE GROUPS OF SET-THEORETIC SOLUTIONS TO THE YANG–BAXTER EQUATION

VICTORIA LEBED AND LEANDRO VENDRAMIN

ABSTRACT. This paper explores the structure groups $G_{(X,r)}$ of finite non-degenerate set-theoretic solutions (X, r) to the Yang–Baxter equation. Namely, we construct a finite quotient $\overline{G}_{(X,r)}$ of $G_{(X,r)}$, generalizing the Coxeter-like groups introduced by Dehornoy for involutive solutions. This yields a finitary setting for testing injectivity: if X injects into $G_{(X,r)}$, then it also injects into $\overline{G}_{(X,r)}$. We shrink every solution to an injective one with the same structure group, and compute the rank of the abelianization of $G_{(X,r)}$. We show that multipermutation solutions are the only involutive solutions with diffuse structure group; that only free abelian structure groups are biorderable; and that for the structure group of a self-distributive solution, the following conditions are equivalent: biorderable, left-orderable, abelian, free abelian, torsion free.

INTRODUCTION

The physics-motivated *Yang–Baxter equation* is now omnipresent in mathematics. The interest to its set-theoretic version goes back to Drinfel′d [Dri92]. Compared to linear solutions, set-theoretic ones are easier to study and classify. At the same time, they form a rich family of structures, and their deformations yield a wide variety of linear solutions. Furthermore, one gets powerful knot and link invariants by counting diagram colorings by such solutions. In this paper, by a *solution* we mean a YBE solution

$$r(x,y) = (\sigma_x(y), \tau_y(x))$$

on a finite set X, with r required to be invertible and *non-degenerate* (i.e., the maps τ_y and σ_y are invertible for all y).

Two types of solutions are particularly well studied: *involutive* solutions (with $r^2 = \mathrm{Id}$), and *self-distributive (SD) solutions*, i.e., those of the form

$$r_\triangleleft(x,y) = (y, x \triangleleft y),$$

where $(X, \triangleleft)$ is a *rack*, i.e., the binary operation $\triangleleft$ is self-distributive and has invertible right translations. These two types can be thought of as perpendicular axes in the variety of solutions. Thus, to any solution one can associate its *structure rack* $(X, \triangleleft_r)$ [Sol00, LYZ00, LV17], which is trivial if and only if the solution is involutive. The interplay between these two axes is fundamental in our work.

Following Etingof, Schedler, and Soloviev [ESS99], consider the *structure group*

$$G_{(X,r)} = \langle X \mid xy = \sigma_x(y)\tau_y(x) \text{ for all } x, y \in X \rangle$$

of a solution (X, r). The group algebra of $G_{(X,r)}$ can be regarded as the universal enveloping algebra of r.

Structure groups bring group-theoretic tools into the study of the YBE. Thus, classifying structure groups (or certain quotients thereof) is a reasonable first step in the classification of solutions. This strategy was successfully implemented, for instance, by Cedó, Jespers, and del Río [CJdR10]. On the other hand, for involutive r, $G_{(X,r)}$ is a quadratic algebra with interesting properties, both geometric and algebraic: it is Bieberbach and of I-type (as shown by Gateva-Ivanova and Van den Bergh [GIVdB98]), and also Garside (according to Chouraqui [Cho10]).

Extending the work of Chouraqui–Godelle [CG14], Dehornoy [Deh15] constructed a *finite quotient* $\overline{G}_{(X,r)}$ of $G_{(X,r)}$ by a normal free abelian subgroup; here r is again involutive. It is analogous to the Coxeter group quotients for Artin–Tits groups. In particular, the solution r and the Garside structure of G reconstruct from $\overline{G}$.

Recently, the *orderability* problem was solved for the groups $G = G_{(X,r)}$ with involutive r, first partially by Chouraqui [Cho16], and then completely by Bachiller, Cedó, and the second author [BCV17]. Their results read as follows:

- G is bi-orderable $\iff$ G is free abelian $\iff$ r is trivial: $r(x, y) = (y, x)$;
- G is left-orderable $\iff$ G is poly-$\mathbb{Z}$ $\iff$ r is MP.

An involutive solution is called *multipermutation (MP)* if several iterations of the retraction construction $X \mapsto \mathrm{Ret}(X) = X/\sim$ yield a one-element set; here $x \sim y$ means $\sigma_x = \sigma_y$, and r induces a solution on $\mathrm{Ret}(X)$ [ESS99]. This gives a new example of a structural property of the solution (being MP) which can be read off its structure group (namely, its orderability). The importance of MP solutions is discussed, for instance, in [CJO10, GIC12, Ven16, BCJO].

These results work for involutive r only. General structure groups are much more mysterious. Among the above properties, only the existence of finite quotients was established for all solutions. Concretely, Lu, Yan, and Zhu [LYZ00] described a finitely generated abelian normal subgroup $Z^0_{(X,r)}$ of $G_{(X,r)}$ of finite index. Soloviev [Sol00] showed the rank of $Z^0_{(X,r)}$ to be $K_r = \# \mathrm{Orb}(X, \lhd_r)$, which is the number of *orbits* of X with respect to the actions $x \mapsto x \lhd_r y$. The quotient $G^0_{(X,r)} = G_{(X,r)}/Z^0_{(X,r)}$ looses a lot of information about (X, r). Thus, there are infinitely many solutions sharing the same G^0 [CJdR10]. In the involutive case, G^0 is only a quotient of Dehornoy's $\overline{G}$, and no longer encodes (X, r) faithfully. In the self-distributive case, a quotient $\overline{G}$ of $G = G_{(X,\lhd)}$ refining G^0 was described for 1-orbit racks by Graña, Heckenberger, and the second author [GHV11]. Their construction is as close to faithfulness as possible: the natural map $X \to G$ is injective if and only if it remains so after passing to the quotient $X \to \overline{G}$.

This paper extends some of the above results to all solutions (X, r). Theorem 5.6 describes a normal free abelian subgroup $Z_{(X,r)}$ of $G_{(X,r)}$ of rank K_r, such that

- the quotient $\overline{G}_{(X,r)} = G_{(X,r)}/Z_{(X,r)}$ is finite;
- the natural map $X \to G_{(X,r)}$ is injective if and only if it remains so after passing to the quotient $X \to \overline{G}_{(X,r)}$.

A solution is called *injective* if the map $X \to G_{(X,r)}$ is so. Involutive solutions are archetypal examples: many of their properties, such as the group-theoretical characterization, generalize to all injective solutions [Sol00]. Our construction yields an injectivity test involving only finite objects X and $\overline{G}_{(X,r)}$, as opposed to the infinite group $G_{(X,r)}$. This answers a question of Soloviev [Sol00]. The subgroup

$Z_{(X,r)}$ is generated by appropriately chosen powers $x^d \in G_{(X,\lhd_r)}$ of $x \in X$ (which coincide for x's from the same $\lhd_r$-orbit), pulled back by the bijective 1-cocycle $J \colon G_{(X,r)} \to G_{(X,\lhd_r)}$ from [Sol00, LYZ00, LV17]. For SD solutions, $\overline{G}$ recovers the above quotient; for involutive solutions, it is a slight variation thereof. Our construction is explicit and the proofs are elementary; this is to be compared with the study of G^0 in [Sol00], which required the Hochschild–Serre sequence.

As a by-product, we characterize finite injective racks as sub-racks of finite *conjugation racks* (that is, finite groups with the conjugation operation $g \lhd h = h^{-1}gh$).

Using the finite quotients $\overline{G}$ and other arguments, we improve the understanding of structure groups. In particular, we show that:

- $G_{(X,r)}$ is *virtually abelian*, hence *linear*, hence *residually finite*;
- the rank of its *abelianization* is the number k_r of its *orbits* with respect to the actions $x \mapsto \sigma_y(x)$ and $x \mapsto \tau_y(x)$:

$$\mathrm{rk}(\mathrm{Ab}\, G_{(X,r)}) = k_r;$$

- every solution shrinks to an injective one with the same structure group; this construction is completely algorithmic;
- MP solutions are the only involutive solutions with *diffuse* structure group; this answers a question of Chouraqui [Cho16];
- $G_{(X,r)}$ is biorderable $\iff G_{(X,r)} \cong \mathbb{Z}^{k_r}$;
- for the structure group of an SD solution, the following conditions are equivalent:

  biorderable $\iff$ left-orderable $\iff$ (free) abelian $\iff$ torsion free.

Left orderability and diffusion for general structure groups are more delicate problems, and remain open. Another open question is to understand the torsion of $\mathrm{Ab}\, G_{(X,r)}$ in terms of basic characteristics of (X,r).

One more interesting question, not addressed in this paper, would be to determine what finite groups can be obtained as quotients of a given structure group $G_{(X,r)}$ by normal abelian subgroups. Is $G^0_{(X,r)}$ minimal in this family? Is our $\overline{G}_{(X,r)}$ minimal among quotients preserving injectivity?

The paper is organized as follows. Sections 1–2 summarize basic definitions and results on structure groups and racks. They also contain new results:

- The right and the left structure racks of a solution are isomorphic.
- The structure groups of a solution and of its biquandle quotient are isomorphic. This can be understood in terms of the structure rack and its quandle quotient. (*Biquandles* and *quandles* are, respectively, solutions and racks satisfying an additional condition, which simplifies the study of their structure groups.)

Section 3 contains a technical lemma on passing to quotients in bijective (semi)group 1-cocycles, illustrated with the 1-cocycle $J \colon G_{(X,r)} \to G_{(X,\lhd_r)}$. In Section 5, this lemma is used to pull back the finite quotient $\overline{G}_{(X,\lhd_r)}$, described in Section 4, to get the desired finite quotient $\overline{G}_{(X,r)}$. Sections 6–7 contain applications of our construction, and prove the properties of structure groups listed above. In Appendix A, we describe all size 3 biquandles, their structure groups, and the finite quotients $\overline{G}$ thereof. Even these small examples exhibit a wide range of behaviours. Thus among solutions with the same structure rack we find solutions with different G, or the same G but different $\overline{G}$, or else the same G and $\overline{G}$ but distinct 1-cocycles J.

1. Structure groups for YBE solutions

In this paper, by a *solution* we mean a finite invertible non-degenerate set-theoretic solution (X, r) of the *Yang–Baxter equation* (YBE)

$$r_1 r_2 r_1 = r_2 r_1 r_2, \qquad \text{where } r_1 = r \times \operatorname{Id}_X,\ r_2 = \operatorname{Id}_X \times r.$$

This means that X is a finite set, the map

$$r \colon X \times X \to X \times X,$$

$$(x, y) \mapsto (\sigma_x(y), \tau_y(x))$$

is bijective, with the inverse

$$r^{-1} \colon (x, y) \mapsto (\widehat{\sigma}_x(y), \widehat{\tau}_y(x)),$$

and its components $\sigma_x, \tau_x \colon X \to X$ are bijective for all $x \in X$. Such solutions are used for producing efficient coloring invariants of knots and their higher-dimensional analogues: see [FRS93, NV06, Rum07] and references therein. They are thus actively studied by knot theorists, who call them *biracks*, and use the word *biquandles* for biracks endowed with a bijection $t \colon X \to X$ satisfying

(1.1) $\forall x \in X, \qquad r(t(x), x) = (t(x), x).$

To illustrate certain concepts and proofs, we will use graphical calculus, providing a bare minimum of explanations. More details can be found, for instance, in [LV17]. The map r is presented as on Fig. 1.1. Our conditions on r mean that any two neighboring colors on its diagram uniquely determine the two remaining colors. The YBE translates as the topological Reidemeister III move. This graphical calculus provides a bridge towards knot theory.
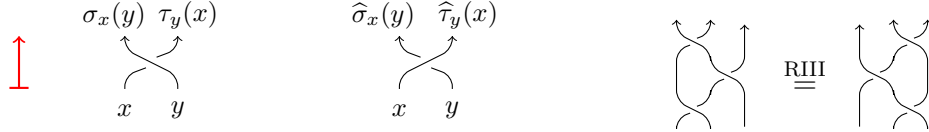

Figure 1.1. Crossings representing a solution, and the RIII move representing the YBE.

The category **YBESol** of solutions and solution morphisms is defined in the obvious way.

A (right) *rack* is a set X with a (right) self-distributive binary operation $\triangleleft$, in the sense of

$$(x \triangleleft y) \triangleleft z = (x \triangleleft z) \triangleleft (y \triangleleft z)$$

for all $x, y, z \in X$, such that the right translations

$$\rho_y \colon x \mapsto x \triangleleft y$$

are bijections $X \to X$ for all $y \in X$. A *quandle* is a rack satisfying $x \triangleleft x = x$ for all $x \in X$. A rack $(X, \triangleleft)$ yields two solutions: $\operatorname{Sol}(X, \triangleleft) = (X, r_\triangleleft)$ and $\operatorname{Sol}'(X, \triangleleft) = (X, r'_\triangleleft)$, with

$$r_\triangleleft(x, y) = (y, x \triangleleft y), \qquad\qquad r'_\triangleleft(x, y) = (y \triangleleft x, x),$$

called *SD solutions*. We mainly work with $r_\triangleleft$ here, the properties of $r'_\triangleleft$ being similar. An SD solution $(X, r_\triangleleft)$ is a biquandle if and only if $(X, \triangleleft)$ is a quandle, hence the

terminology. There are also symmetric notions of a *left rack* $(X, \triangleright)$, and *left SD solutions* $(X, r_\triangleright)$ and $(X, r'_\triangleright)$, with $r_\triangleright(x, y) = (x \triangleright y, x)$, $r'_\triangleright(x, y) = (y, y \triangleright x)$.

Involutive and SD solutions form the two best understood solution families. While involutive solutions are particularly interesting to algebraists, SD ones were, until recently, the realm of knot theorists. The structure rack construction recalled in Section 2 shows that these solutions also have an algebraic interest.

The *structure group* of a solution (X, r) is defined by generators and relations:

$$G_{(X,r)} = \langle X \mid xy = \sigma_x(y)\tau_y(x) \text{ for all } x, y \in X \rangle.$$

The structure group of a rack $(X, \triangleleft)$ is defined as the structure group of $(X, r_\triangleleft)$ or $(X, r'_\triangleleft)$, denoted by $G_{(X,\triangleleft)}$ or $G'_{(X,\triangleleft)}$ respectively. The map $x_1^{\varepsilon_1} \ldots x_s^{\varepsilon_s} \mapsto x_s^{\varepsilon_s} \ldots x_1^{\varepsilon_1}$, where $x_i \in X$, $\varepsilon_i = \pm 1$, induces a group isomorphism $G^{op}_{(X,\triangleleft)} \cong G'_{(X,\triangleleft)}$.

A solution is called *injective* if the natural map

$$\iota \colon X \to G_{(X,r)},$$
$$x \mapsto x$$

is injective. All involutive solutions are injective (see Section 3). Conversely, many properties of involutive solutions generalize to injective ones. A simple example of a non-injective solution is $(\mathbb{Z}, r_\triangleleft)$, where $\mathbb{Z}$ is considered as a rack, with $x \triangleleft y = x + 1$ for all $x, y \in \mathbb{Z}$. Indeed, from $r_\triangleleft(x, x) = (x, x + 1)$ one deduces $G_{(\mathbb{Z},\triangleleft)} \cong (\mathbb{Z}, +)$, and the map $\iota \colon \mathbb{Z} \to \mathbb{Z}$ sends all $x \in \mathbb{Z}$ to 1. A rack $(X, \triangleleft)$ is called *injective* if the corresponding solution $(X, r_\triangleleft)$ (or, equivalently, $(X, r'_\triangleleft)$) is such.

If (X, r) is a solution, then so is (X, r^{-1}). The YBE for r and r^{-1} implies

$$(1.2) \qquad \tau_y \tau_x = \tau_{\tau_y(x)}\tau_{\sigma_x(y)}, \qquad\qquad \widehat{\tau}_y \widehat{\tau}_x = \widehat{\tau}_{\tau_y(x)}\widehat{\tau}_{\sigma_x(y)},$$

$$(1.3) \qquad \sigma_x \sigma_y = \sigma_{\sigma_x(y)}\sigma_{\tau_y(x)}, \qquad\qquad \widehat{\sigma}_x \widehat{\sigma}_y = \widehat{\sigma}_{\sigma_x(y)}\widehat{\sigma}_{\tau_y(x)}$$

for all $x, y \in X$. As a consequence, τ and $\widehat{\tau}$ induce right actions of $G_{(X,r)}$ on X, and σ and $\widehat{\sigma}$ induce left actions.

We will prove results on structure groups of racks and solutions while working mostly with (bi)quandles. The following construction makes it possible.

Proposition 1.1. *For a solution (X, r), consider the smallest equivalence relation $\eqsim$ such that $x \eqsim \sigma_x(y)$ for all $x, y \in X$ satisfying $y = \tau_y(x)$. Then r induces a biquandle structure r' on $X/\eqsim$. Moreover, the quotient map $X \twoheadrightarrow X/\eqsim$ induces a group isomorphism*

$$G_{(X,r)} \xrightarrow{\sim} G_{(X/\eqsim,\, r')}.$$

Definition 1.2. The biquandle $(X/\eqsim, r')$ from the proposition is called the *induced biquandle* of (X, r), denoted by $\mathrm{BQ}(X, r)$.

The relation $\eqsim$ is best understood diagrammatically: one identifies x and x' whenever the coloring situation from Fig. 1.2 occurs.
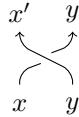

FIGURE 1.2. Identifying x with x' in all such situations, one shrinks a solution to its induced biquandle.

Proof. Take any $x, y \in X$ satisfying $y = \tau_y(x)$. Put $x' = \sigma_x(y)$. By Equations (1.2)–(1.3), one has $\tau_{x'} = \tau_x$ and $\sigma_{x'} = \sigma_x$, implying

$$r(x, z) = (\sigma_x(z), \tau_z(x)), \qquad\qquad r(z, x) = (\sigma_z(x), \tau_x(z)),$$
$$r(x', z) = (\sigma_x(z), \tau_z(x')), \qquad\qquad r(z, x') = (\sigma_z(x'), \tau_x(z))$$

for any $z \in X$. To show that r induces a map r' on $(X/\simeq)^{\times 2}$, it suffices to check the relations $\tau_z(x) \simeq \tau_z(x')$, $\sigma_z(x) \simeq \sigma_z(x')$. In other terms, one needs to verify that the right and left $G_{(X,r)}$-actions on X via τ and σ respect the relation $\simeq$.

Put $r(z, x') = (\sigma_z(x'), w)$, and $r(w, y) = (u, v)$; precise expressions of u, v, w in terms of x, y, z are not important here. All these notations are summarized in Fig. 1.3. Then

$$(\sigma_z(x'), u, v) = r_2 r_1 r_2(z, x, y) = r_1 r_2 r_1(z, x, y),$$

which means $r(z, x) = (\sigma_z(x), \tilde{w})$, $r(\tilde{w}, y) = (\tilde{u}, v)$, and $r(\sigma_z(x), \tilde{u}) = (\sigma_z(x'), u)$ for some $\tilde{u}, \tilde{w} \in X$. By the non-degeneracy of r, $r(w, y) = (u, v)$ and $r(\tilde{w}, y) = (\tilde{u}, v)$ imply $w = \tilde{w}, u = \tilde{u}$. But then $r(\sigma_z(x), u) = (\sigma_z(x'), u)$, hence $\sigma_z(x) \simeq \sigma_z(x')$. The proof of $\tau_z(x) \simeq \tau_z(x')$ is similar.
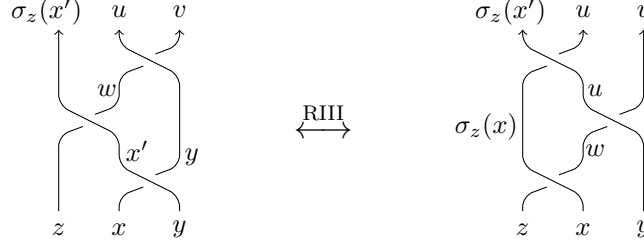

FIGURE 1.3. Relation $x \simeq x'$ implies $\sigma_z(x) \simeq \sigma_z(x')$ for all z.

The YBE and the surjectivity for r', as well as the surjectivity of its σ'- and τ'-components, follow from the corresponding properties for r. Since the set $X/\simeq$ is finite, surjectivity implies bijectivity. So, $(X/\simeq, r')$ is indeed a solution.

For any $y \in X$, the element $x = \tau_y^{-1}(y)$ satisfies $y = \tau_y(x)$. The definition of the relation $\simeq$ yields $r'(x, y) = (x, y)$; here we abusively use the same notation for elements from X and their images in $X/\simeq$. Since r' is non-degenerate, the map $y \mapsto \tau_y'^{-1}(y)$ has to be injective, hence bijective. So, $(X/\simeq, r')$ is a biquandle.

Finally, for all $x, y \in X$ satisfying $y = \tau_y(x)$, from $xy = \sigma_x(y)\tau_y(x)$ one deduces $x = \sigma_x(y)$ in $G_{(X,r)}$, so when passing to the quotient $X/\simeq$, one does not change the structure group. $\qquad\square$

Remark 1.3. Induced biquandles enjoy the following universal property: for any morphism $\phi\colon X \to Y$ of solutions, where Y is a biquandle, there is a unique morphism $\phi'\colon X/\simeq \to Y$ with $\phi = \phi'\pi$. Here π is the quotient map $X \twoheadrightarrow X/\simeq$.

Arguments from the proof of Proposition 1.1 imply the following elementary observation:

**Lemma 1.4.** *An injective solution is necessarily a biquandle.*

Our induced biquandle construction in fact defines a functor BQ: **YBESol** → **Biquandle**, which is a retraction for the inclusion functor **Biquandle** → **YBESol**. Indeed, if (X, r) is already a biquandle, then $\mathrm{BQ}(X, r) = (X, r)$.

For a solution $(X, r_\lhd)$ associated with a rack, the quotient $X/\eqsim$ simply identifies x with $x \lhd x$ for all $x \in X$. The operation $\lhd$ induces a quandle operation $\lhd'$ on $X/\eqsim$. The quandle $\mathrm{Q}(X, \lhd) = (X/\eqsim, \lhd')$ is the *induced quandle* of $(X, \lhd)$. It appeared in [Bri88, AG03]. At the level of solutions and structure groups, one has

$$\mathrm{BQ}(\mathrm{Sol}(X, \lhd)) \cong \mathrm{Sol}(\mathrm{Q}(X, \lhd)),$$

$$G_{(X,\lhd)} \cong G_{\mathrm{Q}(X,\lhd)}.$$

The functoriality of all our constructions yields the following result.

Proposition 1.5. *The following functors assemble into a commutative diagram:*
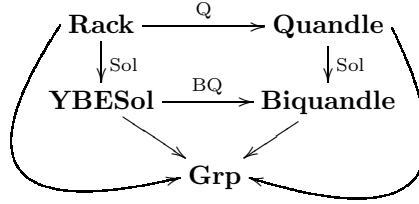
Here all unlabelled arrows correspond to the structure group functors.

2. STRUCTURE RACKS FOR YBE SOLUTIONS

We now describe retractions for the inclusion functors Sol above. As explained in [Sol00, LYZ00, LV17], to any solution (X, r) one can associate its (right) *structure rack* $\mathrm{R}(X, r) = (X, \lhd_r)$, where

$$x \lhd_r y = \tau_y \sigma_{\tau_x^{-1}(y)}(x) = \tau_y \widehat{\tau}_y^{-1}(x)$$

for all $x, y \in X$. Recall that $\widehat{\tau}$ is the right component of the map r^{-1}. In the literature, $\mathrm{R}(X, r)$ is also called the *associated* or *derived rack* of (X, r). It has a symmetric left version $(X, \rhd_r)$, which we will show to be isomorphic to $\mathrm{R}(X, r)$ (Proposition 2.8). The graphical definition of structure racks from Fig. 2.1 makes this construction more intuitive.

FIGURE 2.1. The colors x, y uniquely determine all colors in both diagrams; the upper right/left color defines the right/left structure rack of a solution.

The structure rack captures basic properties of the original solution:
- (X, r) is involutive $\iff$ $(X, \lhd_r)$ is trivial: $x \lhd_r y = x$ for all $x, y \in X$;
- (X, r) is a biquandle $\iff$ $(X, \lhd_r)$ is a quandle;
- the actions of the braid groups B_n on the tensor powers $X^{\times n}$ induced by r and by $\lhd_r$ are isomorphic (without the solutions (X, r) and $(X, r_{\lhd_r})$ being necessarily isomorphic).

The structure rack construction yields a functor R: **YBESol** → **Rack**, which is a left inverse of the functor Sol: **Rack** → **YBESol**. They restrict to functors R : **Biquandle** ⇄ **Quandle** : Sol, satisfying R ∘ Sol = Id$_{\textbf{Quandle}}$; we abusively use the same notation in both situations.

We next show that the two functors R intertwine the functors Q and BQ. Some technical results are first due:

Lemma 2.1. *Let (X, r) be a solution. Take $x, y \in X$. Then*

(1) $\tau_y(x) = y \iff \sigma_x(y) = x \rhd_r x$;

(2) $\sigma_x(y) = x \iff \tau_y(x) = y \lhd_r y$;

(3) $x \lhd_r x = x \rhd_r x$;

(4) *the map*

$$T \colon X \to X,$$

$$y \mapsto \tau_y^{-1}(y)$$

is bijective, with the inverse $T^{-1} \colon x \mapsto \sigma_x^{-1}(x \rhd_r x)$.

Proof.   (1) Suppose that $\tau_y(x) = y$, that is, $x = T(y)$. Then relations (1.3) imply $\widehat{\sigma}_x = \widehat{\sigma}_{\sigma_x(y)}$. So,

$$\widehat{\sigma}_x(y) = \widehat{\sigma}_{\sigma_x(y)}(y) = \widehat{\sigma}_{\sigma_x(y)}(\tau_y(x)) = x,$$

where we used that the map $(x, y) \mapsto (\widehat{\sigma}_x(y), \widehat{\tau}_y(x))$ is the inverse of $(x, y) \mapsto (\sigma_x(y), \tau_y(x))$. This yields $\sigma_x(y) = x \rhd_r x$, as shown in Fig. 2.2.

Since r is non-degenerate, the composition $y \mapsto (y, y) \mapsto (x, x \rhd_r x)$, where $x = T(y)$, is injective. Then the map T is also injective, hence bijective, since X is finite. Now, take any $x, y \in X$ with $\sigma_x(y) = x \rhd_r x$. We have just seen that there exists a unique y' with $r(x, y') = (x \rhd_r x, y')$. Then $\sigma_x(y') = x \rhd_r x = \sigma_x(y)$, hence $y = y'$, and $\tau_y(x) = y$.

FIGURE 2.2. Left: $\tau_y(x) = y$ implies $\sigma_x(y) = x \rhd_r x$. Right: $\sigma_x(y) = x$ implies $\tau_y(x) = y \lhd_r y$.

(2) is proved similarly.

(3) In 1, we saw that $\forall x \in X, \exists! y \in X$ satisfying $r(x, y) = (x \rhd_r x, y)$. Put $z = \tau_{x \rhd_r x}^{-1}(x)$. By the YBE, one has

$$r_2 r_2 r_1 r_2(z, x, y) = r_2 r_1 r_2 r_1(z, x, y) = r_1 r_2 r_1 r_1(z, x, y).$$

Let us study the three expressions in more detail. First,

$(z, x, y) \overset{r_2}{\mapsto} (z, x \rhd_r x, y) \overset{r_1}{\mapsto} (u, x, y) \overset{r_2}{\mapsto} (u, x \rhd_r x, y) \overset{r_2}{\mapsto} (u, x \rhd_r x, y \lhd_r y)$,

where $u = \sigma_z(x \rhd_r x)$, and we used the consequence $\sigma_x = \sigma_{x \rhd_r x}$ of (1.3) to get $r(x \rhd_r x, y) = (x \rhd_r x, y \lhd_r y)$. Further, $r_1 r_2 r_1(z, x, y) = r_2 r_1 r_2(z, x, y) = (u, x \rhd_r x, y)$, so

$(z, x, y) \overset{r_1}{\mapsto} (v, x', y) \overset{r_2}{\mapsto} (v, w, y) \overset{r_1}{\mapsto} (u, x \rhd_r x, y) \overset{r_2}{\mapsto} (u, x \rhd_r x, y \lhd_r y)$

for certain $x', v, w \in X$. Since r is non-degenerate, $r(x', y) = (w, y)$ implies $x' = x$ and $w = x \triangleright_r x$. Finally,

$$(z, x, y) \overset{r_1}{\mapsto} (v, x, y) \overset{r_1}{\mapsto} (s, x \triangleleft_r x, y) \overset{r_2}{\mapsto} (s, t, y \triangleleft_r y) \overset{r_1}{\mapsto} (u, x \triangleright_r x, y \triangleleft_r y)$$

for certain $s, t \in X$. The key relation here is $r(x \triangleleft_r x, y) = (t, y \triangleleft_r y)$. Together with $r(x \triangleright_r x, y) = (x \triangleright_r x, y \triangleleft_r y)$ and the non-degeneracy of r, it implies $x \triangleleft_r x = x \triangleright_r x$, as desired.
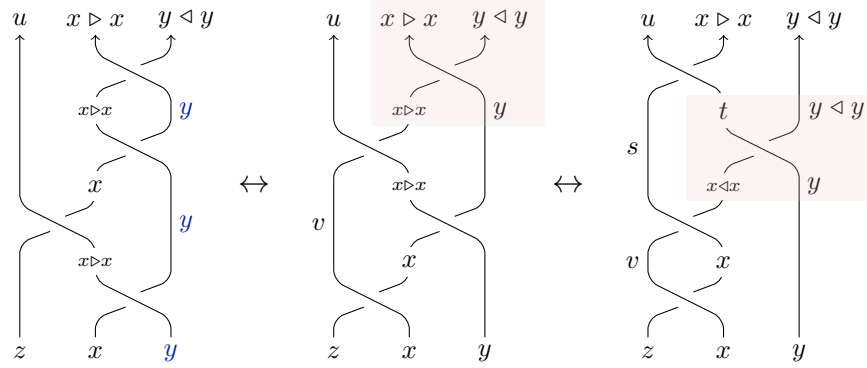
These computations are summarized in Fig. 2.3.

FIGURE 2.3. The three colors y, y, y in the left diagram uniquely determine all colors in all the diagrams. Comparing the two highlighted crossings, one obtains $x \triangleleft_r x = x \triangleright_r x$. Here $z = \tau_{x \triangleright_r x}^{-1}(x)$.

(4) follows from Point 1 and its proof. $\qquad\qquad\qquad\qquad\qquad$ □

Example 2.2. If (X, r) is a biquandle, then $T = t$, where the map t is defined by (1.1).

Example 2.3. Let $(X, \triangleleft)$ be a rack. Then for the solution $(X, r_\triangleleft)$, one has $T = \mathrm{Sq}^{-1}$, where the map Sq is defined in Lemma 2.4. For the solution $(X, r'_\triangleleft)$, the T-map is just Id_X.

Lemma 2.4. *Given a rack $(X, \triangleleft)$, consider the map $\mathrm{Sq} \colon X \to X$, $x \mapsto x \triangleleft x$. For any $x, y \in X$, one has:*
(1) $\mathrm{Sq}(x \triangleleft y) = \mathrm{Sq}(x) \triangleleft y$;
(2) $x \triangleleft \mathrm{Sq}(y) = x \triangleleft y$;
(3) the map Sq is bijective.

More properties of this map can be found in [AG03, Szy16].

Proof. (1) By self-distributivity, $(x \triangleleft y) \triangleleft (x \triangleleft y) = (x \triangleleft x) \triangleleft y$.
(2) Since the right translation $\bullet \mapsto \bullet \triangleleft y$ is bijective, there exists a unique $z \in X$ satisfying $z \triangleleft y = x$. Then

$$x \triangleleft (y \triangleleft y) = (z \triangleleft y) \triangleleft (y \triangleleft y) = (z \triangleleft y) \triangleleft y = x \triangleleft y.$$

(3) Again by the bijectivity of right translations, for any $x \in X$ there exists a unique $z \in X$ with $z \triangleleft x = x$. Then

$$\mathrm{Sq}(z) \triangleleft x = \mathrm{Sq}(z \triangleleft x) = \mathrm{Sq}(x) = x \triangleleft x,$$

implying $\mathrm{Sq}(z) = x$. So, the map Sq is surjective. Further, if $\mathrm{Sq}(z) = \mathrm{Sq}(z')$ for some $z, z' \in X$, then by the preceding point, for all $u \in X$ one has

$$u \lhd z = u \lhd \mathrm{Sq}(z) = u \lhd \mathrm{Sq}(z') = u \lhd z',$$

implying $z \lhd z = z' \lhd z' = z' \lhd z$, hence $z = z'$.   □

Notation 2.5. Given a solution (X, r), we will write $\mathrm{Sq}(x) = x \lhd_r x = x \rhd_r x$.

From the two lemmas, one obtains the coloring pattern from Fig. 2.4.

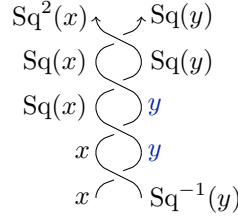FIGURE 2.4. This coloring pattern applies for any $y \in X$ and $x = T(y)$.

One also immediately deduces two important corollaries:

Proposition 2.6. *Let (X, r) be a solution. The equivalence relation $\simeq$ on X defined in Proposition 1.1 has the following alternative description:*

$$x \simeq y \qquad \Longleftrightarrow \qquad y = \mathrm{Sq}^m(x) \ \text{for some } m \in \mathbb{Z}.$$

The second one is the promised compatibility relation between the functors R, Q, and BQ:

Proposition 2.7. *The following functors assemble into a commutative diagram:*

In contrast to the induced (bi)quandle functor, the structure rack functor does not yield isomorphisms at the structure group level. Instead, it gives bijective group 1-cocycles, as we will see in the next section.

We finish this section with a comparison of right and left structure racks. It is not used in what follows, but makes our structure rack story more coherent.

Proposition 2.8. *The right and the left structure racks of a solution (X, r) are isomorphic. Concretely, the relation*

(2.1) $$T(y \rhd_r x) = T(x) \lhd_r T(y)$$

holds for all $x, y \in X$. Here T is the bijection $y \mapsto \tau_y^{-1}(y)$ from Lemma 2.1.

The relation $x \lhd_r x = x \rhd_r x$ from Lemma 2.1 is in fact a consequence of this proposition.

Proof. Recall that the structure rack operations can be written as

$$x \lhd_r y = \tau_y \sigma_{\tau_x^{-1}(y)}(x) = \tau_y \widehat{\tau}_y^{-1}(x), \qquad y \rhd_r x = \sigma_y \tau_{\sigma_x^{-1}(y)}(x) = \sigma_y \widehat{\sigma}_y^{-1}(x).$$

We will also use two properties of the map τ_y:

- it is an automorphism of the rack $(X, \vartriangleleft_r)$ (Lemma 3.3);
- it induces a right action of $G_{(X,r)}$ on X (relation (1.2))

With this in mind, the two sides of (2.1) rewrite as

$$T(y \vartriangleright_r x) = T\sigma_y \widehat{\sigma}_y^{-1}(x),$$

$$T(x) \vartriangleleft_r T(y) = \tau_y^{-1}(\tau_y T(x) \vartriangleleft_r \tau_y T(y)) = \tau_y^{-1}(\tau_y T(x) \vartriangleleft_r y) = \tau_y^{-1}\tau_y \widehat{\tau}_y^{-1}\tau_y T(x)$$
$$= \widehat{\tau}_y^{-1}\tau_y T(x).$$

It remains to check the relation

$$T\sigma_y \widehat{\sigma}_y^{-1} = \widehat{\tau}_y^{-1}\tau_y T$$

in $\mathrm{Sym}(X)$. We split it into two parts:

$$T\sigma_y = \widehat{\tau}_y^{-1}T, \qquad\qquad T\widehat{\sigma}_y = \tau_y^{-1}T.$$

They are verified as follows:

$$T\sigma_y(x) = \tau_{\sigma_y(x)}^{-1}\sigma_y(x) = \tau_{\sigma_y(x)}^{-1}\tau_{\tau_x(y)}^{-1}\tau_{\tau_x(y)}\sigma_y(x)$$
$$= \tau_y^{-1}\tau_x^{-1}(x \vartriangleleft_r \tau_x(y)) = \tau_y^{-1}(T(x) \vartriangleleft_r y) = \widehat{\tau}_y^{-1}T(x);$$

$$T\widehat{\sigma}_y(x) = \tau_{\widehat{\sigma}_y(x)}^{-1}\widehat{\sigma}_y(x) = \tau_{\widehat{\sigma}_y(x)}^{-1}\tau_{\widehat{\tau}_x(y)}^{-1}\tau_{\widehat{\tau}_x(y)}\widehat{\sigma}_y(x)$$
$$= \tau_y^{-1}\tau_x^{-1}\tau_{\widehat{\tau}_x(y)}\widehat{\sigma}_y(x) = \tau_y^{-1}\tau_x^{-1}(x) = \tau_y^{-1}T(x).$$

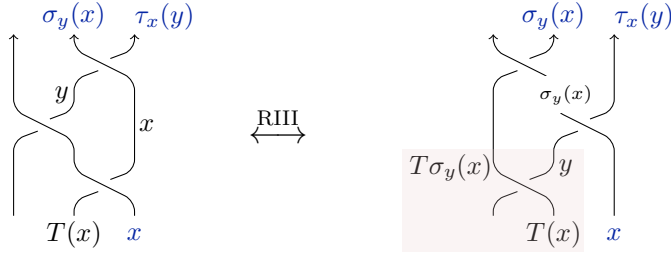For a more enlightening graphical proof, see Figs 2.5 and 2.6.   □

FIGURE 2.5. At the highlighted crossing, one gets $\widehat{\tau}_y T\sigma_y = T$. Here the two rightmost top colors and the rightmost bottom color uniquely determine the remaining ones for both diagrams.
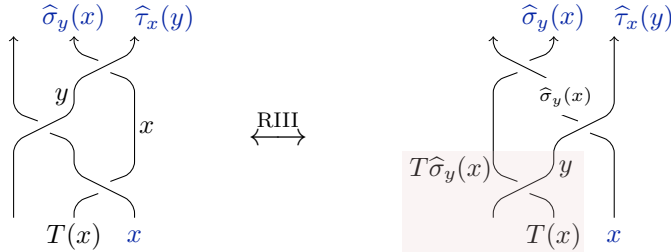

FIGURE 2.6. At the highlighted crossing, one gets $\tau_y T\widehat{\sigma}_y = T$.

3. Bijective 1-cocycles

In this section we prove a technical lemma on passing to quotients in bijective 1-cocycles. We illustrate it with the example of the structure group $G_{(X,r)}$ of a solution (X, r), and the structure group $G_{(X, \triangleleft_r)}$ of its structure rack $(X, \triangleleft_r)$. This lemma is instrumental for constructing a nice finite quotient of $G_{(X,r)}$ in Section 5.

Let a group G act on a group H on the right by group automorphisms. That is, the following conditions hold for all $g_i \in G, h_i \in H$:

$$h^{g_1 g_2} = (h^{g_1})^{g_2}, \qquad\qquad\qquad h^1 = h,$$
$$(h_1 h_2)^g = h_1^g h_2^g, \qquad\qquad\qquad 1^g = 1.$$

A *group 1-cocycle* is a map $\varphi \colon G \to H$ satisfying

$$\varphi(g_1 g_2) = \varphi(g_1)^{g_2} \, \varphi(g_2)$$

for all $g_i \in G$. It can be seen as a twisted group morphism.

The definitions of monoid/semigroup actions and 1-cocycles repeat verbatim the above definitions. Note that we consider only actions by monoid/semigroup automorphisms, i.e., the maps $h \mapsto h^g$ are all bijective.

We are particularly interested in bijective 1-cocycles and their quotients.

Lemma 3.1. *Let* $\varphi \colon G \to H$ *be a bijective (semi-)group/monoid 1-cocycle. Let*

$$\mathcal{R}_G = \{\, g_i = g_i' \,|\, i \in I \,\}, \qquad\qquad \mathcal{R}_H = \{\, \varphi(g_i) = \varphi(g_i') \,|\, i \in I \,\}$$

be a set of relations we would like to impose on G, and its image in H respectively. Thus, $g_i, g_i' \in G$ for all i. Assume that
 (1) $h^{g_i} = h^{g_i'}$ for all $h \in H$ and $i \in I$;
 (2) $\mathcal{R}_H = \{\, \varphi(g_i)^g = \varphi(g_i')^g \,|\, i \in I \,\}$ for all $g \in G$.
Then the G-action on H induces a $G/\mathcal{R}_G$-action on $H/\mathcal{R}_H$, and φ induces a bijective (semi-)group/monoid 1-cocycle $\overline{\varphi} \colon G/\mathcal{R}_G \to H/\mathcal{R}_H$ with respect to this induced action.

Proof. Condition 1 is precisely what is needed to get a $G/\mathcal{R}_G$-action on H, and condition 2 allows one to descend to $H/\mathcal{R}_H$. The cocycle condition for $\overline{\varphi}$ follows from that for φ. It remains to check the bijectivity. Passing to the quotient $G/\mathcal{R}_G$ means identifying $xg_i y$ with $xg_i' y$ for all $x, y \in G$, $i \in I$. The 1-cocycle φ sends these pairs to $\varphi(x)^{g_i y} \varphi(g_i)^y \varphi(y)$ and $\varphi(x)^{g_i y} \varphi(g_i')^y \varphi(y)$. Since φ is bijective and G acts on H by bijections, and because of condition 2, one gets precisely all pairs $z\varphi(g_j)v$ and $z\varphi(g_j')v$ for all $z, v \in H$, $j \in I$. So, the induced cocycle $\overline{\varphi}$ is bijective. $\square$

Remark 3.2. Lemma 3.1 has a symmetric version for left actions and the corresponding notion of 1-cocycles. Left actions are denoted by ${}^g h$ and $g \rightharpoonup h$ here.

As an example, take a YBE solution (X, r), and put $G = H = SG_X$, the free semigroup on X. This semigroup acts on itself by $x^y = \tau_y(x)$, extended to a semigroup action by semigroup morphisms in the obvious way. This action is by bijections, since all τ_y are bijective. By the freeness, there exists a unique semigroup 1-cocycle $\varphi \colon SG_X \to SG_X$ with $\varphi(x) = x$ for all $x \in X$. It is clearly bijective. Put

$$\mathcal{R}_G = \{\, xy = \sigma_x(y)\tau_y(x) \,|\, x, y \in X \,\}.$$

Then $\varphi(xy) = x^y\, y = \tau_y(x)y$, and $\varphi(\sigma_x(y)\tau_y(x)) = \sigma_x(y)^{\tau_y(x)}\,\tau_y(x) = (y \triangleleft_r \tau_y(x))\,\tau_y(x)$. Since τ_y is bijective,

$$\mathcal{R}_H = \{\, xy = (y \triangleleft_r x)\, x \mid x, y \in X \,\}.$$

For these data, condition 1 from Lemma 3.1 follows from 1.2, and condition 2 from the following property.

Lemma 3.3. *Let (X, r) be a solution. For all $z \in X$, both τ_z, and $\widehat{\tau}_z$ are rack automorphisms of $(X, \triangleleft_r)$: for all $x, y \in X$, one has*

$$\tau_z(x \triangleleft_r y) = \tau_z(x) \triangleleft_r \tau_z(y), \qquad\qquad \widehat{\tau}_z(x \triangleleft_r y) = \widehat{\tau}_z(x) \triangleleft_r \widehat{\tau}_z(y).$$

Proof. For τ_z, the argument is similar to that from the last part of Lemma 2.1. In Fig. 3.1, we give its graphical version. The proof for $\widehat{\tau}_z$ in analogous. Graphically, it suffices to turn the diagrams from Fig. 3.1 upside down. $\square$
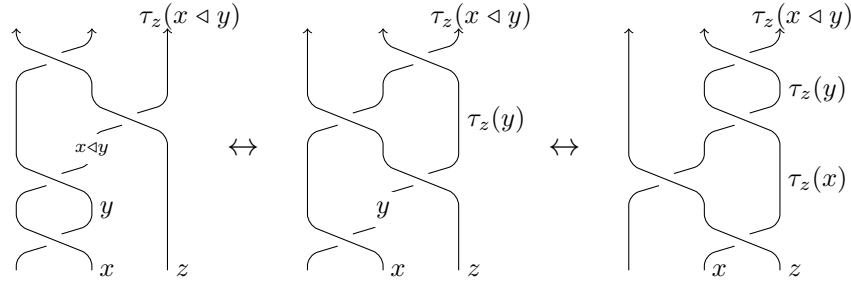

FIGURE 3.1. The three colors x, y, z in the left diagram uniquely determine all colors in all the diagrams. From the rightmost diagram, one gets $\tau_z(x \triangleleft_r y) = \tau_z(x) \triangleleft_r \tau_z(y)$.

Our arguments work for monoids instead of semigroups; in this case one necessarily has $\varphi(1) = 1$. Lemma 3.1 then yields bijective semigroup/monoid 1-cocycles

$$\varphi_{SG}\colon SG_{(X,r)} \to SG'_{(X,\triangleleft_r)}, \qquad\qquad \varphi_{Mon}\colon Mon_{(X,r)} \to Mon'_{(X,\triangleleft_r)},$$

where *structure semigroups/monoids* of solutions or racks are defined by the same generators and relations as structure groups.

Next, let (X, r) be a biquandle, and consider the *double* $D(X)$ of the set X, consisting of the elements $x = x^{+1}$ and x^{-1}, $x \in X$. This time, choose $G = H = Mon_{D(X)}$, the free monoid on $D(X)$. This monoid acts on itself by

$$(3.1) \qquad x^{\varepsilon_x} \leftharpoonup y^{\varepsilon_y} = \tau_y^{\varepsilon_y}(x)^{\varepsilon_x}, \qquad\qquad x, y \in X,\ \varepsilon_x, \varepsilon_y \in \{\pm 1\},$$

extended to a monoid action by monoid morphisms in the obvious way. Together with the personalized notation $\leftharpoonup$, we use the subscript notation x^y for this or any other action, when it does not create ambiguity. This action is again by bijections. By the freeness, there exists a unique monoid 1-cocycle $\varphi\colon Mon_{D(X)} \to Mon_{D(X)}$ with $\varphi(1) = 1$, $\varphi(x) = x$, and $\varphi(x^{-1}) = t(x)^{-1}$ for all $x \in X$; see (1.1) for the map t. This cocycle is bijective, since so is the map t. Put

$$\mathcal{R}_G = \{\, xy = \sigma_x(y)\tau_y(x) \mid x, y \in X \,\} \sqcup \{\, xx^{-1} = x^{-1}x = 1 \mid x \in X \,\}.$$

Then $\varphi(xx^{-1}) = x^{x^{-1}}t(x)^{-1} = \tau_x^{-1}(x)t(x)^{-1} = t(x)t(x)^{-1}$, since $\tau_x(t(x)) = x$ due to (1.1). Similarly, $\varphi(x^{-1}x) = (t(x)^{-1})^x x = \tau_x(t(x))^{-1}x = x^{-1}x$. Since t is bijective, one concludes

$$\mathcal{R}_H = \{\, xy = (y \triangleleft_r x)\, x \mid x, y \in X \,\} \sqcup \{\, xx^{-1} = x^{-1}x = 1 \mid x \in X \,\}.$$

For relations of the first type (braid type), conditions from Lemma 3.1 hold for the same reasons as before. For relations of the second type (group type), they follow from definition (3.1). Lemma 3.1 then yields a 1-cocycles for quotients:

Theorem 3.4. *Let (X, r) be a solution. There exists a unique bijective group 1-cocycle $J\colon G_{(X,r)} \to G'_{(X,\triangleleft_r)}$ such that the following diagram commutes:*

$$
\begin{array}{ccc}
 & X & \\
\iota \swarrow & & \searrow \iota \\
G_{(X,r)} \xrightarrow{\quad J \quad} & & G'_{(X,\triangleleft_r)}.
\end{array}
$$

Here

- *$G_{(X,r)}$ and $G'_{(X,\triangleleft_r)}$ are the structure groups of (X, r) and of its structure rack $(X, \triangleleft'_r)$ respectively;*
- *$G_{(X,r)}$ acts on $G'_{(X,\triangleleft_r)}$ on the right by group automorphisms extending (3.1);*
- *the two maps ι are defined by $\iota(x) = x$ for all $x \in X$.*

Proof. If (X, r) is a biquandle, then the argument preceding the theorem yields a bijective group 1-cocycle $J = \overline{\varphi}\colon G_{(X,r)} \to G'_{(X,\triangleleft_r)}$, with $\overline{\varphi}(x) = x$ for all $x \in X$ by construction. This cocycle is unique, since a group 1-cocycle is uniquely determined by its values on the generators. If (X, r) is a general solution, one can replace it with its induced biquandle using Propositions 1.5 and 2.7. Alternatively, one can work directly with non-biquandle solutions, replacing the map t with the map T from Lemma 2.1. $\square$

This result appears in a weaker form and/or with a much more involved proof in [Sol00, LYZ00, LV17]. The map J is called the *J map*, or the *guitar map* there.

For involutive r, $G'_{(X,\triangleleft_r)}$ is the free abelian group on X, and the diagram from the theorem yields the injectivity of r, its powerful characterization in group-theoretic terms [ESS99], and an I-structure on $G_{(X,r)}$ [GIVdB98]. In the general case, the situation is much more delicate.

We finish this section with a graphical way of computing $\varphi(x_1 \ldots x_m) = x'_1 \ldots x'_m$ for $x_i \in X$, presented in Fig. 3.2. The 1-cocycle condition for φ yields $x'_i = x_i^{x_{i-1}\ldots x_1} = \tau_{x_1}\cdots\tau_{x_{i-1}}(x_i)$.
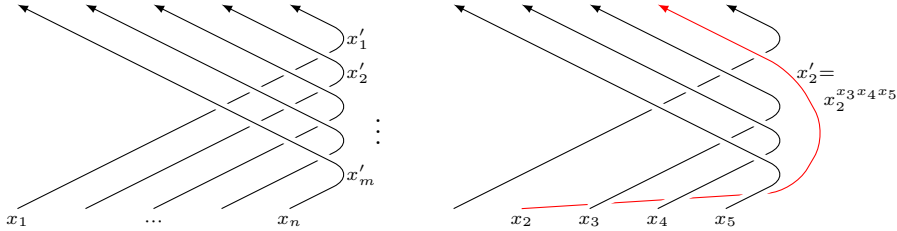

FIGURE 3.2. The guitar map J.

Remark 3.5. Bijective group 1-cocycles have many alternative descriptions: as braided commutative groups, as skew braces, as a skew version of linear cycle sets, as certain factorized groups [LYZ00, GIM08, GV17, SV17]. The results of this section can be translated into any of these languages.

4. Finite quotients for structure groups of racks

We now describe finite quotients of structure groups of racks which preserve injectivity (that is, the injectivity of the map $\iota\colon X \to G_{(X,\triangleleft)}$).

Notation 4.1. Let $(X, \triangleleft)$ be a finite rack. Denote by

$$K_\triangleleft = \#\operatorname{Orb}(X, \triangleleft)$$

the number of its orbits with respect to the actions $\rho_y\colon x \mapsto x \triangleleft y$. Further, for $y \in X$, denote by D_y the minimal integer D satisfying

$$D \geq 2 \qquad \text{and} \qquad \rho_y^D = \operatorname{Id}_X.$$

Theorem 4.2. *Let $(X, \triangleleft)$ be a finite rack. The powers x^{D_x}, $x \in X$, generate a central subgroup $Z_{(X,\triangleleft)}$ of the structure group $G_{(X,\triangleleft)}$. This subgroup is free abelian of rank $K_\triangleleft$. The quotient*

$$\overline{G}_{(X,\triangleleft)} = G_{(X,\triangleleft)}/Z_{(X,\triangleleft)}$$

is finite. Finally, the map $\iota\colon X \to G_{(X,\triangleleft)}$ is injective if and only if it remains so when composed with the quotient map $G_{(X,\triangleleft)} \twoheadrightarrow \overline{G}_{(X,\triangleleft)}$.

The last property from the theorem is called the *injectivity preservation* for $\overline{G}$.
In the 1-orbit case, these finite quotients were described in [GHV11].

Proof. Since $\rho_{x \triangleleft y} = \rho_y^{-1}\rho_x\rho_y$ for all $x, y \in X$, one has $D_x = D_z$ for all x, z from the same orbit of X. Further, relations

$$xy^n = y^n\rho_y^n(x), \qquad\qquad x^n y = y(x \triangleleft y)^n$$

in $G_{(X,\triangleleft)}$ imply that the powers y^{D_y} are central in $G_{(X,\triangleleft)}$, and that

$$x^{D_x} = (x \triangleleft y)^{D_x} = (x \triangleleft y)^{D_{x \triangleleft y}} \quad \text{for all } x, y \in X.$$

Thus, $x^{D_x} = z^{D_z}$ for all x, z from the same orbit. Let $\mathcal{O}_1, \ldots, \mathcal{O}_k$, where $k = K_\triangleleft$, be the orbits of $(X, \triangleleft)$, let $x_1, \ldots, x_k$ be their representatives, and put $D_i = D_{x_i}$. Consider the group morphism

$$\theta\colon G_{(X,\triangleleft)} \to \oplus_i \mathbb{Z}\mathcal{O}_i \cong \mathbb{Z}^k,$$
$$x \mapsto \mathcal{O}(x),$$

where $\mathcal{O}(x)$ is the orbit of x. This map is clearly well defined and surjective. The powers $x_i^{D_i}$ are sent to linearly independent elements $\mathcal{O}_i^{D_i}$ of $\oplus_i \mathbb{Z}\mathcal{O}_i$. Therefore the abelian group $Z_{(X,\triangleleft)}$ is free abelian of rank k, with generators $x_1^{D_1}, \ldots, x_k^{D_k}$.

To prove the finiteness of the quotient $\overline{G}_{(X,\triangleleft)}$, we will show that any of its elements can be represented by a word from $G_{(X,\triangleleft)}$ with at most $2n(d-1)$ letters $x^{\pm 1}$, $x \in X$, where $n = \#X$, and d is the maximum of the D_x. Indeed, a word with more than $2n(d-1)$ letters contains one of the $2n$ letters $x^{\pm 1}$ at least d times. The relation $yx = x(y \triangleleft x)$ allows one to pull all occurrences of this letter to the left; the remaining letters might change, but not their number. Since $d \geq D_x$, one can replace $(x^{\pm 1})^d$ with $(x^{\pm 1})^{d - D_x}$ to get a shorter representative of the same word.

Finally, assume that the map $\iota\colon X \to G_{(X,\lhd)}$ is injective, but its composition with $G_{(X,\lhd)} \to \overline{G}_{(X,\lhd)}$ is not. It means that there exist $x \neq z$ in X with

$$xz^{-1} = (x_1^{D_1})^{\alpha_1} \cdots (x_k^{D_k})^{\alpha_k} \in G_{(X,\lhd)}$$

for some $\alpha_i \in \mathbb{Z}$. Applying the above map θ to both sides, one gets $\mathcal{O}(x) - \mathcal{O}(z) = \sum_i D_i \alpha_i \mathcal{O}_i$. Since the $\mathcal{O}_i$ form a basis of $\oplus_i \mathbb{Z}\mathcal{O}_i$, and since $D_i \geq 2$ for all i, this implies $D_i \alpha_i = 0$ and thus $\alpha_i = 0$ for all i. But then $xz^{-1} = 1$ in $G_{(X,\lhd)}$, hence $\iota(x) = \iota(z)$, which is impossible for injective ι. $\hfill\square$

Imposing $D_x \geq 1$ instead of $D_x \geq 2$ would be more natural, and would make most of the assertions of the theorem still hold true. The only exception is the injectivity preservation. Indeed, for the trivial rack $x \lhd y = x$, $G_{(X,\lhd)}$ is the free abelian group on X, so $\iota\colon X \to G_{(X,\lhd)}$ is injective. Further, $\rho_x^1 = \mathrm{Id}_X$ for all x, and the powers $x^1 = x$ generate the whole $G_{(X,\lhd)}$, so the quotient $\overline{G}_{(X,r)}$ would be zero with this definition.

Remark 4.3. One can replace the groups $G_{(X,\lhd)}$ and $\overline{G}_{(X,\lhd)}$ in Theorem 4.2 with their symmetric versions $G'_{(X,\lhd)}$ and $\overline{G}'_{(X,\lhd)}$, constructed using the solution $r'_\lhd(x,y) = (y \lhd x, x)$ instead of $r_\lhd$. To see this, use the map $x_1^{\varepsilon_1} \ldots x_s^{\varepsilon_s} \mapsto x_s^{\varepsilon_s} \ldots x_1^{\varepsilon_1}$.

Observe that the map ι and its composition $\overline{\iota}$ with $G_{(X,\lhd)} \twoheadrightarrow \overline{G}_{(X,\lhd)}$ are rack morphisms, where both groups are seen as *conjugation quandles*, with $g \lhd_{Conj} h = h^{-1}gh$. Theorem 4.2 then yields a characterization of injective racks:

Corollary 4.4. *For a finite rack $(X, \lhd)$, the following conditions are equivalent:*
  (1) $(X, \lhd)$ is injective;
  (2) $(X, \lhd)$ is isomorphic to a sub-quandle of a finite conjugation quandle;
  (3) $(X, \lhd)$ is isomorphic to a sub-quandle of a conjugation quandle.

Proof. Theorem 4.2 yields $1 \Rightarrow 2$, and $2 \Rightarrow 3$ is trivial. Recall the universal property of the structure group $G_{(X,\lhd)}$: for any group H and any rack map $\phi\colon (X, \lhd) \to (H, \lhd_{Conj})$, there is a unique group map $\phi^*\colon G_{(X,\lhd)} \to (H, \lhd_{Conj})$ satisfying $\phi = \phi^*\iota$:

$$
\begin{array}{ccc}
X & \xrightarrow{\ \iota\ } & G_{(X,\lhd)} \\
 & \searrow^{\phi} & \big\downarrow{\scriptstyle \exists!\phi^*} \\
 & & H
\end{array}
$$

Now, if ϕ is injective, then so is ι. Hence $3 \Rightarrow 1$. $\hfill\square$

The injectivity question for a rack is not at all obvious, as can be seen in the examples below. In the second one, the finite quotient was crucial to establish injectivity.

Example 4.5. Let $X = \{1, 2, \ldots, 8\}$ be the quandle given by

$$\rho_1 = (376)(485), \quad \rho_2 = (376)(485), \quad \rho_3 = (168)(257), \quad \rho_4 = (168)(257),$$
$$\rho_5 = (174)(283), \quad \rho_6 = (174)(283), \quad \rho_7 = (135)(246), \quad \rho_8 = (135)(246).$$

In $G'_{(X,\lhd)}$, one has $x_1 x_3 = x_7 x_1 = x_3 x_7 = x_2 x_3$, hence $x_1 = x_2$. Thus X is not injective.

Example 4.6. Let $X = \{1,2,3,4,5,6,7,8,9,a,b,c\}$ be the quandle given by

$$\rho_1 = (34)(59)(6a)(7c)(8b), \qquad \rho_2 = (34)(59)(6a)(7c)(8b),$$
$$\rho_3 = (12)(5b)(6c)(7a)(89), \qquad \rho_4 = (12)(5b)(6c)(7a)(89),$$
$$\rho_5 = (19)(2a)(3c)(4b)(78), \qquad \rho_6 = (19)(2a)(3c)(4b)(78),$$
$$\rho_7 = (1c)(2b)(39)(4a)(56), \qquad \rho_8 = (1c)(2b)(39)(4a)(56),$$
$$\rho_9 = (15)(26)(38)(47)(bc), \qquad \rho_a = (15)(26)(38)(47)(bc),$$
$$\rho_b = (17)(28)(36)(45)(9a), \qquad \rho_c = (17)(28)(36)(45)(9a).$$

Computer calculations show that $\overline{G}'_{(X,\lhd)} \simeq \mathbf{GL}(2,3)$, and X embeds into this finite group. More precisely, $(X,\lhd)$ is isomorphic to the sub-quandle of $\mathbf{GL}(2,3)$ consisting of the conjugates of $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. This rack is retractable (see Definition 7.5).

5. Finite quotients for structure groups of YBE solutions

We next turn to finite quotients of the structure group of a solution (X,r).

Notation 5.1. Let (X,r) be a YBE solution. Denote by

$$K_r = K_{\lhd_r} = \#\operatorname{Orb}(X, \lhd_r)$$

the number of orbits of its structure rack. Further, for $y \in X$ and $d \in \mathbb{N}$, put

$$y^{[d]} = J^{-1}(y^d) \in G_{(X,r)}.$$

Here J is the bijective group 1-cocycle $J\colon G_{(X,r)} \to G'_{(X,\lhd_r)}$ from Theorem 3.4, with respect to the action $\leftharpoonup$ of $G_{(X,r)}$ on $G'_{(X,\lhd_r)}$ defined by (3.1).

Lemma 5.2. *For any $y \in X$ and $d \in \mathbb{N}$, one has*

(5.1) $$y^{[d]} = T^{d-1}(y) \dots T(y)y,$$

where the map $T\colon X \to X$ sends x to $\tau_x^{-1}(x)$.

Formula (5.1) explains the name *T-twisted powers of y* we will give to the $y^{[d]}$.

Proof. By definition of the map T, one has $T(x)^x = \tau_x T(x) = x$ for all x. So, for all $m \in \mathbb{N}$,

$$T^m(y)^{T^{m-1}(y)\dots T(y)y} = (T^m(y)^{T^{m-1}(y)})^{T^{m-2}(y)\dots T(y)y} = T^{m-1}(y)^{T^{m-2}(y)\dots T(y)y},$$

which, after several iterations, yields y. Using this and the 1-cocycle property for J, one gets $J(T^{d-1}(y)\dots T(y)y) = y^d$, so $y^{[d]} = J^{-1}(y^d) = T^{d-1}(y)\dots T(y)y$. $\qquad\square$

Notation 5.3. By (1.2)–(1.3), the group $G_{(X,r)}$ acts on the set X in several ways. We will denote these actions as follows:

$$x \leftharpoonup y = x^y = \tau_y(x), \qquad y \rightharpoonup x = {}^y x = \sigma_y(x),$$
$$x \overset{\frown}{\leftharpoonup} y = \widehat{\tau}_y(x), \qquad y \overset{\frown}{\rightharpoonup} x = \widehat{\sigma}_y(x)$$

for all $x,y \in X$. The superscript notation will be used only when it cannot be mistaken for the analogous notation for the $G_{(X,r)}$-action on $G'_{(X,\lhd_r)}$.

Lemma 5.4. *Let (X,r) be a solution. For any $y \in X$ there exists a $d \in \mathbb{N}$ such that $x \leftharpoonup y^{[m]} = y^{[m]} \rightharpoonup x = x$ for all $x \in X$ and all $m \in \mathbb{N}$ divisible by d.*

Proof. By Lemma 2.1, T is a bijection. Since X is finite, $T^p = \mathrm{Id}_X$ for some $p \in \mathbb{N}$. The map $\psi(x) = x \leftharpoonup y^{[p]}$ is a bijection on X as well, so $\psi^q = \mathrm{Id}_X$ for some $q \in \mathbb{N}$. From (5.1), one deduces $y^{[pm]} = (y^{[p]})^m$ for all $m \in \mathbb{N}$, hence $x \leftharpoonup y^{[pqs]} = \psi^{qs}(x) = x$ for all $x \in X$, $s \in \mathbb{N}$. A similar argument yields a $q' \in \mathbb{N}$ with $y^{[pq's]} \rightharpoonup x = x$ for all $x \in X$, $s \in \mathbb{N}$. Then $d = p(q \vee q')$, where $\vee$ stands for the least common multiple, satisfies our requirements. $\qquad\square$

Lemma 5.4 justifies the following definition.

Definition 5.5. Let (X, r) be a solution, and $y \in X$. The *degree* d_y of y is the minimal integer d satisfying the following conditions:
  (1) d is even if $\rho_y = \mathrm{Id}_X$ for the map $\rho_y \colon x \mapsto x \vartriangleleft_r y$;
  (2) $\rho_y^d = \mathrm{Id}_X$;
  (3) $x \leftharpoonup y^{[d]} = y^{[d]} \rightharpoonup x = x$ for all $x \in X$.

Everything is now ready for the main result of this section:

Theorem 5.6. *Let (X, r) be a solution. The powers $x^{[d_x]}$, $x \in X$, generate a normal subgroup $Z_{(X,r)}$ of the structure group $G_{(X,r)}$. This subgroup is free abelian of rank K_r. The quotient*

$$\overline{G}_{(X,r)} = G_{(X,r)}/Z_{(X,r)}$$

is finite. Finally, the map $\iota \colon X \to G_{(X,r)}$ is injective if and only if it remains so when composed with the quotient map $G_{(X,r)} \to \overline{G}_{(X,r)}$.

The theorem gives us the following short exact sequence:

$$0 \to \mathbb{Z}^{K_r} \to G_{(X,r)} \to \overline{G}_{(X,r)} \to 0.$$

The proof combines finite quotients of the structure group $G'_{(X,\vartriangleleft_r)}$ of the structure rack of our solution (Theorem 4.2 and Remark 4.3); the bijective cocycle J as a means of transport between $G_{(X,r)}$ and $G'_{(X,\vartriangleleft_r)}$ (Theorem 3.4 and Lemma 3.1); and a study of T-twisted powers, on which we now concentrate.

Our solution r extends from X to the (infinite) set $T(X) = \sqcup_{n \geq 0} X^{\times n}$ in the obvious way, as shown in Fig. 5.1. We keep the notation r for this extended solution, and σ and τ for its components.

$$\sigma_{\overline{a}}(\overline{b}) \in X^{\times m} \qquad\qquad \tau_{\overline{b}}(\overline{a}) \in X^{\times n}$$

$$\overline{a} \in X^{\times n} \qquad\qquad \overline{b} \in X^{\times m}$$
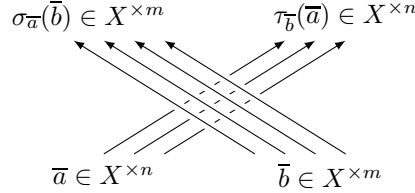
FIGURE 5.1. Solution on X extended to $T(X)$.

Lemma 5.7. *For any $y, z \in X$ and $m \in \mathbb{N}$, one has*

$$r(y^{[m]}, z) = (y^{[m]} \rightharpoonup z, (y^z)^{[m]}), \qquad r(z, y^{[m]}) = (u^{[m]}, z \leftharpoonup y^{[m]}),$$

where $u = \widehat{\tau}_{z'}^{-1}(y)$, $z' = z \leftharpoonup y^{[m]}$, and $\widehat{\tau}$ is the right component of r^{-1}.

The first relations implies that the map $\Delta_m \colon X \to X^{\times m}$, $y \mapsto y^{[m]}$, is $G_{(X,r)}$-equivariant, where $G_{(X,r)}$ acts on the powers of X on the right by the (extension of the) τ component of r: $\tau_z(y^{[m]}) = \tau_z(y)^{[m]}$. The equivariance with respect to the left actions via σ does not hold in general.

Proof. Both statements follow by repeatedly applying the following property:

$$r(T(y)y, z) = ((T(y)y) \rightharpoonup z, T(y^z)y^z),$$
$$r(z, yT^{-1}(y)) = ({}^z y T^{-1}({}^z y), z \leftharpoonup (yT^{-1}(y))).$$

We'll prove the first property, the second one being similar. The extension of r works as follows:

$$r(T(y)y, z) = (\mathrm{Id}_X \times c) r_1 r_2(T(y), y, z) = ((T(y)y) \rightharpoonup z, vy^z)$$

for a certain $v \in X$. Here c is the concatenation map $X \times X \to X^{\times 2}$. It remains to show $v = T(y^z)$, that is, $v^{(y^z)} = y^z$. This is done as follows:

$$((T(y)y) \rightharpoonup z, {}^v(y^z), v^{(y^z)}) = r_2 r_1 r_2(T(y), y, z)$$
$$= r_1 r_2 r_1(T(y), y, z) = r_1 r_2(\bullet, y, z) = r_1(\bullet, {}^y z, y^z) = (\bullet, \bullet, y^z),$$

where the $\bullet$ replace irrelevant entries. □

Remark 5.8. Lemma 5.7 implies that the map

$$r^{[m]} : (x, y) \mapsto (T^{-(m-1)}(x^{[m]} \rightharpoonup T^{m-1}(y)), x \leftharpoonup y^{[m]})$$

defines a solution on X. Even better: it yields the *cabling functor*

$$\mathrm{Cab}_m \colon \mathbf{YBESol} \to \mathbf{YBESol}.$$

The name comes from its diagrammatic interpretation. By Lemma 5.4, the sequence of functors $(\mathrm{Cab}_m)_{m \geq 1}$ is periodic.

Definition 5.9. By *orbits* of a solution (X, r) we will mean orbits with respect to the actions $y \mapsto \tau_z(y)$ and $y \mapsto \sigma_z(y)$ for all $z \in X$.

This notion should be distinguished from the finer notion of orbits of the structure rack $(X, \lhd_r)$ of our solution. Thus, for involutive r, the structure rack is trivial, so all its orbits contain one element only, whereas the orbits of the solution itself can be much bigger.

Lemma 5.10. *The degrees of all elements from the same orbit of (X, r) coincide.*

Proof. It suffices to check that conditions (1)–(3) from Definition 5.5 do not change when y is replaced with $y \leftharpoonup z = \tau_z(y)$ or with $\widehat{\tau}_z^{-1}(y)$ for any z. Indeed, $r(z, y) = (\sigma_z(y), \tau_y(z))$ implies $\widehat{\tau}_{\tau_y(z)} \sigma_z(y) = y$, so in the definition of the orbits of (X, r), the actions σ_z can be replaced with $\widehat{\tau}_z^{-1}$.

For (1)–(2), the desired equivalence follows from Lemma 3.3. Condition (3) needs more work. Take any $y, z \in X$ and an $m \in \mathbb{N}$. Suppose that $x \leftharpoonup y^{[m]} = y^{[m]} \rightharpoonup x = x$ holds for all $x \in X$. It suffices to check the relations

$$x \leftharpoonup \tau_z(y)^{[m]} = \tau_z(y)^{[m]} \rightharpoonup x = x \leftharpoonup \widehat{\tau}_z^{-1}(y)^{[m]} = \widehat{\tau}_z^{-1}(y)^{[m]} \rightharpoonup x = x.$$

Indeed, checking the triviality of the actions of $\tau_z^{-1}(y)^{[m]}$ and $\widehat{\tau}_z(y)$ is not necessary, since $\tau_z^{-1} = \tau_z^p$ and $\widehat{\tau}_z = (\widehat{\tau}_z^{-1})^q$ for some $p, q \in \mathbb{N}$ due to the finiteness of X.

Lemma 5.7 yields the relation $y^{[m]} z = z \tau_z(y)^{[m]}$ in $G_{(X,r)}$. By assumption, $y^{[m]}$ acts trivially on X with respect to the two actions $\rightharpoonup$ and $\leftharpoonup$. Thus $\tau_z(y)^{[m]}$ acts

trivially as well. Similarly, Lemma 5.7 yields the relation $zy^{[m]} = \widehat{\tau}_z^{-1}(y)^{[m]}z$ in $G_{(X,r)}$. The triviality of the actions of $\widehat{\tau}_z^{-1}(y)^{[m]}$ follows. $\square$

Proof of Theorem 5.6. By Lemmas 5.7 and 5.10, the relation

$$x^{[d_x]}\, z = z\,\tau_z(x)^{[d_x]} = z\,\tau_z(x)^{[d_{\tau_z(x)}]}$$

holds in $G_{(X,r)}$ for all $x, z \in X$. Therefore, the subgroup $Z_{(X,r)}$ generated by the $x^{[d_x]}$ is normal.

Take a $y \in X$. Since $x \leftharpoondown y^{[d_y]} = x$ for all $x \in X$, one gets

(5.2) $g \leftharpoondown y^{[d_y]} = g$ for all $g \in G'_{(X,\lhd_r)}$.

Therefore,

$$J(x^{[d_x]}\, y^{[d_y]}) = (J(x^{[d_x]}) \leftharpoondown y^{[d_y]})\, J(y^{[d_y]}) = J(x^{[d_x]})J(y^{[d_y]}).$$

A similar argument yields $J((x^{[d_x]})^{-1}) = J(x^{[d_x]})^{-1}$. So, J restricted to $Z_{(X,r)}$ is a group isomorphism. The degree d_x of x is a multiple of D_x by definition[1]; recall that D_x is the minimal integer D satisfying $D \geq 2$ and $\rho_y^D = \mathrm{Id}_X$. Also, $J(x^{[d_x]}) = x^{d_x} \in G'_{(X,\lhd_r)}$. Thus the image $J(Z_{(X,r)})$ is the subgroup of $Z_{(X,\lhd_r)} \cong \bigoplus_{i=1}^{K_r} x_i^{D_i}$ generated by the $x_i^{\alpha_i D_i}$ for certain $\alpha_i \in \mathbb{N}$; cf. the proof of Theorem 4.2 for notations. The image $J(Z_{(X,r)})$, and hence the subgroup $Z_{(X,r)}$ itself, is then free abelian of rank K_r.

Let us check that Lemma 3.1 applies to the bijective group 1-cocycle $J\colon G_{(X,r)} \to G'_{(X,\lhd_r)}$, and to the relations

$$\mathcal{R}_{G_{(X,r)}} = \{\, x^{[d_x]} = 1 \,|\, x \in X \,\}, \qquad \mathcal{R}_{G'_{(X,\lhd_r)}} = \{\, x^{d_x} = 1 \,|\, x \in X \,\}.$$

The first condition follows from (5.2). The second one reads

$$\{\, x^{d_x} \leftharpoondown z \,|\, x \in X \,\} = \{\, x^{d_x} \,|\, x \in X \,\}$$

for all $z \in X$. Lemmas 5.7 and 5.10 yield $x^{[d_x]} \leftharpoondown z = \tau_z(x)^{[d_x]} = \tau_z(x)^{[d_{\tau_z(x)}]}$. Since the τ_z are bijective, we are done.

So, Lemma 3.1 yields a bijective group 1-cocycle

$$\overline{J}\colon \overline{G}_{(X,r)} \to G'_{(X,\lhd_r)}\big/\{x^{d_x} = 1\}.$$

The group $\overline{G}'_{(X,\lhd_r)}$ from Remark 4.3 is in general only a quotient of this second group, which we denote by H. But the argument from the proof of Theorem 4.2 repeats verbatim for H, and yields its finiteness and injectivity preservation, which imply finiteness and injectivity preservation for $\overline{G}_{(X,r)}$. $\square$

Example 5.11. Let $(X, \lhd)$ be a rack. Consider the solution $(X, r'_\lhd)$. One has $x^y = x$ for all $x, y \in X$, hence $J = \mathrm{Id}$, and $y^{[m]} = y^m \in G_{(X,r'_\lhd)}$ for all $y \in X$, $m \in \mathbb{N}$. Further, $x \leftharpoondown y = x$ and $y \rightharpoondown x = x \lhd y = \rho_y(x)$. Then d_y is 2 if $\rho_y = \mathrm{Id}_X$, and the degree of ρ_y otherwise. But this is precisely D_y. Thus the quotient $\overline{G}_{(X,r'_\lhd)}$ from Theorem 5.6 recovers the quotient $\overline{G}'_{(X,\lhd)}$ from Remark 4.3.

Example 5.12. For an involutive solution (X, r), the structure rack is trivial, i.e., $\rho_y = \mathrm{Id}_X$ for all $y \in X$. Thus d_y is the smallest even d satisfying $x \leftharpoondown y^{[d]} = y^{[d]} \rightharpoondown x = x$ for all x. The quotient $\overline{G}_{(X,r)}$ is in this case very close to that from [Deh15]. There the same power d was taken for all y, and the only condition imposed was

---

[1]We imposed d_x to be even when $\rho_x = \mathrm{Id}_X$ precisely to get this property.

$x \leftharpoondown y^{[d]} = x$ for all x, y. Note that the symmetric condition $y^{[d]} \rightharpoonup x = x$ is a consequence thereof, because of the relation between the actions $\leftharpoondown$ and $\rightharpoonup$ in the involutive case. Moreover, if the solution is indecomposable (i.e., has a unique orbit), then Lemma 5.10 implies $d_x = d_y$ for all $x, y \in X$. Thus, compared to the quotient from [Deh15], our $\overline{G}_{(X,r)}$ looses precision due to the evenness requirement for d, but gains precision for decomposable solutions.

Remark 5.13. The solution r on X induces an infinite invertible non-degenerate YBE solution R on $G_{(X,r)}$. Even better: $G_{(X,r)}$ becomes a *braided commutative group*. The condition $x \leftharpoondown y^{[d_y]} = y^{[d_y]} \rightharpoonup x = x$ is precisely what is needed for R to survive in the quotient $\overline{G}_{(X,r)}$. One thus obtains a rich source of finite braided commutative groups, finite *skew braces* etc.; cf. Remark 3.5. Also, Theorem 5.6 implies that a finite injective solution (X, r) injects into a finite skew brace, in such a way that r is the restriction to X of the solution constructed on the skew brace in [GV17]. For involutive solutions (which are always injective), this yields a result of [CGIS17, Remark 7].

Remark 5.14. A weaker version of Theorem 5.6 holds for structure monoids, with analogous proof. Namely, one gets a normal abelian sub-monoid of finite index. For SD solutions, it is a central sub-monoid. It is not free abelian in general. Injectivity is an automatic property for structure monoids, since they are graded and have degree 2 relations only.

We finish this section with an alternative definition of the degrees d_x. For this, the formula $\rho_y(x) = x \triangleleft_r y = \tau_y \widehat{\tau}_y^{-1}(x)$ needs to be generalized. For $\overline{y} = y_1 \ldots y_n \in X^{\times n}$, put $\rho_{\overline{y}} = \rho_{y_n} \cdots \rho_{y_1}$. Thus, conditions (2)–(3) from Definition 5.5 read

$$\rho_{y^d} = \tau_{y^{[d]}}|_X = \sigma_{y^{[d]}}|_X = \mathrm{Id}_X \,.$$

Lemma 5.15. *For any* $\overline{y} = y_1 \ldots y_n \in X^{\times n}$*, one has*

$$\rho_{\varphi(\overline{y})} = \tau_{\overline{y}} \widehat{\tau}_{\overline{y}}^{-1}, \qquad \qquad where \ \ \varphi(y_1 \ldots y_n) = y_1^{y_2 \ldots y_n} \ \ldots \ y_{n-1}^{y_n} \ y_n.$$

Proof. We use induction on n. The case $n = 1$ follows from the definition of ρ. To get from $n - 1$ to n, we need Lemma 3.3, rewritten as

$$\tau_z \rho_y = \rho_{\tau_z(y)} \tau_z$$

for all $y, z \in X$. Then, for any $\overline{y} = y_1 \ldots y_n \in X^{\times n}$, one has

$$\tau_{\overline{y}} \widehat{\tau}_{\overline{y}}^{-1} = \tau_{y_n} \cdots \tau_{y_1} \widehat{\tau}_{y_1}^{-1} \cdots \widehat{\tau}_{y_n}^{-1} = \tau_{y_n} \cdots \tau_{y_2} \rho_{y_1} \widehat{\tau}_{y_2}^{-1} \cdots \widehat{\tau}_{y_n}^{-1}$$
$$= \rho_{\tau_{y_n} \cdots \tau_{y_2}(y_1)} \, \tau_{y_n} \cdots \tau_{y_2} \widehat{\tau}_{y_2}^{-1} \cdots \widehat{\tau}_{y_n}^{-1} = \rho_{y_1^{y_2 \ldots y_n}} \, \rho_{\varphi(y_2 \ldots y_n)} = \rho_{\varphi(\overline{y})}.$$

We used the induction hypothesis for $y_2 \ldots y_n$. $\square$

An immediate corollary is the following observation.

Proposition 5.16. *Any two of the relations* $\rho_{y^d}|_X = \mathrm{Id}_X$*,* $\tau_{y^{[d]}}|_X = \mathrm{Id}_X$*,* $\widehat{\tau}_{y^{[d]}}|_X = \mathrm{Id}_X$*, each considered for all* $y \in X$*, imply the third one.*

6. Applications

Theorem 5.6 has several immediate implications.

Corollary 6.1. *Let (X, r) be a solution. The subgroup*

$$Z^0_{(X,r)} = \{\, g \in G_{(X,r)} \,|\, \forall x \in X,\ x \leftharpoonup g = g \rightharpoonup x = x \,\}$$

of $G_{(X,r)}$ is normal, of finite index, and abelian of rank K_r.

Proof. One can see $Z^0_{(X,r)}$ as the intersection of the kernels of the right and the left $G_{(X,r)}$-actions on X. Hence it is a normal subgroup of $G_{(X,r)}$. Further, r induces a YBE solution R on $G_{(X,r)}$ compatible with its group structure (Remark 5.13), which yields a right and a left $G_{(X,r)}$-actions on itself, whose kernels include the kernels of the $G_{(X,r)}$-actions on X. For any $g, h \in G_{(X,r)}$, one deduces $R(g, h) = (h, g)$, hence $gh = hg$. So, the subgroup $Z^0_{(X,r)}$ is abelian. Finally, it contains $Z_{(X,r)}$ as a subgroup, hence its finite index and its rank K_r. $\qquad\square$

We thus recover Theorem 2.6 from [Sol00] and Proposition 6 from [LYZ00].

Corollary 6.2. *Let (X, r) be a solution. Its structure group $G_{(X,r)}$ is*
  (1) *virtually $\mathbb{Z}^{K_r}$, where K_r is the number of orbits of the structure rack $(X, \lhd_r)$;*
  (2) *linear;*
  (3) *residually finite.*

Proof. Point 1 is a reformulation of Theorem 5.6. Further, consider the obvious degree K_r faithful representation of $Z_{(X,r)} \cong \mathbb{Z}^{K_r}$ over R. Its induced representation is faithful of degree $K_r |\overline{G}_{(X,r)}|$. Finally, all finitely generated linear groups are residually finite (Mal'cev 1940). $\qquad\square$

Another property of structure groups follows from our explicit description of the subgroups $Z_{(X,r)}$:

Proposition 6.3. *Let (X, r) be a solution. The abelianization $\mathrm{Ab}\, G_{(X,r)}$ of its structure group is of rank k_r, which is the number of its orbits (cf. Definition 5.9).*

Proof. Put $k = k_r$, $K = K_r$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_k$ be the orbits of (X, r), and let $\mathcal{RO}_1, \ldots, \mathcal{RO}_K$ be the orbits of $(X, \lhd_r)$. Recall that the latter refine the former; this yields a surjection $m\colon \{1, \ldots, K\} \twoheadrightarrow \{1, \ldots, k\}$. The free abelian groups $\oplus_i \mathbb{Z}\mathcal{O}_i \cong \mathbb{Z}^k$ and $\oplus_i \mathbb{Z}\mathcal{RO}_i \cong \mathbb{Z}^K$ will be abusively denoted by $\mathbb{Z}^k$ and $\mathbb{Z}^K$ respectively. Thus, the map m induces a group morphism $\mu\colon \mathbb{Z}^K \twoheadrightarrow \mathbb{Z}^k$. For the reader's convenience, we summarize all group morphisms used in this proof in a commutative diagram:

$$
\begin{array}{ccc}
\mathbb{Z}^K & \xrightarrow{\ \ \kappa\ \ } & G \\
{\scriptstyle\mu}\downarrow \quad {\scriptstyle\kappa'} \searrow & & \downarrow{\scriptstyle\pi} \quad \searrow{\scriptstyle\nu} \\
\mathbb{Z}^k & \xrightarrow[\ \ \kappa''\ \ ]{} \ \mathrm{Ab}\,G & \xtwoheadrightarrow[\ \ \nu'\ \ ]{} \mathbb{Z}^k
\end{array}
$$

Choose representatives y_i of the orbits $\mathcal{RO}_i$. Put $d_i = d_{y_i}$. In the proofs of Theorems 4.2 and 5.6, we showed that the group morphism $\kappa\colon \mathbb{Z}^K \to G_{(X,r)}$ defined by $\mathcal{RO}_i \mapsto y_i^{[d_i]}$ is injective. Consider also the natural projection $\pi\colon G_{(X,r)} \twoheadrightarrow \mathrm{Ab}\, G_{(X,r)}$, and the composition $\kappa' = \pi\kappa$. Further, the morphism $\nu\colon G_{(X,r)} \twoheadrightarrow \mathbb{Z}^k$ sending every x to its orbit is well defined and induces $\nu'\colon \mathrm{Ab}\, G_{(X,r)} \twoheadrightarrow \mathbb{Z}^k$. Lemmas 5.7 and 5.10 imply the relations $y^{[d_y]}z = z\tau_z(y)^{[d_{\tau_z(y)}]}$ and $zy^{[d_y]} = \widehat{\tau}_z^{-1}(y)^{[d_{\widehat{\tau}_z^{-1}(y)}]}z$ in $G_{(X,r)}$, hence $y^{[d_y]} = \tau_z(y)^{[d_{\tau_z(y)}]} = \widehat{\tau}_z^{-1}(y)^{[d_{\widehat{\tau}_z^{-1}(y)}]}$ in $\mathrm{Ab}\, G_{(X,r)}$. Therefore, κ' induces a group morphism $\kappa''\colon \mathbb{Z}^k \to \mathrm{Ab}\, G_{(X,r)}$. Now, the composition $\nu'\kappa''$ multiplies each $\mathcal{O}_i$ by d_j, for any $j \in m^{-1}(i)$. Hence κ'' is injective. To conclude, it

remains to show that $\kappa''(\mathbb{Z}^k)$ is of finite index in $\mathrm{Ab}\,G_{(X,r)}$. This follows from the finiteness of $\overline{G}_{(X,r)}$ and from the surjection

$$\overline{G} = G/\kappa(Z^K) \twoheadrightarrow \mathrm{Ab}\,G/\pi\kappa(Z^K) = \mathrm{Ab}\,G/\kappa''\mu(Z^K) = \mathrm{Ab}\,G/\kappa''(\mathbb{Z}^k). \qquad \square$$

It would also be interesting to understand the torsion of $\mathrm{Ab}\,G_{(X,r)}$. It is trivial for SD solutions. However, in general this is not the case:

Example 6.4. Consider the involution $\psi\colon a \leftrightarrow b$ on the set $X = \{a,b\}$. The map $r(x,y) = (\psi(y), \psi(x))$ yields an involutive solution. Its structure group is

$$G_{(X,r)} = \langle\, a,b \,|\, a^2 = b^2 \,\rangle, \qquad\qquad \mathrm{Ab}\,G_{(X,r)} \cong \mathbb{Z} \times \mathbb{Z}_2.$$

Let us also describe the finite quotient $\overline{G}_{(X,r)}$. The degrees are $d_a = d_b = 2$. The corresponding T-twisted powers are $J^{-1}(a,a) = (b,a)$, $J^{-1}(b,b) = (a,b)$. One gets

$$\overline{G}_{(X,r)} = \langle\, a,b \,|\, a^2 = b^2, ab = ba = 1 \,\rangle \cong \mathbb{Z}_4,$$

where a is sent to 1 and b to -1. Thus our solution is injective. Any attempt to extend $Z_{(X,r)}$ would destroy the injectivity of $X \to \overline{G}_{(X,r)}$ here.

Example 6.5. A slight modification of the previous example produces torsion-free $\mathrm{Ab}\,G_{(X,r)}$. Namely, extend ψ to $Y = \{a,b,c\}$ by $\psi(c) = c$. As before, $r(x,y) = (\psi(y), \psi(x))$ is an involutive solution, with

$$G_{(X,r)} = \langle\, a,b,c \,|\, a^2 = b^2, ac = cb, bc = ca \,\rangle \cong \langle\, a,c \,|\, ac^2 = c^2a, a^2c = ca^2 \,\rangle,$$

$$\mathrm{Ab}\,G_{(X,r)} \cong \mathbb{Z}^2.$$

All degrees are 2, and $J^{-1}(c,c) = (c,c)$. So,

$$\overline{G}_{(X,r)} = \langle\, a,b \,|\, a^2 = b^2, ac = cb, bc = ca, ab = ba = c^2 = 1 \,\rangle \cong \mathbb{Z}_4 \rtimes \mathbb{Z}_2,$$

where $\mathbb{Z}_2$ acts on $\mathbb{Z}_4$ by the sign change. This equivalence works as follows: $a \mapsto (1,0)$, $b \mapsto (-1,0)$, $c \mapsto (0,1)$. Here again $Z_{(X,r)}$ is a maximal subgroup satisfying all requirements of Theorem 5.6.

Recall that according to Proposition 1.1, the structure group does not change if a solution is replaced with a biquandle quotient. We will now construct an even smaller quotient which is injective and still has the same structure group. As a result, in a study of structure groups one can work with injective biquandles only. While the natural definition of this quotient involves comparing elements of the (infinite) group $G_{(X,r)}$, an alternative definition compares elements of our finite quotients $\overline{G}_{(X,r)}$ only, which is realizable by a computer.

Proposition 6.6. *For a solution (X,r), define an equivalence relation by $x \approx x'$ if and only if $\iota(x) = \iota(x')$ in $G_{(X,r)}$. Then r induces an injective solution r' on $X/\approx$. Moreover, the quotient map $X \twoheadrightarrow X/\approx$ induces a group isomorphism*

$$G_{(X,r)} \xrightarrow{\;\sim\;} G_{(X/\approx,\, r')}.$$

Proof. For $x,x' \in X$, the relation $x \approx x'$ implies $\sigma_x = \sigma_{x'}$ and $\tau_x = \tau_{x'}$. So in $G_{(X,r)}$ one has

$$\sigma_x(y)\tau_y(x) = xy = x'y = \sigma_x(y)\tau_y(x'),$$

hence $\tau_y(x) \approx \tau_y(x')$. Similarly, $\sigma_y(x) \approx \sigma_y(x')$. As a result, the induced map r' is well-defined. The remaining assertions are straightforward. $\qquad \square$

Definition 6.7. The biquandle $(X/\approx, r')$ from the proposition will be called the *induced injective solution (IIS)* of (X, r), denoted by $\mathrm{IIS}(X, r)$.

By Remark 1.3 and Lemma 1.4, the IIS of (X, r) is a quotient of its induced biquandle. Also, the IIS construction enjoys a universal property analogous to that from Remark 1.3. Moreover, it defines a functor **YBESol** $\to$ **InjSol** to the category of injective solutions, which is a retraction for the inclusion functor. This construction restricts to racks and yields a functor **Rack** $\to$ **InjRack** to the category of injective racks (which are necessarily quandles). By the bijectivity of the guitar map J, the structure rack construction intertwines these "injectivization" functors. One gets a commutative diagrams of functors analogous to those from Propositions 1.5 and 2.7:

$$
\begin{array}{ccc}
\textbf{Rack} & \longrightarrow & \textbf{InjRack} \\
\downarrow & & \downarrow \\
\textbf{YBESol} & \longrightarrow & \textbf{InjSol} \\
\downarrow & & \downarrow \\
\textbf{Rack} & \longrightarrow & \textbf{InjRack}
\end{array}
$$

Id (left) Id (right)

The injectivity preservation argument from the proof of Theorem 4.2 has the following by-product:

Lemma 6.8. *Elements $x, x' \in X$ yield the same element of $G_{(X,r)}$ if and only if they yield the same element of $\overline{G}_{(X,r)}$.*

As a result, the relation $x \approx x'$ can be tested in the finite group $\overline{G}_{(X,r)}$.

7. Orderability

Recall that a group G is *left-orderable* if it can be endowed with a total order stable by left translations: $a < b \implies ca < cb$. If the order can be chosen to be also stable by right translations, then G is called *bi-orderable*. Orderability has useful algebraic implications, the simplest of which is torsion-freeness. It has also remarkable connexions with topology, geometry, dynamics, probability [SW00, DDRW08, DNR14]. This section explores orderability properties of structure groups.

We need a general result on bi-orderability:

Proposition 7.1. *Let G be a virtually abelian finitely generated group. Then G is bi-orderable if and only if it is free abelian.*

Proof. The "if" implication is straightforward. Conversely, assume that G is bi-orderable but non-abelian. Take $g, h \in G$ such that $gh > hg$, i.e. $h^{-1}gh > g$. This implies $h^{-1}g^n h > g^n$, hence $g^n h > hg^n$ for all $n \in \mathbb{N}$. Similarly, one proves $g^n h^n > h^n g^n$. Since G has an abelian subgroup H of finite index, there exists an $n \in \mathbb{N}$ such that $g^n, h^n \in H$, hence $g^n h^n = h^n g^n$, contradiction. $\qquad\square$

Coupled with Theorem 5.6, this result characterizes bi-orderable structure groups:

Theorem 7.2. *Let (X, r) be a solution. Then $G_{(X,r)}$ is bi-orderable if and only if it is free abelian. In this case,*
  (1) the orbits of the solution (X, r) and of its structure rack $(X, \triangleleft_r)$ coincide, and $k_r = K_r$;

(2) the group morphism $\nu \colon G_{(X,r)} \twoheadrightarrow \mathbb{Z}^{k_r}$ sending every x from the orbit $\mathcal{O}_i$ to the generator e_i of $\mathbb{Z}^{k_r}$ is an isomorphism.

Proof. It remains to prove the last two statements. We use notations from the proof of Proposition 6.3.

(1) We will prove a slightly more general statement. If $G_{(X,r)}$ is abelian, then the quotient map $\pi \colon G_{(X,r)} \twoheadrightarrow \mathrm{Ab}\, G_{(X,r)}$ is the identity. Since the rank of $\mathrm{Ab}\, G_{(X,r)}$ is k_r, this yields $G_{(X,r)} = \mathrm{Ab}\, G_{(X,r)} \cong \mathbb{Z}^{k_r} \times A$ for some finite abelian group A. Recall the map $\kappa \colon \mathbb{Z}^{K_r} \hookrightarrow G_{(X,r)} \cong \mathbb{Z}^{k_r} \times A$. Its injectivity implies $K_r \leq k_r$. Since the K_r orbits of $(X, \lhd_r)$ refine the k_r orbits of (X, r), this inequality means that these two partitions into orbits coincide.

(2) Now, suppose $G_{(X,r)}$ free abelian. Then ν surjects $G_{(X,r)} \cong \mathbb{Z}^{k_r}$ onto $\mathbb{Z}^{k_r}$, and is thus an isomorphism. $\qquad\square$

Structure groups of *trivial* solutions $r(x,y) = (y,x)$ are free abelian. In general the converse is false: for instance, the structure group of the rack $(\mathbb{Z},\, x \lhd y = x+1)$ is $\mathbb{Z}$. However, it holds for involutive solutions:

Proposition 7.3. *Let (X,r) be an involutive solution. Then $G_{(X,r)}$ is abelian if and only if r is trivial.*

Proof. Assume that $G_{(X,r)}$ is abelian. Our proof of Theorem 7.2 identifies the two partitions into orbits. Recall that the induced rack of an involutive solution is trivial, $x \lhd_r y = x$, so all its orbits are one-element. Hence all orbits of (X,r) are one-element as well. This means $\sigma_x = \tau_x = \mathrm{Id}$ for all $x \in X$, hence r is trivial. $\quad\square$

Thus, among involutive solutions, only the trivial ones have bi-orderable structure groups.

To deal with left-orderability, we need a general notion of MP solutions, which is well studied in the literature for the particular case of involutive solutions.

Lemma 7.4. *Let (X,r) be a solution. Define an equivalence relation on X by*

$$x \sim x' \quad \Longleftrightarrow \quad \sigma_x = \sigma_{x'} \;\&\; \tau_x = \tau_{x'}.$$

Then r induces a solution $\overline{r}$ on $\overline{X} = X/\!\sim$.

Proof. We only have to check that $\overline{r}$ is well defined. This boils down to verifying $\sigma_{\phi(x)} = \sigma_{\phi(x')}$, $\tau_{\phi(x)} = \tau_{\phi(x')}$ for $x \sim x'$ and $\phi \in \{\sigma_y, \tau_y\}$, $y \in X$. But this directly follows from Equations (1.2)–(1.3). $\qquad\square$

Definition 7.5. The solution from Lemma 7.4 is called the *retraction* of (X,r), denoted by $\mathrm{Ret}(X,r) = (\overline{X}, \overline{r})$. A solution is called *multipermutation (MP) of level n* if n is the minimal non-negative integer such that $\# \mathrm{Ret}^n(X,r) = 1$. A solution is called *retractable* if $\overline{X}$ is smaller than X, and *irretractable* otherwise.

Example 7.6. The trivial one-element solution is the only MP solution of level 0. Being of level 1 means having the form $r(x,y) = (f(y), g(x))$, where f and g are commuting symmetries of X.

Example 7.7. For involutive solutions, relation $\sigma_x = \sigma_{x'}$ implies $\tau_x = \tau_{x'}$. We thus recover the definition of [ESS99].

Example 7.8. For an SD solution $(X, r_\lhd)$, $x \sim x'$ means $z \lhd x = z \lhd x'$ for all $z \in X$. Then $\lhd$ induces a rack operation $\overline{\lhd}$ on $\overline{X} = X/\sim$, and the solution $\overline{r_\lhd}$ is associated to this rack operation: $\overline{r_\lhd} = r_{\overline{\lhd}}$. The pair $(\overline{X}, \overline{\lhd})$ is called the *retraction* of $(X, \lhd)$. A rack is called *MP of level n* if the associated solution is so.

Lemma 7.9. *The retraction $X/\sim$ of a solution is a quotient of its induced injective solution $X/\approx$.*

Proof. Since the collections of maps σ and τ define $G_{(X,r)}$-actions on X, the relation $x \approx x'$ implies $x \sim x'$. □

Multipermutation involutive solutions are known to be the only involutive solutions with left-orderable structure group. One of the implications of the following theorem was prove in [Cho16]; see also [JO05, Proposition 4.2]. The other was proved in [BCV17, Theorem 2.1].

Theorem 7.10. *Let (X, r) be an involutive solution. Then $G_{(X,r)}$ is left-orderable if and only if (X, r) is multipermutation.*

Moreover, the space of left orders of the structure group of a non-trivial MP involutive solution with $\#X \geq 3$ is known to be extremely rich [Cho16].

Example 7.11. Examples 6.4 and 6.5 describe structure groups of two level 1 involutive solutions. These groups are then left-orderable, and have the following remarkable feature: the element $a^2 = b^2$ has at least two square roots.

A group G is said to be *diffuse* if for every finite non-empty subset A of G there exists an $a \in A$ such that for all $g \in G \setminus \{1\}$, either $ga \notin A$ or $g^{-1}a \notin A$. Such a group satisfies the *unique product property (UPP)*: for every finite non-empty subsets A, B of G there is an element x which can be written uniquely as $x = ab$ with $a \in A$, $b \in B$. These technical properties imply Kaplansky's conjectures for G, and were conceived as efficient tools for proving them. See [KR16] for an up-to-date survey of these questions.

We now show that for structure groups of involutive solutions, being diffuse and left-orderable is the same. This answers a question of Chouraqui [Cho16].

Theorem 7.12. *Let (X, r) be an involutive solution. Then $G_{(X,r)}$ is diffuse if and only if (X, r) is MP.*

Proof. Implication "left-orderable $\implies$ diffuse" is classical. Indeed, for a finite non-empty subset A of G, the minimal element a of A satisfies the property from the definition. Further, our group $G_{(X,r)}$ is virtually abelian. By [KR16, Theorem 3.3], such a group is diffuse exactly if it is locally indicable (that is, any of its finitely generated non-trivial subgroups surjects onto $\mathbb{Z}$). To conclude, use the classical implication "locally indicable $\implies$ left-orderable" (see [DNR14], or any other textbook on orderable groups), and Theorem 7.10. □

Question 7.13. *Can structure groups of irretractable involutive solutions satisfy the UPP?*

A positive answer would yield an example of a non-diffuse group with UPP, solving an open question.

Example 7.14. One of the simplest irretractable involutive solutions is given by $X = \{1, 2, 3, 4\}$ and $r(x, y) = (\sigma_x(y), \sigma^{-1}_{\sigma_x(y)}(x))$, where

$$\sigma_1 = (23), \quad \sigma_2 = (14), \quad \sigma_3 = (1243), \quad \sigma_4 = (1342).$$

In [JO07, Example 8.2.14] Jespers and Okniński proved that the UPP is false for its structure group.

Let us now turn to our second favourite class of solutions. For SD solutions, left-orderability turns out to be equivalent to bi-orderability:

Theorem 7.15. *For a finite rack $(X, \lhd)$, the following statements are equivalent:*
  (1) $G_{(X, \lhd)}$ is bi-orderable;
  (2) $G_{(X, \lhd)}$ is left-orderable;
  (3) $G_{(X, \lhd)}$ has no torsion;
  (4) $G_{(X, \lhd)}$ is free abelian;
  (5) $G_{(X, \lhd)}$ is abelian;
  (6) the induced injective rack $X/\approx$ of $(X, \lhd)$ is trivial.
Any of these statements implies that $(X, \lhd)$ is a multipermutation rack of level at most 2.

From this theorem we learn that structure groups of racks yield no new examples of left-orderable groups. On the bright side, for this class of groups we obtain an interesting dichotomy: either they are free abelian, or they are non-abelian and have torsion. This dichotomy is decided by testing the relation $x \approx x \lhd y$ for all $x, y \in X$, which, according to Lemma 6.8, can be tested in the finite group $\overline{G}_{(X, \lhd)}$.

Proof. Implications $4 \Rightarrow 1 \Rightarrow 2 \Rightarrow 3$ are classical. Let us show $3 \Rightarrow 4$. Assume that $G_{(X, \lhd)}$ has no torsion. Operation $\lhd$ induces a $G_{(X, \lhd)}$-action on X, whose kernel is contained in the center of $G_{(X, \lhd)}$. So this center is of finite index. According to Schur's theorem, the commutator subgroup of $G_{(X, \lhd)}$ is then finite (cf. [Rot95, Theorem 5.32]). Since $G_{(X, \lhd)}$ has no torsion, this subgroup is trivial, and $G_{(X, \lhd)}$ is free abelian.

Now, assume $G_{(X, \lhd)}$ abelian. For any $x, y \in X$, from $yx = xy = y(x \lhd y)$ in $G_{(X, \lhd)}$ one deduces $x \approx x \lhd y$. Hence the induced injective rack $(X/\approx, \lhd')$ of $(X, \lhd)$ is trivial. Further, since the structure groups of $(X, \lhd)$ and $(X/\approx, \lhd')$ are isomorphic, the triviality of $(X/\approx, \lhd')$ means that $G_{(X/\approx, \lhd')}$, and hence $G_{(X, \lhd)}$, is free abelian. We get $5 \Rightarrow 6 \Rightarrow 4$. Implication $4 \Rightarrow 5$ is trivial.

Finally, by Lemma 7.9, if $(X/\approx, \lhd')$ is trivial then so is $\mathrm{Ret}(X, \lhd)$. Hence $\mathrm{Ret}^2(X, \lhd)$ has one element only. $\qquad\square$

Note that some level 2 MP racks do not satisfy the conditions of the theorem:

Example 7.16. The set $X = \{a, b, c, d\}$ with right translations $\rho_a = \rho_b \colon c \leftrightarrow d$ and $\rho_c = \rho_d \colon a \leftrightarrow b$ is a level 2 quandle. Consider the group

$$H = \langle\, a, c, t \,|\, a^2 = c^2 = t^2 = 1,\ t \text{ central},\ ac = tca \,\rangle.$$

It is isomorphic to $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$, where a, t, c generate the three copies of $\mathbb{Z}_2$, in this order, and c acts on $\mathbb{Z}_2 \times \mathbb{Z}_2$ by sending $a^\alpha t^\tau$ to $a^\alpha t^{\tau + \alpha}$. In particular, a, at, c, ct are four distinct elements of H. Now, a surjection $G_{(X, \lhd)} \twoheadrightarrow H$ can be defined as follows: $a \mapsto a, b \mapsto at, c \mapsto c, d \mapsto ct$. (In fact, H is the finite quotient $\overline{G}_{(X, \lhd)}$. That is how it appeared in our argument!) Therefore, a, b, c, d are four distinct elements of $G_{(X, \lhd)}$, and our quandle is injective. In particular, $X/\approx$ is just X,

which is non-trivial. Also, ab^{-1} is a 2-torsion element in $G_{(X,\lhd)}$. In this example, the finite quotient $\overline{G}_{(X,\lhd)}$ was essential to determine that our structure group does not satisfy the properties from the theorem.

Among injective quandles, only trivial ones satisfy the conditions of the theorem. This is not true for non-injective quandles:

Example 7.17. Consider the quotient of the quandle from the previous example by the relation $b = c$. This is a 3-element quandle with the structure group $\mathbb{Z}^2$.

Left-orderability question for general structure groups remains open:

Question 7.18. *Let (X,r) be a non-involutive injective solution. Can its structure group $G_{(X,r)}$ be left orderable?*

We suspect the answer to be negative. Indeed, the structure rack $(X, \lhd_r)$ of such a solution is injective and non-trivial, so, by Theorem 7.15, the group $G_{(X,\lhd_r)}$ has torsion. The groups $G_{(X,r)}$ and $G_{(X,\lhd_r)}$ being related by the bijective 1-cocycle J, this must have serious implications for $G_{(X,r)}$.

APPENDIX A. SIZE 3 BIQUANDLES

To illustrate our results, we will classify all solutions whose structure racks are size 3 quandles. We will describe their structure groups, and finite quotients $\overline{G}$ thereof. We will always work up to solution/quandle isomorphism. While reading this appendix, the reader might keep in mind the following question.

Question A.1. *Given a finite rack $(X, \lhd)$, how can one construct all solutions having $(X, \lhd)$ as their right structure rack?*

There are precisely three quandle structures on the set $X = \{0, 1, 2\}$:
  (1) the trivial quandle T: $\rho_x = \mathrm{Id}$, $K_\lhd = 3$, $G_T \cong \mathbb{Z}^3$, $\overline{G}_T \cong \mathbb{Z}_2^3$, $\mathrm{Iso}_T = 1$, the quandle is injective and MP of level 1;
  (2) the two-orbit quandle S: $\rho_0 = (12)$, $\rho_1 = \rho_2 = \mathrm{Id}$, $K_\lhd = 2$, $G_S \cong \mathbb{Z}^2$, $\overline{G}_S \cong \mathbb{Z}_2^2$, $\mathrm{Iso}_S = 3$, the quandle is not injective and is MP of level 2;
  (3) the dihedral quandle D: $\rho_0 = (12)$, $\rho_1 = (02)$, $\rho_2 = (01)$, $K_\lhd = 1$, $\mathrm{Iso}_D = 1$, the quandle is injective (as we shall now see) and irretractable.
This description uses the maps $\rho_y \colon x \mapsto x \lhd y$, the notation $K_\lhd = \# \mathrm{Orb}(X, \lhd)$ for the number of orbits of a quandle, and the notation Iso_Q for the number of quandle structures on X isomorphic to Q.

The structure group of D is a quotient of the braid group B_3:

$$G_D \cong \langle\, 1, 2 \mid 121 = 212, 1^2 = 2^2 \,\rangle \cong {B_3}\big/{1^2 = 2^2}, \qquad \mathrm{Ab}\, G_D \cong \mathbb{Z}.$$

All $x \in D$ are of degree $D_x = 2$, so the finite quotient from Theorem 4.2 is the symmetric group: $\overline{G}_D \cong S_3$. The injectivity of D can be easily tested in S_3. In fact, D is isomorphic to the conjugation class of transpositions in S_3.

The kernel of the surjection $\pi \colon G_D \twoheadrightarrow S_3$ is freely generated by the central element $1^2 = 2^2$; freeness follows from the surjection $p \colon G_D \twoheadrightarrow \mathbb{Z}$, $1, 2 \mapsto 1$. So, G_D is a central extension of S_3:

$$0 \to \mathbb{Z} \to G_D \to S_3 \to 0.$$

Since G_D surjects onto the non-abelian group S_3, it is non-abelian. It has torsion: the element $1^{-1}2$ is non-trivial since $\pi(1^{-1}2) \neq \mathrm{Id}$, and $\pi((1^{-1}2)^3) = \mathrm{Id}$ implies

$(1^{-1}2)^3 = 1^{2n}$ for some $n \in \mathbb{Z}$, which is 0 because of the surjection p. We obtain an elementary illustration of the main assertions of Theorem 7.15.

Given a finite rack $(X, \triangleleft)$, a *chain* in $(X, \triangleleft)$ is a sequence $(x_i) \in X^{\mathbb{Z}}$ such that $x_{i-1} \triangleleft x_i = x_{i+1}$ for all $i \in \mathbb{Z}$. It is periodic. The *period pattern* of a rack is the multi-set of periods of all its chains. These periods sum up to $|X|^2$. For instance, the period patterns of size 3 quandles are:

(1) $1, 1, 1, 2, 2, 2$ for T;
(2) $1, 1, 1, 2, 4$ for S;
(3) $1, 1, 1, 3, 3$ for D.

Similarly, a *chain* in a finite solution (X, r) is a sequence of pairs $((x_i, y_i)) \in (X \times X)^{\mathbb{Z}}$ such that $r(x_i, y_i) = (x_{i+1}, y_{i+1})$ for all $i \in \mathbb{Z}$. It is periodic. Moreover, (x_i) is a chain in $(X, \triangleright_r)$, and (y_i) is a chain in $(X, \triangleleft_r)$. Since r is non-degenerate, the periods of both chains coincide with that of $((x_i, y_i))$. Hence a period-respecting bijection between the chains of the left and the right structure racks of (X, r).

These chain bijections allow us to classify size 3 biquandles. Details are tedious but straightforward, and are omitted here.

Recall that a solution (X, r) is called *decomposable* if $X = Y \sqcup Z$, $Y \neq \emptyset \neq Z$, and r restricts to both $Y \times Y$ and $Z \times Z$.

(1) Structure quandle T. That is, one classifies involutive solutions of size 3. They are always injective.

  (a) The trivial solution $r(x, y) = (y, x)$.
  $$G \cong \mathrm{Ab}\, G \cong \mathbb{Z}^3, \qquad \overline{G} \cong \mathbb{Z}_2^3.$$
  It is MP of level 1, with the number of orbits $k_r = 3$.

  (b) The unique indecomposable solution $r(x, y) = (y+1, x-1)$ (cf. [ESS99]). It is MP of level 1. Here $k_r = 1$, and
  $$G \cong \langle\, 0, 1 \,|\, 0^3 = 1^3, (10)^3 = 1^3 0^3 \,\rangle, \qquad \mathrm{Ab}\, G \cong \mathbb{Z} \times \mathbb{Z}_3,$$
  We do not see any conceptual description of this structure group or its finite quotient. In particular, the left orderability of G and the finiteness of $\overline{G}$ are not obvious from their presentations.

  (c) Solution from Example 6.5: $r(x, y) = (-y, -x)$. It is MP of level 1. Here $k_r = 2$,
  $$G \cong \langle\, 0, 1 \,|\, 01^2 = 1^2 0, 0^2 1 = 10^2 \,\rangle, \qquad \mathrm{Ab}\, G \cong \mathbb{Z}^2, \qquad \overline{G} \cong \mathbb{Z}_4 \rtimes \mathbb{Z}_2.$$

  (d) The two remaining solutions are MP of level 2, and have $k_r = 2$. The first one is $r(x, y) = (\sigma_x(y), \sigma_y(x))$, with $\sigma_1 = \sigma_2 = (12), \sigma_0 = \mathrm{Id}$.
  $$G \cong \langle\, 1, 2 \,|\, 1^2 = 2^2 \,\rangle \times \mathbb{Z}, \qquad \mathrm{Ab}\, G \cong \mathbb{Z}^2 \times \mathbb{Z}_2, \qquad \overline{G} \cong \mathbb{Z}_4 \times \mathbb{Z}_2.$$

  (e) The second one is $r(x, y) = (\sigma_x(y), \sigma_y(x))$, $\sigma_1 = \sigma_2 = \mathrm{Id}, \sigma_0 = (12)$.
  $$G \cong \mathbb{Z}^2 \rtimes \mathbb{Z}, \qquad \mathrm{Ab}\, G \cong \mathbb{Z}^2, \qquad \overline{G} \cong \mathbb{Z}_2^2 \rtimes \mathbb{Z}_2.$$
  In both semidirect products, the action is by component permutation: $1 \cdot (a, b) = (b, a)$.

(2) Structure quandle S. Here there are four non-isomorphic solutions, but they all yield the same groups:
$$G \cong \mathrm{Ab}\, G \cong G_{(X, \triangleleft)} \cong \mathbb{Z}^2, J = \mathrm{Id}, \qquad \overline{G} \cong \mathbb{Z}_2^2.$$
All solutions are decomposable, MP of level 2, non-injective, with $k_r = 2$. Their induced injective solutions are trivial of size 2.

  (a) The SD solution $r = r_\triangleleft$.
  (b) $r(x,y) = (\sigma_x(y), -x)$, with $\sigma_1 = \sigma_2 = (12), \sigma_0 = \mathrm{Id}$.
(3) Structure quandle D. All solutions are indecomposable, irretractable, injective, with $k_r = 1$. Their structure groups have 3-torsion, and are thus not left-orderable.
  (a) The SD solution $r = r_\triangleleft$. Here $G \cong G_D$, $\overline{G} \cong \overline{G}_D$.
  (b) $r(x,y) = (y+1, 1-x-y)$. Here $G \cong G_D$, $\overline{G} \cong G_D/1^6$. The latter group surjects onto $\mathbb{Z}_6$, and is thus different from $\overline{G}_D \cong S_3$.
  (c) $r(x,y) = (-y, x-y)$. Here $G \cong \mathrm{Ab}\, G \cong \mathbb{Z} \times \mathbb{Z}_3$, $\overline{G} \cong \mathbb{Z}_6$.

For S and D, one should also include the inverses r^{-1} of the listed solutions. Replacing r by r^{-1} does not change the structure group and its finite quotient $\overline{G}$, but for D it does change the 1-cocycle J.

References

[AG03]   Nicolás Andruskiewitsch and Matías Graña. From racks to pointed Hopf algebras. *Adv. Math.*, 178(2):177–243, 2003.
[BCJO]   D. Bachiller, F. Cedo, E. Jespers, and J. Okninski. A family of irretractable square-free solutions of the Yang–Baxter equation. *Accepted for publication in Forum Mathematicum.*
[BCV17]   D. Bachiller, F. Cedó, and L. Vendramin. A characterization of finite multipermutation solutions of the Yang–Baxter equation. *ArXiv e-prints*, January 2017.
[Bri88]   E. Brieskorn. Automorphic sets and braids and singularities. In *Braids (Santa Cruz, CA, 1986)*, volume 78 of *Contemp. Math.*, pages 45–115. Amer. Math. Soc., Providence, RI, 1988.
[CG14]   Fabienne Chouraqui and Eddy Godelle. Finite quotients of groups of I-type. *Adv. Math.*, 258:46–68, 2014.
[CGIS17] Ferran Cedó, Tatiana Gateva-Ivanova, and Agata Smoktunowicz. On the Yang–Baxter equation and left nilpotent left braces. *J. Pure Appl. Algebra*, 221:751–756, 2017.
[Cho10]   Fabienne Chouraqui. Garside groups and Yang–Baxter equation. *Comm. Algebra*, 38(12):4441–4460, 2010.
[Cho16]   Fabienne Chouraqui. Left orders in Garside groups. *Internat. J. Algebra Comput.*, 26(7):1349–1359, 2016.
[CJdR10] Ferran Cedó, Eric Jespers, and Ángel del Río. Involutive Yang–Baxter groups. *Trans. Amer. Math. Soc.*, 362(5):2541–2558, 2010.
[CJO10]   Ferran Cedó, Eric Jespers, and Jan Okniński. Retractability of set theoretic solutions of the Yang–Baxter equation. *Adv. Math.*, 224(6):2472–2484, 2010.
[DDRW08] Patrick Dehornoy, Ivan Dynnikov, Dale Rolfsen, and Bert Wiest. *Ordering braids*, volume 148 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2008.
[Deh15]   Patrick Dehornoy. Set-theoretic solutions of the Yang–Baxter equation, RC-calculus, and Garside germs. *Adv. Math.*, 282:93–127, 2015.
[DNR14]   B. Deroin, A. Navas, and C. Rivas. Groups, Orders, and Dynamics. *ArXiv e-prints*, August 2014.
[Dri92]   V. G. Drinfel'd. On some unsolved problems in quantum group theory. In *Quantum groups (Leningrad, 1990)*, volume 1510 of *Lecture Notes in Math.*, pages 1–8. Springer, Berlin, 1992.
[ESS99]   Pavel Etingof, Travis Schedler, and Alexandre Soloviev. Set-theoretical solutions to the quantum Yang–Baxter equation. *Duke Math. J.*, 100(2):169–209, 1999.

[FRS93]   Roger Fenn, Colin Rourke, and Brian Sanderson. An introduction to species and the
           rack space. In *Topics in knot theory (Erzurum, 1992)*, volume 399 of *NATO Adv. Sci.
           Inst. Ser. C Math. Phys. Sci.*, pages 33–55. Kluwer Acad. Publ., Dordrecht, 1993.
[GHV11]   M. Graña, I. Heckenberger, and L. Vendramin. Nichols algebras of group type with
           many quadratic relations. *Adv. Math.*, 227(5):1956–1989, 2011.
[GIC12]   Tatiana Gateva-Ivanova and Peter Cameron. Multipermutation solutions of the Yang–
           Baxter equation. *Comm. Math. Phys.*, 309(3):583–621, 2012.
[GIM08]   Tatiana Gateva-Ivanova and Shahn Majid. Matched pairs approach to set theoretic
           solutions of the Yang–Baxter equation. *J. Algebra*, 319(4):1462–1529, 2008.
[GIVdB98] Tatiana Gateva-Ivanova and Michel Van den Bergh. Semigroups of I-type. *J. Algebra*,
           206(1):97–112, 1998.
[GV17]   L. Guarnieri and L. Vendramin. Skew braces and the Yang–Baxter equation. *Math.
           Comp.*, 86(307):2519–2534, 2017.
[JO05]   Eric Jespers and Jan Okniński. Monoids and groups of I-type. *Algebr. Represent.
           Theory*, 8(5):709–729, 2005.
[JO07]   Eric Jespers and Jan Okniński. *Noetherian semigroup algebras*, volume 7 of *Algebras
           and Applications*. Springer, Dordrecht, 2007.
[KR16]   Steffen Kionke and Jean Raimbault. On geometric aspects of diffuse groups. *Doc.
           Math.*, 21:873–915, 2016. With an appendix by Nathan Dunfield.
[LV17]   Victoria Lebed and Leandro Vendramin. Homology of left non-degenerate set-theoretic
           solutions to the Yang–Baxter equation. *Adv. Math.*, 304:1219–1261, 2017.
[LYZ00]   Jiang-Hua Lu, Min Yan, and Yong-Chang Zhu. On the set-theoretical Yang–Baxter
           equation. *Duke Math. J.*, 104(1):1–18, 2000.
[NV06]   Sam Nelson and John Vo. Matrices and finite biquandles. *Homology Homotopy Appl.*,
           8(2):51–73, 2006.
[Rot95]   Joseph J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate
           Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.
[Rum07]   Wolfgang Rump. Generalized radical rings, unknotted biquandles, and quantum
           groups. *Colloq. Math.*, 109(1):85–100, 2007.
[Sol00]   Alexander Soloviev. Non-unitary set-theoretical solutions to the quantum Yang–
           Baxter equation. *Math. Res. Lett.*, 7(5-6):577–596, 2000.
[SV17]   A. Smoktunowicz and L. Vendramin. On skew braces. *ArXiv e-prints*, May 2017.
[SW00]   Hamish Short and Bert Wiest. Orderings of mapping class groups after Thurston.
           Enseign. Math. (2), 46(3-4):279–312, 2000.
[Szy16]   M. Szymik. Permutations, power operations, and the center of the category of racks.
           ArXiv e-prints, September 2016.
[Ven16]   L. Vendramin. Extensions of set-theoretic solutions of the Yang–Baxter equation and
           a conjecture of Gateva-Ivanova. *J. Pure Appl. Algebra*, 220(5):2064–2076, 2016.

School of Mathematics, Trinity College, Dublin 2, Ireland
E-mail address: `lebed.victoria@gmail.com, lebed@maths.tcd.ie`

IMAS–CONICET and Departamento de Matemática FCEN, Universidad de Buenos
Aires, Pab. I – Ciudad Universitaria (1428), Buenos Aires – Argentina
E-mail address: `lvendramin@dm.uba.ar`