THE RETRACTION RELATION FOR BIRACKS

PŘEMYSL JEDLIČKA, AGATA PILITOWSKA, AND ANNA ZAMOJSKA-DZIENIO

Abstract. In [9] Etingof, Schedler and Soloviev introduced, for each non-degenerate involutive set-theoretical solution (X, σ, τ) of the Yang-Baxter equation, the equivalence relation $\sim$ defined on the set X and they considered a new non-degenerate involutive induced *retraction* solution defined on the quotient set $X^{\sim}$. It is well known that translating set-theoretical non-degenerate solutions of the Yang-Baxter equation into the universal algebra language we obtain an algebra called a *birack*. In the paper we introduce the *generalized retraction* relation $\approx$ on a birack, which is equal to $\sim$ in an involutive case. We present a complete algebraic proof that the relation $\approx$ is a congruence of the birack. Thus we show that the retraction of a set-theoretical non-degenerate solution is well defined not only in the involutive case but also in the case of all non-involutive solutions.

1. Introduction

The Yang-Baxter equation is a fundamental equation occurring in integrable models in statistical mechanics and quantum field theory [14]. Let V be a vector space. A *solution of the Yang–Baxter equation* is a linear mapping $r : V \otimes V \to V \otimes V$ such that

$$(id \otimes r)(r \otimes id)(id \otimes r) = (r \otimes id)(id \otimes r)(r \otimes id).$$

Description of all possible solutions seems to be extremely difficult and therefore there were some simplifications introduced (see e.g. [6]).

Let X be a basis of the space V and let $\sigma : X^2 \to X$ and $\tau : X^2 \to X$ be two mappings. We say that (X, σ, τ) is a *set-theoretical solution of the Yang–Baxter equation* if the mapping $x \otimes y \mapsto \sigma(x, y) \otimes \tau(x, y)$ extends to a solution of the Yang–Baxter equation. It means that $r\colon X^2 \to X^2$, where $r = (\sigma, \tau)$ satisfies the *braid relation*:

$$(id \times r)(r \times id)(id \times r) = (r \times id)(id \times r)(r \times id). \tag{1.1}$$

A solution is called *non-degenerate* if the mappings $\sigma(x, \_)$ and $\tau(\_, y)$ are bijections, for all $x, y \in X$. A solution (X, σ, τ) is *involutive* if $r^2 = \mathrm{id}_{X^2}$, and it is *square free* if $r(x, x) = (x, x)$, for every $x \in X$.

Convention 1.1. All solutions we study in this paper are set-theoretical and non-degenerate, so we will call them simply *solutions*. The set X can be of arbitrary cardinality. We investigate both involutive and non-involutive solutions.

It is known (see e.g. [23, 12, 5]) that there is a one-to-one correspondence between (involutive) solutions of the Yang-Baxter equation and (involutive) *biracks* $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ – algebras which have a structure of two one-sided quasigroups $(X, \circ, \backslash_\circ)$ and $(X, \bullet, /_\bullet)$ and satisfy some additional identities (2.3)–(2.5). This fact allows one to characterize solutions of the Yang-Baxter equation applying the universal algebra tools.

Date: January 17, 2019.

2010 *Mathematics Subject Classification.* Primary: 16T25, 08A30. Secondary: 20N02, 08A62, 03C05.

Key words and phrases. Yang-Baxter equation, set-theoretical solution, retraction of a solution, one-sided quasigroup, birack, congruence of an algebra.

In [9] Etingof, Schedler and Soloviev introduced, for each involutive solution (X, σ, τ), the equivalence relation $\sim$ on the set X: for each $x, y \in X$

$$x \sim y \quad \Leftrightarrow \quad \tau(\_, x) = \tau(\_, y).$$

Using properties of the *structure group* $G(X, r) := \langle X \mid xy = \sigma(x, y)\tau(x, y)\ \forall x, y \in X \rangle$ of a solution (X, σ, τ) they argued that there was a natural induced involutive solution, called the *retraction* of (X, σ, τ), defined on the quotient set $X^{\sim}$. Just recently, Lebed and Vendramin considered in [15, Lemma 7.4] for finite *invertible* solutions (which generalize the involutive ones by replacing the condition $(\sigma, \tau)^2 = \mathrm{id}_{X^2}$ by the assumption that (σ, τ) is a bijection), the relation $\sim$ on the set X: for each $x, y \in X$

$$x \sim y \quad \Leftrightarrow \quad \sigma(x, \_) = \sigma(y, \_) \quad \text{and} \quad \tau(\_, x) = \tau(\_, y).$$

They showed that in this case the mapping r also induces a solution on the quotient set $X^{\sim}$.

In the language of biracks the fact that the induced solution is well defined on the quotient set simply means that the relation $\sim$ is a congruence of the corresponding involutive birack. According to our knowledge, the direct proof of this fact was not presented anywhere.

In the paper we introduce the *generalized retraction* relation $\approx$ on a birack $(X, \circ, \backslash_{\circ}, \bullet, /_{\bullet})$: for each $x, y \in X$

$$x \approx y \Leftrightarrow \text{ for each } z \in X:\ x \circ z = y \circ z \text{ and } z \bullet x = z \bullet y, \tag{1.2}$$

and we present a complete algebraic proof that the relation $\approx$ is a congruence of the birack (Theorem 3.3). This fact generalizes the results of Etingof et al. and Lebed and Vendramin.

We also show in Subsection 4.1 that in involutive biracks the generalized retraction relation $\approx$ is equal to the relation $\sim$. Hereby our result confirms that the relation $\sim$ is a congruence of the corresponding involutive birack. What is interesting, our proofs are formulated in a pure universal algebra language and we do not need a structure group of the solution at all. In Section 4 we give short and direct proofs in this manner of some results presented by Etingof et al. in [9] or Rump in [20].

But we obtain even more. We show that the retraction of a solution is well defined also in the case of a non-involutive solution which means that the generalized retraction relation allows to study a new class of non-involutive solutions.

The paper is organized as follows. In Section 2 we recall details of the connection between (involutive) biracks and (involutive) solutions of the Yang-Baxter equation to make the paper self-contained. In Section 3 we introduce the generalized retraction relation on a birack and prove that it is a congruence of it. Theorem 3.3 is the main result of the paper. The proof of the theorem was found using the automated deduction software Prover9 [16]. Finally, in Section 4 we define the retraction of an arbitrary solution. We also show that the retraction relation plays an important role in different algebraic constructions, not only for biracks.

2. Biracks and solutions of the Yang-Baxter equation

Let X be a non-empty set and $*\colon X^2 \to X$ be a binary operation. In universal algebra, a pair $(X, *)$ is called a *groupoid* (or a *binar*, a *binary algebra*, a *magma*). In this paper we will also consider algebraic structures with a few binary operations defined on a set X.

Given a groupoid $(X, *)$ and an element $x \in X$, one can define two mappings: a *left translation* by x and a *right translation* by x, respectively:

$$L_x\colon X \to X;\ a \mapsto x * a \quad \text{and} \quad R_x\colon X \to X:\ a \mapsto a * x.$$

Definition 2.1. A groupoid $(X, *)$ is a *quasigroup* if L_x and R_x are bijections, for each $x \in X$.

In particular, this means that, for every $x, y \in X$, the equations $x * u = y$ and $u * x = y$ have unique solutions in X. One may then define on X two additional operations:

$$x\backslash y := L_x^{-1}(y), \quad \text{and} \quad x/y := R_y^{-1}(x)$$

of *left division* and *right division*, respectively and consider the quasigroup as an algebra $(X, *, \backslash, /)$ with three binary operations satisfying for every $x, y \in X$ the following conditions:

$$x * (x\backslash y) = y, \quad x\backslash(x * y) = y, \tag{2.1}$$

$$(y/x) * x = y, \quad (y * x)/x = y. \tag{2.2}$$

For example, every group $(G, \cdot)$ can be made into a quasigroup $(G, *, \backslash, /)$ by taking $x * y = x \cdot y$, $x\backslash y = x \cdot y^{-1}$ and $x/y = x^{-1} \cdot y$.

A quasigroup $(X, *)$ may be seen as a generalization of a group — the operation $*$ can be non-associative but its multiplication table, for a finite set X, is a *latin square*, that means in every row as well as in every column, each element appears exactly once. These algebras are widely studied and have many interesting applications, e.g. in cryptography, see [1, 18, 21].

When studying quasigroups, one usually works with the permutation group generated by L_x and R_x. This group is called the *multiplication* group of X and denoted by $\mathrm{Mlt}(X)$.

If all left translations in a groupoid $(X, *)$ are bijections then the algebra is called a *left quasigroup*. A *right quasigroup* is defined analogously. In one-sided quasigroups only one-sided multiplication groups are considered, that means $\mathrm{LMlt}(X) = \langle L_x : \ x \in X \rangle$ for left quasigroups and $\mathrm{RMlt}(X) = \langle R_x : \ x \in X \rangle$ for right ones.

One can regard a left quasigroup $(X, *)$ as an algebra $(X, *, \backslash)$ with two binary operations satisfying (2.1) and right quasigroup $(X, *)$ as an algebra $(X, *, /)$ satisfying (2.2). It is obvious that $(X, \backslash, *)$ is also a left quasigroup and $(X, /, *)$ is a right quasigroup. However, even if we consider a one-sided quasigroup as an algebra with one basic binary operation, the second binary operation is implicitly present here anyway. There is an important reason for this — it is well-known that the homomorphic image of a (one-sided) quasigroup defined with a single binary operation, need not be a (one-sided) quasigroup, see, e.g., [20, Example 1]. And our aim is to study a quotient of an algebraic structure with (one-sided) quasigroup operations. Roughly speaking, the class $\mathcal{A}$ of algebraic structures (of a given signature) is closed under the formation of homomorphic images if $\mathcal{A}$ is defined by a set of equations (famous Birkhoff's Theorem or **HSP** Theorem).

A groupoid $(X, *)$ is *idempotent* if, for every $x \in X$,

$$L_x(x) = x,$$

or equivalently, if for every $x \in X$,

$$x * x = x.$$

In a left quasigroup $(X, *, \backslash)$, the groupoid $(X, *)$ is idempotent if and only if $(X, \backslash)$ is idempotent. In this case we say that $(X, *, \backslash)$ is idempotent.

Example 2.2. Let $(A, \cdot)$ be a group, $c \in A$ be a fixed element and f, g be two mutually inverse group automorphisms. Then algebraic structure $(A, *, \backslash)$ with operations defined as follows

$$x * y = x \cdot f(y \cdot x^{-1}) \cdot c,$$
$$x\backslash y = g(y \cdot x^{-1}) \cdot g(c^{-1}) \cdot x,$$

where x^{-1} is an inverse element to x, is a left quasigroup. If c is a neutral element in A, then $(A, *, \backslash)$ is idempotent.

Example 2.3. Let $X = \{1, 2, \dots, n\}$ be a finite set and let π_i for $i = 1, 2, \dots n$ be its permutations (they needn't be different). Define on X the operations

$$m * k = \pi_m(k),$$
$$m\backslash k = \pi_m^{-1}(k).$$

Then $(X, *, \backslash)$ is a left quasigroup, and it is idempotent if and only if, for each $m \in X$, $\pi_m(m) = m$.

Biracks are algebras that appear in low-dimensional topology. They are associated with a link diagram and they are invariant (up to isomorphism) under the generalized Reidemeister moves for virtual knots and links. On the other hand, they provide solutions to the Yang-Baxter equation [10]. The equational definition of a birack we use here was given first in [23].

Definition 2.4. An algebra $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ with four binary operations is called a *birack*, if $(X, \circ, \backslash_\circ)$ is a left quasigroup, $(X, \bullet, /_\bullet)$ is a right quasigroup and the following holds for any $x, y, z \in X$:

$$x \circ (y \circ z) = (x \circ y) \circ ((x \bullet y) \circ z), \tag{2.3}$$
$$(x \circ y) \bullet ((x \bullet y) \circ z) = (x \bullet (y \circ z)) \circ (y \bullet z), \tag{2.4}$$
$$(x \bullet y) \bullet z = (x \bullet (y \circ z)) \bullet (y \bullet z). \tag{2.5}$$

A birack is *idempotent* if both one-sided quasigroups $(X, \circ, \backslash_\circ)$ and $(X, \bullet, /_\bullet)$ are idempotent. And it is *involutive* if it additionally satisfies for every $x, y \in X$:

$$(x \circ y) \circ (x \bullet y) = x \quad \Leftrightarrow \quad x \bullet y = (x \circ y)\backslash_\circ x, \tag{2.6}$$
$$(x \circ y) \bullet (x \bullet y) = y \quad \Leftrightarrow \quad x \circ y = y/_\bullet(x \bullet y). \tag{2.7}$$

The identities (2.6) and (2.7) are equivalent to another ones regarded by Rump [20, Definition 1] (see (2.9) and (2.10) below, and [5, Definition 1.6.]), namely:

$$(x \circ y) \circ (x \bullet y) = x \quad \Leftrightarrow \quad x \bullet y = (x \circ y)\backslash_\circ x \quad \Leftrightarrow \quad x = ((x \circ y)\backslash_\circ x)/_\bullet y \overset{(2.1)}{\Leftrightarrow}$$
$$x = ((x \circ y)\backslash_\circ x)/_\bullet(x\backslash_\circ(x \circ y)). \tag{2.8}$$

Now, substituting y by $x\backslash_\circ y$ in (2.8), one obtains

$$(y\backslash_\circ x)/_\bullet(x\backslash_\circ y) = x. \tag{2.9}$$

On the other side, substitution of y by $x \circ y$ in (2.9), gives (2.8). Similarly,

$$(x \circ y) \bullet (x \bullet y) = y \quad \Leftrightarrow \quad x \circ y = y/_\bullet(x \bullet y) \quad \Leftrightarrow$$
$$x\backslash_\circ(y/_\bullet(x \bullet y)) = y \quad \Leftrightarrow \quad ((x \bullet y)/_\bullet y)\backslash_\circ(y/_\bullet(x \bullet y)) = y \quad \Leftrightarrow$$
$$(x/_\bullet y)\backslash_\circ(y/_\bullet x) = y. \tag{2.10}$$

Taking $y = x$ in (2.9) and (2.10) we obtain that in an involutive birack for every $x \in X$ holds:

$$(x\backslash_\circ x)/_\bullet(x\backslash_\circ x) = x \quad \text{and} \quad (x/_\bullet x)\backslash_\circ(x/_\bullet x) = x, \tag{2.11}$$

which means that each involutive birack is a *biquandle* (see [10]). Stanovský proved [23, Lemma] that the identities (2.11) are equivalent in any birack.

In particular, the conditions (2.11) imply that in an involutive birack $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ the mappings

$$T\colon X \to X; \quad x \mapsto x\backslash_\circ x, \tag{2.12}$$

and

$$S\colon X \to X; \quad x \mapsto x/_\bullet x \tag{2.13}$$

are mutually inverse bijections. Recall that Etingof et al. in [9, Proposition 1.4] and Rump in [20, Proposition 2] obtained the same results but using the properties of the structure group for an involutive solution.

Now we are ready to translate the constrain of a solution (X, σ, τ) of the Yang-Baxter equation into the language of the universal algebra. For sake of simplicity let denote $\sigma(x, y)$ by $x \circ y$ and $\tau(x, y)$ by $x \bullet y$. Then

$$r(x, y) = (\sigma(x, y), \tau(x, y)) = (x \circ y, x \bullet y) = (L_x(y), \boldsymbol{R}_y(x)),$$

where for each $s \in X$, $L_s \colon X \to X$ is the left translation with respect to the operation $\circ$, and $\boldsymbol{R}_s \colon X \to X$ is the right translation with respect to the operation $\bullet$.

This justifies the replacement of the notion (X, σ, τ), for a solution of the Yang-Baxter equation, by $(X, L, \boldsymbol{R})$, where $L \colon X \to X^X$; $x \mapsto L_x$ and $\boldsymbol{R} \colon X \to X^X$; $x \mapsto \boldsymbol{R}_x$. On the other hand, we can treat a solution $(X, L, \boldsymbol{R})$ as an algebra $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ with four binary operations defined on the set X.

Using this notation, the braid relation (1.1) implies that in the algebra $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ the conditions (2.3)–(2.5) hold (see [5, 23]).

Furthermore, the assumption that a solution $(X, L, \boldsymbol{R})$ is non-degenerate gives that, for every $s \in X$, the mappings L_s and $\boldsymbol{R}_s$ are invertible. Hence simply, $(X, \circ, \backslash_\circ)$ is a left quasigroup with $x \backslash_\circ y := L_x^{-1}(y)$ and $(X, \bullet, /_\bullet)$ is a right quasigroup with $x /_\bullet y := \boldsymbol{R}_y^{-1}(x)$.

Finally, a solution $(X, L, \boldsymbol{R})$ is involutive if $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ satisfies (2.6) and (2.7), and it is square free if both one-sided quasigroups $(X, \circ, \backslash_\circ)$ and $(X, \bullet, /_\bullet)$ are idempotent.

Hence, each (involutive) solution of the Yang-Baxter equation yields an (involutive) birack.

The converse is also true.

Theorem 2.5. [5, Lemma 1.2] *If $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ is an (involutive) birack, then defining $r(x, y) = (x \circ y, x \bullet y)$ we obtain an (involutive) solution of the Yang-Baxter equation.*

By Theorem 2.5 there is a one-to-one correspondence between (involutive) solutions of the Yang-Baxter equation and (involutive) biracks.

Example 2.6 (Lyubashenko, see [6])**.** Let X be a non-empty set and let $x \circ y = f(y)$, $x \bullet y = g(x)$, where $f, g \colon X \to X$. Then conditions (2.3)–(2.5) are satisfied if and only if $fg = gf$. If f and g are bijections, we can define two additional binary operations $x \backslash_\circ y = f^{-1}(y)$, $x /_\bullet y = g^{-1}(x)$. The algebra $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ is a birack which is involutive if and only if $g = f^{-1}$.

Such involutive birack corresponds to a solution which is called a *permutation solution*. If $f = g = id$, the birack is called a *projection* one and the corresponding solution is called *trivial*.

By Theorem 2.5 we can see that not only involutive biracks are biquandles. By results of Smoktunowicz and Vendramin [22, Corollary 3.3] biracks corresponding to solutions of the Yang-Baxter equation which originate from *skew braces* are biquandles. Moreover, by observation of Lebed and Vendramin [15, Lemma 1.4] any finite birack corresponding to an *injective* solution (the canonical mapping $i \colon X \to G(X, r)$; $x \mapsto x$ is an injection) is a biquandle, too.

Clearly, all involutive solutions are injective.

Many explicit examples of biracks can be found in [2, 7, 17]. We use some of them, translating them into the notion used in this paper.

Example 2.7. [17, Example 10] Consider a set $X = \{1, 2, 3, 4\}$ with permutations $L_1 = \boldsymbol{R}_2 = (12)$, $L_2 = \boldsymbol{R}_1 = (12)(34)$, $L_3 = L_4 = \mathrm{id}$, $\boldsymbol{R}_3 = \boldsymbol{R}_4 = (34)$. Then, one can define operations $\circ$ and $\bullet$: $i \circ j := L_i(j)$ and $i \bullet j := \boldsymbol{R}_j(i)$, similarly as in Example 2.3. In this way, one obtains a birack $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ with the following multiplication tables for operations $\circ$ and $\bullet$ (note that here $\circ = \backslash_\circ$

and $\bullet = /_\bullet$)

$\circ$	1	2	3	4
1	2	1	3	4
2	2	1	4	3
3	1	2	3	4
4	1	2	3	4

$\bullet$	1	2	3	4
1	2	2	1	1
2	1	1	2	2
3	4	3	4	4
4	3	4	3	3

.

This birack is non-idempotent, non-involutive, e.g. $(3 \circ 1) \circ (3 \bullet 1) = 4$, and it is not a biquandle since $(3\backslash_\circ 3)/_\bullet(3\backslash_\circ 3) = (3 \circ 3) \bullet (3 \circ 3) = 3 \bullet 3 = 4$.

3. Generalized retraction congruence

One of the basic notions in general algebra is the one of a *congruence* — an equivalence relation on an algebraic structure compatible with this structure (the operations are well-defined on the equivalence classes). As the Fundamental Homomorphism Theorem (First Isomorphism Theorem) says, for a given algebraic structure its homomorphic images and quotients are exactly the same (up to isomorphism). For details, see any textbook on Universal Algebra e.g. [3, Section 1.5]. In case of biracks, necessary definitions look as follows.

Definition 3.1. An equivalence relation θ on the set X of elements of a birack $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ is a *congruence on* $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ if it is compatible with all four operations of the birack X, i.e. if $x\ \theta\ y$ and $z\ \theta\ t$ then also

$$(x \circ z)\ \theta\ (y \circ t)$$
$$(x\backslash_\circ z)\ \theta\ (y\backslash_\circ t)$$
$$(x \bullet z)\ \theta\ (y \bullet t)$$
$$(x/_\bullet z)\ \theta\ (y/_\bullet t).$$

If θ is a congruence on a birack $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$, then the quotient set $X^\theta = \{x^\theta : x \in X\}$ of the equivalence classes under θ, is again a birack, called the *quotient birack*, under operations defined by

$$x^\theta \circ z^\theta = (x \circ z)^\theta$$
$$x^\theta\backslash_\circ z^\theta = (x\backslash_\circ z)^\theta$$
$$x^\theta \bullet z^\theta = (x \bullet z)^\theta$$
$$x^\theta/_\bullet z^\theta = (x/_\bullet z)^\theta.$$

Definition 3.2. Let $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ be a birack. The equivalence relation $\approx$ defined on X in the following way

$$x \approx y \Leftrightarrow L_x = L_y \text{ and } \boldsymbol{R}_x = \boldsymbol{R}_y \tag{3.1}$$

is called the *generalized retraction*.

Obviously, the condition (3.1) can be formulated equivalently as

$$\forall\, z \in X \quad x \circ z = y \circ z \text{ and } z \bullet x = z \bullet y \tag{3.2}$$

or

$$\forall\, z \in X \quad x\backslash_\circ z = y\backslash_\circ z \text{ and } z/_\bullet x = z/_\bullet y. \tag{3.3}$$

Theorem 3.3. *The generalized retraction is a congruence of a birack* $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$.

Proof. Let a, b, c, d be elements of a birack $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ such that $a \approx b$ and $c \approx d$. Now we show that $L_{a\circ c} = L_{b\circ d}$, $\boldsymbol{R}_{a\circ c} = \boldsymbol{R}_{b\circ d}$, $L_{a\backslash_\circ c} = L_{b\backslash_\circ d}$ and $\boldsymbol{R}_{a\backslash_\circ c} = \boldsymbol{R}_{b\backslash_\circ d}$. We start with a sequence of claims.

For each $x, y, z \in X$ the following hold in a birack:

Claim 1.

$$y \bullet (x\backslash_\circ z) = [(x/_\bullet y) \bullet (y \circ (x\backslash_\circ z))]\backslash_\circ[((x/_\bullet y) \circ y) \bullet z]. \tag{3.4}$$

Proof. We have

$$[(x/_\bullet y) \bullet (y \circ (x\backslash_\circ z))] \circ [y \bullet (x\backslash_\circ z)] \overset{(2.4)}{=} [(x/_\bullet y) \circ y] \bullet [((x/_\bullet y) \bullet y) \circ (x\backslash_\circ z)] \overset{(2.2)}{=}$$
$$= [(x/_\bullet y) \circ y] \bullet [x \circ (x\backslash_\circ z)] \overset{(2.1)}{=} ((x/_\bullet y) \circ y) \bullet z,$$

and Claim 1 is obtained by dividing both sides with $[(x/_\bullet y) \bullet (y \circ (x\backslash_\circ z))]$ from the left. □

Claim 2.

$$y \circ (x\backslash_\circ z) = (x/_\bullet y)\backslash_\circ[((x/_\bullet y) \circ y) \circ z]. \tag{3.5}$$

Proof.

$$(x/_\bullet y) \circ [y \circ (x\backslash_\circ z)] \overset{(2.3)}{=} [(x/_\bullet y) \circ y] \circ [((x/_\bullet y) \bullet y) \circ (x\backslash_\circ z)] \overset{(2.2)}{=}$$
$$= [(x/_\bullet y) \circ y] \circ [x \circ (x\backslash_\circ z)] \overset{(2.1)}{=} ((x/_\bullet y) \circ y) \circ z,$$

and we divide both sides with $(x/_\bullet y)$. □

Claim 3.

$$(x \bullet y) \circ [(x\backslash_\circ z) \bullet ((x\backslash_\circ z)\backslash_\circ y)] = z \bullet [z\backslash_\circ(x \circ y)]. \tag{3.6}$$

Proof.

$$(x \bullet y) \circ [(x\backslash_\circ z) \bullet ((x\backslash_\circ z)\backslash_\circ y)] \overset{(2.1)}{=} [x \bullet ((x\backslash_\circ z) \circ ((x\backslash_\circ z)\backslash_\circ y)] \circ [(x\backslash_\circ z) \bullet ((x\backslash_\circ z)\backslash_\circ y)] \overset{(2.4)}{=}$$
$$= [x \circ (x\backslash_\circ z)] \bullet [(x \bullet (x\backslash_\circ z)) \circ ((x\backslash_\circ z)\backslash_\circ y)] \overset{(2.1)}{=} z \bullet [(x \bullet (x\backslash_\circ z)) \circ ((x\backslash_\circ z)\backslash_\circ y)] \overset{(2.3)}{=}$$
$$= z \bullet [(x \circ (x\backslash_\circ z))\backslash_\circ(x \circ ((x\backslash_\circ z) \circ ((x\backslash_\circ z)\backslash_\circ y)))] \overset{(2.1)}{=} z \bullet [z\backslash_\circ(x \circ y)],$$

where (2.3) is used in the form $(x \bullet y) \circ z = (x \circ y)\backslash_\circ(x \circ (y \circ z))$. □

Claim 4.

$$x \bullet (x\backslash_\circ c) = x \bullet (x\backslash_\circ d). \tag{3.7}$$

Proof.

$$x \bullet (x\backslash_\circ c) \overset{(3.4)}{=} [(x/_\bullet x) \bullet (x \circ (x\backslash_\circ c))]\backslash_\circ[((x/_\bullet x) \circ x) \bullet c] \overset{(2.1)}{=}$$
$$= [(x/_\bullet x) \bullet c]\backslash_\circ[((x/_\bullet x) \circ x) \bullet c] \overset{(3.2)}{=} [(x/_\bullet x) \bullet d]\backslash_\circ[((x/_\bullet x) \circ x) \bullet d] \overset{(2.1),(3.4)}{=} x \bullet (x\backslash_\circ d).$$ □

Claim 5.

$$z \bullet (z\backslash_\circ(x \circ c)) = z \bullet (z\backslash_\circ(x \circ d)). \tag{3.8}$$

Proof.

$$z \bullet (z\backslash_\circ(x \circ c)) \overset{(3.6)}{=} (x \bullet c) \circ [(x\backslash_\circ z) \bullet ((x\backslash_\circ z)\backslash_\circ c)] \overset{(3.2)}{=}$$
$$= (x \bullet d) \circ [(x\backslash_\circ z) \bullet ((x\backslash_\circ z)\backslash_\circ c)] \overset{(3.7)}{=} (x \bullet d) \circ [(x\backslash_\circ z) \bullet ((x\backslash_\circ z)\backslash_\circ d)] \overset{(3.6)}{=} z \bullet (z\backslash_\circ(x \circ d)).$$ □

Claim 6.

$$(x/_\bullet y)\bullet(y\circ(x\backslash_\circ c))=(x/_\bullet y)\bullet(y\circ(x\backslash_\circ d)). \tag{3.9}$$

Proof.

$$(x/_\bullet y)\bullet(y\circ(x\backslash_\circ c)) \overset{(3.5)}{=} (x/_\bullet y)\bullet[(x/_\bullet y)\backslash_\circ(((x/_\bullet y)\circ y)\circ c)] \overset{(3.8)}{=}$$
$$=(x/_\bullet y)\bullet[(x/_\bullet y)\backslash_\circ(((x/_\bullet y)\circ y)\circ d)] \overset{(3.5)}{=} (x/_\bullet y)\bullet(y\circ(x\backslash_\circ d)). \qquad \square$$

Claim 7.

$$b\circ((a\backslash_\circ z)\circ x)=z\circ((b\bullet(a\backslash_\circ z))\circ x). \tag{3.10}$$

Proof.

$$b\circ((a\backslash_\circ z)\circ x) \overset{(2.3)}{=} (b\circ(a\backslash_\circ z))\circ((b\bullet(a\backslash_\circ z))\circ x) \overset{(3.2)}{=}$$
$$=(a\circ(a\backslash_\circ z))\circ((b\bullet(a\backslash_\circ z))\circ x) \overset{(2.1)}{=} z\circ((b\bullet(a\backslash_\circ z))\circ x). \qquad \square$$

Claim 8.

$$b\bullet(a\backslash_\circ c)=b\bullet(a\backslash_\circ d). \tag{3.11}$$

Proof. By (2.4), the following condition holds

$$y\bullet z=[x\bullet(y\circ z)]\backslash_\circ[(x\circ y)\bullet((x\bullet y)\circ z)]. \tag{3.12}$$

Hence,

$$b\bullet(a\backslash_\circ x) \overset{(3.12)}{=} [(b/_\bullet a)\bullet(b\circ(a\backslash_\circ x))]\backslash_\circ[((b/_\bullet a)\circ b)\bullet(((b/_\bullet a)\bullet b)\circ(a\backslash_\circ x))] \overset{(3.2)}{=}$$
$$=[(b/_\bullet a)\bullet(a\circ(a\backslash_\circ x))]\backslash_\circ[((b/_\bullet a)\circ b)\bullet(((b/_\bullet a)\bullet a)\circ(a\backslash_\circ x))] \overset{(2.1),(2.2)}{=}$$
$$=((b/_\bullet a)\bullet x)\backslash_\circ[((b/_\bullet a)\circ b)\bullet((b\circ(a\backslash_\circ x))] \overset{(3.2)}{=}$$
$$=((b/_\bullet a)\bullet x)\backslash_\circ[((b/_\bullet a)\circ b)\bullet((a\circ(a\backslash_\circ x))] \overset{(2.1)}{=}$$
$$=((b/_\bullet a)\bullet x)\backslash_\circ(((b/_\bullet a)\circ b)\bullet x).$$

Hence,

$$b\bullet(a\backslash_\circ c)=((b/_\bullet a)\bullet c)\backslash_\circ(((b/_\bullet a)\circ b)\bullet c) \overset{(3.2)}{=} ((b/_\bullet a)\bullet d)\backslash_\circ(((b/_\bullet a)\circ b)\bullet d)=b\bullet(a\backslash_\circ d). \qquad \square$$

Summarizing, we obtain

$$L_{a\circ c}(x)=(a\circ c)\circ x \overset{(3.2)}{=} (b\circ c)\circ x \overset{(2.1)}{=}$$
$$(b\circ c)\circ((b\bullet c)\circ((b\bullet c)\backslash_\circ x)) \overset{(2.3)}{=} b\circ(c\circ((b\bullet c)\backslash_\circ x)) \overset{(3.2)}{=}$$
$$=b\circ(d\circ((b\bullet d)\backslash_\circ x)) \overset{(2.3)}{=} (b\circ d)\circ((b\bullet d)\circ((b\bullet d)\backslash_\circ x)) \overset{(2.1)}{=}$$
$$=(b\circ d)\circ x=L_{b\circ d}(x),$$

and

$$\boldsymbol{R}_{a\circ c}(x)=x\bullet(a\circ c) \overset{(3.2)}{=} x\bullet(b\circ c) \overset{(2.5)}{=}$$
$$=((x\bullet b)\bullet c)/_\bullet(b\bullet c) \overset{(3.2)}{=} ((x\bullet b)\bullet d)/_\bullet(b\bullet d) \overset{(2.5)}{=}$$
$$=x\bullet(b\circ d)=\boldsymbol{R}_{b\circ d}(x),$$

which gives that $(a\circ c)\approx(b\circ d)$.

Furthermore, one has

$$\begin{aligned}
&L_b((a\backslash_\circ d)\circ x) = b\circ((a\backslash_\circ d)\circ x) \overset{(3.10)}{=} d\circ((b\bullet(a\backslash_\circ d))\circ x) \overset{(3.2)}{=}\\
&= c\circ((b\bullet(a\backslash_\circ d))\circ x) \overset{(3.11)}{=} c\circ((b\bullet(a\backslash_\circ c))\circ x) \overset{(3.10)}{=}\\
&= b\circ((a\backslash_\circ c)\circ x) = L_b((a\backslash_\circ c)\circ x).
\end{aligned}$$

Since L_b is a bijection, it follows that for each $x\in X$,

$$L_{L_a^{-1}(c)}(x) = L_{a\backslash_\circ c}(x) = (a\backslash_\circ c)\circ x = (a\backslash_\circ d)\circ x = L_{a\backslash_\circ d}(x) = L_{L_a^{-1}(d)}(x). \tag{3.13}$$

Moreover,

$$\begin{aligned}
&y\bullet(x\backslash_\circ c) \overset{(3.4)}{=} [(x/_\bullet y)\bullet(y\circ(x\backslash_\circ c))]\backslash_\circ[((x/_\bullet y)\circ y)\bullet c] \overset{(3.2)}{=}\\
&[(x/_\bullet y)\bullet(y\circ(x\backslash_\circ c))]\backslash_\circ[((x/_\bullet y)\circ y)\bullet d] \overset{(3.9)}{=}\\
&[(x/_\bullet y)\bullet(y\circ(x\backslash_\circ d))]\backslash_\circ[((x/_\bullet y)\circ y)\bullet d] \overset{(3.4)}{=} y\bullet(x\backslash_\circ d).
\end{aligned}$$

Hence, for each $y\in X$

$$\boldsymbol{R}_{L_a^{-1}(c)}(y) = \boldsymbol{R}_{a\backslash_\circ c}(y) = y\bullet(a\backslash_\circ c) = y\bullet(a\backslash_\circ d) = \boldsymbol{R}_{a\backslash_\circ d}(y) = \boldsymbol{R}_{L_a^{-1}(d)}(y). \tag{3.14}$$

By assumption, $L_a^{-1} = L_b^{-1}$. Then one gets

$$L_{a\backslash_\circ c} = L_{L_a^{-1}(c)} \overset{(3.13)}{=} L_{L_a^{-1}(d)} = L_{L_b^{-1}(d)} = L_{b\backslash_\circ d},$$

and

$$\boldsymbol{R}_{a\backslash_\circ c} = \boldsymbol{R}_{L_a^{-1}(c)} \overset{(3.14)}{=} \boldsymbol{R}_{L_a^{-1}(d)} = \boldsymbol{R}_{L_b^{-1}(d)} = \boldsymbol{R}_{b\backslash_\circ d}.$$

This finally implies $(a\backslash_\circ c)\approx(b\backslash_\circ d)$.

The proof $(a\bullet c)\approx(b\bullet d)$ and $(a/_\bullet c)\approx(b/_\bullet d)$, is similar due to the symmetry of the defining identities of a birack.

□

Theorem 3.3 immediately forces that each quotient birack of $(X,\circ,\backslash_\circ,\bullet,/_\bullet)$ satisfies all equational properties of $(X,\circ,\backslash_\circ,\bullet,/_\bullet)$. In particular, if $(X,\circ,\backslash_\circ,\bullet,/_\bullet)$ is involutive (square-free, right cyclic (see (4.5)), etc.) then obviously $(X/_\approx,\circ,\backslash_\circ,\bullet,/_\bullet)$ is involutive (square-free, right cyclic, etc.).

The next example shows that both defining conditions of the relation $\approx$ are essential.

Example 3.4. Let $(X,\circ,\backslash_\circ,\bullet,/_\bullet)$ be a birack on the set $X=\{0,1,2,3,4\}$ with the following multiplication tables for operations $\circ$ and $\bullet$:

$\circ$	0	1	2	3	4
0	0	2	1	4	3
1	0	2	1	4	3
2	4	2	1	3	0
3	4	2	1	3	0
4	3	2	1	0	4

$\bullet$	0	1	2	3	4
0	0	3	3	0	0
1	1	2	2	1	1
2	2	1	1	2	2
3	3	0	0	3	3
4	4	4	4	4	4

.

Clearly, $L_0 = L_1 = (12)(34)$ and $L_2 = L_3 = (04)(12)$, but $\boldsymbol{R}_0 \neq \boldsymbol{R}_1$. In consequence, $L_{0\circ 2} = L_1 \neq L_4 = L_{1\circ 3}$.

Note that the birack in Example 3.4 is not involutive, since e.g. $(0\circ 1)\bullet(0\bullet 1) = 2$. In Section 4 we will discuss behavior of the relation of generalized retraction in the case of an involutive birack.

Example 3.5. In [22, Example 3.9] the authors consider a non-involutive, not square-free birack on the set $X = \{1, 2, \dots, 8\}$ obtained from a skew-brace. Namely, $L_1 = L_6 = \mathrm{id}$, $L_2 = L_5 = (25)(47)$, $L_3 = L_8 = (38)(47)$, $L_4 = L_7 = (25)(38)$ and $\boldsymbol{R}_1 = \boldsymbol{R}_4 = \boldsymbol{R}_6 = \boldsymbol{R}_7 = \mathrm{id}$, $\boldsymbol{R}_2 = \boldsymbol{R}_3 = \boldsymbol{R}_5 = \boldsymbol{R}_8 = (25)(38)$. In particular, $L_i = L_i^{-1}$ and $\boldsymbol{R}_i = \boldsymbol{R}_i^{-1}$ for each $i \in X$. Then, there are 4 equivalence classes of a congruence $\approx$: $\{1, 6\}$, $\{2, 5\}$, $\{3, 8\}$, $\{4, 7\}$. The quotient birack $(X/_{\approx}, \circ, \backslash_\circ, \bullet, /_\bullet)$ is isomorphic to the birack on the set $Y = \{a, b, c, d\}$ with $L_i = \boldsymbol{R}_i = \mathrm{id}$ for each $i \in Y$. The latter birack is both involutive and square-free.

4. Applications to other constructions

Relations closely related to the generalized retraction congruence studied in Section 3 are well established in the literature. They play an important role in different constructions applied to algebraic structures. The aim of this section is to recall some of these congruences, mainly in the context of the solutions of the Yang-Baxter equation. We want to present a unified approach to them in the universal algebra language.

4.1. **The retraction of solutions.** Let (X, σ, τ) be a solution of the Yang-Baxter equation. Etingof et al. in [9, Section 3.2] defined the following relation on the set X

$$x \sim y \quad \Leftrightarrow \quad \tau(\_, x) = \tau(\_, y) \tag{4.1}$$

and showed ([9, Proposition 2.2]) that for an involutive solution

$$\tau(\_, x) = \tau(\_, y) \quad \Leftrightarrow \quad \sigma(x, \_) = \sigma(y, \_).$$

In the language of biracks this means that for an involutive case relations $\approx$ and $\sim$ are equal. Below we present the direct proof of the equivalence

$$L_x = L_y \quad \Leftrightarrow \quad \boldsymbol{R}_x = \boldsymbol{R}_y \tag{4.2}$$

which holds in any involutive birack. The idea is similar to the proof from [9] but we don't use the construction of the structure group which simplifies and shortens the proof.

First, note that if $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ is a birack then directly by (2.3) we have that for every $x, y \in X$

$$L_{x \circ y} L_{x \bullet y} = L_x L_y, \tag{4.3}$$

which is equivalent to

$$L^{-1}_{x \bullet y} L^{-1}_{x \circ y} = L_y^{-1} L_x^{-1}. \tag{4.4}$$

Let $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ be an involutive birack. We show that $L_a^{-1} T = T \boldsymbol{R}_a$ for any $a \in X$, where $T \colon X \to X$ is an invertible mapping defined by (2.12). Indeed,

$$L_a^{-1} T(c) = L_a^{-1} L_c^{-1}(c) \overset{(4.4)}{=} L^{-1}_{c \bullet a} L^{-1}_{c \circ a}(c) \overset{(2.7)}{=} L^{-1}_{c \bullet a} \boldsymbol{R}_a(c) = L^{-1}_{\boldsymbol{R}_a(c)} \boldsymbol{R}_a(c) = T \boldsymbol{R}_a(c),$$

for any $c \in X$.

Etingof et al., using bijective 1-cocycles defined on the structure group of an involutive solution (X, σ, τ), reasoned that the quotient set $X^\sim$ has a structure of an involutive solution $(X^\sim, \overline{\sigma}, \overline{\tau})$ with $\overline{\sigma}(x^\sim, y^\sim) = \sigma(x, y)^\sim$ and $\overline{\tau}(x^\sim, y^\sim) = \tau(x, y)^\sim$ for $x^\sim, y^\sim \in X^\sim$ and $x \in x^\sim, y \in y^\sim$. They called such solution the *retraction* of (X, σ, τ) and denoted it by $\mathrm{Ret}(X, \sigma, \tau)$.

Now, it is obvious, by Theorem 3.3 and (4.2), that $\sim$ is just a congruence on an involutive birack. Clearly, the birack corresponding to the retraction solution $\mathrm{Ret}(X, \sigma, \tau)$ is the quotient birack $(X^\sim, \circ, \backslash_\circ, \bullet, /_\bullet)$.

Applying the relation (1.2), a similar kind of retraction procedure appeared in [15, Section 7] for finite, non-degenerate, invertible solutions.

Theorem 3.3 directly shows that the retraction of (X, σ, τ) is well defined not only for involutive or invertible solutions. Applying the notion from Section 3 we can naturally extend the definition.

Definition 4.1. Let $(X, L, \boldsymbol{R})$ be a solution of the Yang-Baxter equation. The solution $(X^{\approx}, L, \boldsymbol{R})$ with $L_{x^{\approx}}(y^{\approx}) = L_x(y)^{\approx}$ and $\boldsymbol{R}_{y^{\approx}}(x^{\approx}) = \boldsymbol{R}_y(x)^{\approx}$ for $x^{\approx}, y^{\approx} \in X^{\approx}$ and $x \in x^{\approx}$, $y \in y^{\approx}$ is the *retraction* solution of $(X, L, \boldsymbol{R})$.

Obviously, the birack corresponding to the retraction solution of $(X, L, \boldsymbol{R})$ is equal to the quotient birack $(X^{\approx}, \circ, \backslash_\circ, \bullet, /_\bullet)$.

Among involutive solutions, an important role is played by *multipermutation solutions*, see e.g. [4, 11, 24].

Let (X, σ, τ) be an involutive solution. One defines *iterated retraction* in the following way: $\mathrm{Ret}^0(X, \sigma, \tau) := (X, \sigma, \tau)$ and $\mathrm{Ret}^k(X, \sigma, \tau) := \mathrm{Ret}(\mathrm{Ret}^{k-1}(X, \sigma, \tau))$, for any natural number $k > 1$.

A solution (X, σ, τ) is called a *multipermutation solution of level* m if m is the least nonnegative integer such that

$$|\mathrm{Ret}^m(X, \sigma, \tau)| = 1.$$

In the language of an involutive birack $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ this means that applying m times the congruence $\sim$ to the subsequent quotient biracks, one obtains the one-element birack. By Definition 4.1 one can generalize the notion for non-involutive solutions.

Example 4.2. The solution $(X, L, \boldsymbol{R})$ corresponding to a birack given in Example 3.5 is a non-involutive multipermutation solution of level 2. In [22, Example 4.18.] the skew-brace which produces this solution is said to have a *finite multipermutation level*.

4.2. **Cycle sets.** In [20] Rump showed that there is a correspondence between involutive solutions of the Yang-Baxter equation and *non-degenerate cycle sets*.

Definition 4.3. [20] A groupoid $(X, \odot)$ is a *cycle set* if all left multiplications are invertible and the equation

$$(x \odot y) \odot (x \odot z) = (y \odot x) \odot (y \odot z) \tag{4.5}$$

holds for all $x, y, z \in X$. A cycle set is *non-degenerate* if

$$\text{the mapping} \quad T\colon X \to X; \quad x \mapsto x \odot x \quad \text{is a bijection.} \tag{4.6}$$

It follows that each cycle set can be regarded as a left quasigroup $(X, \odot, \backslash_\odot)$ which satisfies *right cyclic law* (4.5) with respect to the first operation — this law can be also formulated in the form $L_{x\odot y}L_x = L_{y\odot x}L_y$. If $(X, \odot, \backslash_\odot)$ satisfies both (4.5) and (4.6) with respect to the first operation, we call it a *non-degenerate right cyclic* left-quasigroup.

Let a birack $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ be involutive. Then by (4.3), (2.6) and (2.1) we obtain for every $x, y \in X$

$$L_{x\circ y}L_{(x\circ y)\backslash_\circ x} = L_xL_y \quad \Leftrightarrow \quad L_xL_{x\backslash_\circ y} = L_yL_{y\backslash_\circ x},$$

substituting y by $x\backslash_\circ y$ for $\Rightarrow$, and y by $x \circ y$ for $\Leftarrow$. Since

$$L_xL_{x\backslash_\circ y} = L_yL_{y\backslash_\circ x} \quad \Leftrightarrow \quad L^{-1}_{x\backslash_\circ y}L^{-1}_x = L^{-1}_{y\backslash_\circ x}L^{-1}_y,$$

one obtains that for every $x, y, z \in X$

$$(x\backslash_\circ y)\backslash_\circ(x\backslash_\circ z) = (y\backslash_\circ x)\backslash_\circ(y\backslash_\circ z).$$

Recall that the mapping T defined by (2.12) is a bijection in an involutive birack. Therefore, $(X, \backslash_\circ, \circ)$ is a non-degenerate right cyclic left quasigroup (compare to [20, Proposition 1]).

It is also true that each non-degenerate right cyclic left quasigroup $(X, \backslash, *)$ determines an involutive birack. (Note that here $(X, \backslash)$ is a cycle set.) Introducing the second operation $*$ into the type (which plays the role of left division of $\backslash$, i.e. $*$ is also a left-quasigroup operation but not necessarily right cyclic), one can formulate the result in the language of right cyclic left quasigroups $(X, \backslash, *)$ and involutive biracks.

Theorem 4.4. [20, Proposition 2], [5, Proposition 1.5] *Let $(X, \backslash, *)$ be a non-degenerate right cyclic left quasigroup. Then defining $x \circ y = x * y$, $x \backslash_\circ y = x \backslash y$, $x \bullet y = (x * y) \backslash x$, and $x /_\bullet y = z$, where z is the unique one such that $z \backslash z = y * (x \backslash x)$, the algebra $(X, \circ, \backslash_\circ, \bullet, /_\bullet)$ is an involutive birack.*

Hence, finding all involutive solutions of the Yang-Baxter equation is equivalent to constructing all non-degenerate right cyclic left quasigroups.

Example 4.5. Let $X = \{1, 2, 3, 4\}$ and let $\backslash$ be the following operation:

$\backslash$	1	2	3	4
1	3	4	2	1
2	3	4	2	1
3	4	3	1	2
4	4	3	1	2

The groupoid $(X, \backslash)$ is a cycle set satisfying (4.6) and the corresponding involutive solution $(X, L, \boldsymbol{R})$ is $L_1 = L_2 = \boldsymbol{R}_1 = \boldsymbol{R}_2 = (1423)$ and $L_3 = L_4 = \boldsymbol{R}_3 = \boldsymbol{R}_4 = (1324)$.

Example 4.6. Let $(A, +)$ be an abelian group and f its automorphism. By $(\mathrm{id} - f)$ we denote the endomorphism of $(A, +)$ defined by $x \mapsto x - f(x)$. Assume that $(\mathrm{id} - f)$ is nilpotent of degree 2 and $c \in \mathrm{Ker}(\mathrm{id} - f)$. Then $(A, \backslash, *)$ with

$$x \backslash y = (\mathrm{id} - f)(x) + f(y) + c \ \text{ and } \ x * y = f^{-1}(y - (\mathrm{id} - f)(x) - c)$$

is a non-degenerate right cyclic left quasigroup. Since in this case, $f - \mathrm{id} = \mathrm{id} - f^{-1}$, we obtain that $(A, \circ, \backslash_\circ, \bullet, /_\bullet)$, with $x \circ y = (\mathrm{id} - f)(x) + f(y) + c$ and $x \bullet y = f^{-1}(x) + (\mathrm{id} - f^{-1})(y) - f^{-1}(c)$, is an involutive birack.

Rump showed in [20, Theorem 2] that each finite cycle set is non-degenerate. He introduced the notion of a *cycle group* and used its properties to obtain this result. Actually, he proved a stronger result than this; if we are interested in finite cycle sets only, we can present a short and direct proof based on the properties of finite one-sided quasigroups. It is evident (see e.g. [19, Section 8.6.]) that each finite left quasigroup has a finite left multiplication group and therefore, taking $k = |\mathrm{LMlt}(X)|$, we have, for $x, y \in X$,

$$L_x^{-k}(y) = \underbrace{x \backslash (x \backslash (x \ldots \backslash (x}_{k-\text{times}} \backslash y) \ldots)) = y,$$

or equivalently

$$L_x^{k}(y) = \underbrace{x * (x * (x \ldots * (x}_{k-\text{times}} * y) \ldots)) = y.$$

Due to above properties one can consider finite one-sided quasigroups as algebras with one basic binary operation e.g. of multiplication $*$, the operation $\backslash$ is defined then by means of multiplication: $x \backslash y = L_x^{k-1}(y)$.

Moreover, by (2.1) and (4.5), the following holds for x, y in a right cyclic left quasigroup $(X, \backslash, *)$:

$$x \backslash (y \backslash y) = (y \backslash (y * x)) \backslash (y \backslash y) = ((y * x) \backslash y) \backslash ((y * x) \backslash y). \tag{4.7}$$

(Compare to [20, Lemma 1]). Equivalently, the condition (4.7) can be stated that in a right cyclic left quasigroup $(X, \backslash, *)$, for each $x, y \in X$, there exists an element $a \in X$ such that $x \backslash (y \backslash y) = a \backslash a$. In particular, the latter holds for $y = x$.

Proposition 4.7. [20, Theorem 2] *Each finite right cyclic left quasigroup is non-degenerate.*

Proof. Let $(X, \backslash, *)$ be a finite right cyclic left quasigroup. We will show that the mapping $T\colon X \to X; x \mapsto x\backslash x$ is a surjection. Let $z \in X$ and $k = |\mathrm{LMlt}(X)| > 2$,

$$z = L_z^{-k}(z) = L_z^{-k+2}(z\backslash(z\backslash z)) = L_z^{-k+2}(u_1\backslash u_1) = L_z^{-k+3}(z\backslash(u_1\backslash u_1)) = \ldots = u_{k-2}\backslash u_{k-2} = T(u_{k-2}),$$

where u_i, for $i = 1, \ldots, k-2$, is an element of X defined as in (4.7). For $k \leq 2$ the result is immediate. □

Rump also proved ([20, Lemma 2]) that, for any cycle set $(X, \backslash)$, the relation $\alpha \subseteq X \times X$

$$x \;\alpha\; y \quad \Leftrightarrow \quad \forall z \in X \; x\backslash z = y\backslash z \tag{4.8}$$

is a congruence of $(X, \backslash)$. In the proof, Rump used an assumption that for each $x \in X$, the mapping $a \mapsto x\backslash a$ is a surjection. Again, introducing the operation $*$ into the type, one can present an alternative proof in the language of right cyclic left quasigroups $(X, \backslash, *)$.

Let $x, x', y, y', z \in X$ and $x \;\alpha\; x'$ and $y \;\alpha\; y'$. This means that $x\backslash z = x'\backslash z$ and $y\backslash z = y'\backslash z$ for every $z \in X$. Then by (2.1) and right-cyclic law we have

$$(x\backslash y)\backslash z = (x\backslash y)\backslash(x\backslash(x{*}z)) = (y\backslash x)\backslash(y\backslash(x{*}z)) = (y'\backslash x)\backslash(y'\backslash(x{*}z)) = (x\backslash y')\backslash(x\backslash(x{*}z)) = (x'\backslash y')\backslash z.$$

Hence, $x\backslash y \;\alpha\; x'\backslash y'$.

But the quotient $(X^\alpha, \backslash)$ is again a cycle set only if a cycle set $(X, \backslash)$ was non-degenerate, (see [20, Example 1, Proposition 10]). The reason for this is that in general, for an arbitrary right cyclic left quasigroup $(X, \backslash, *)$, the relation α does not need to be a congruence of $(X, *)$.

But, by Theorem 4.4, the additional condition (4.6) guarantees that the left quasigroup $(X, \backslash, *)$ defines the right quasigroup on X as well. We denote the latter by $(X, /, \cdot)$. Note that the operation $/$ is called *dual* to $\backslash$ in [20, Definition 1], and the algebra $(X, \backslash, /)$ is called *RLC-system* in [5, Definition 1.6]. Moreover, $(X, /)$ is a *left-cyclic* right quasigroup and operations $\backslash$ and $/$ are connected by (2.9) and (2.10) (substituting $\backslash_\circ$ by $\backslash$ and $/_\bullet$ by $/$). This is equivalent to the fact that the mapping $S\colon X \to X; x \mapsto x/x$ is the inverse of T and (4.2) holds. It follows that the relation α is a congruence of the algebra $(X, /)$, too.

In the involutive birack $(X, *, \backslash, \cdot, /)$, the conditions (2.6), (4.7) and (2.11) imply

$$y \cdot x = (y * x)\backslash y = [((y * x)\backslash y)\backslash((y * x)\backslash y)]/[((y * x)\backslash y)\backslash((y * x)\backslash y)] = [x\backslash(y\backslash y)]/[x\backslash(y\backslash y)].$$

Since by (2.7), $x{*}y = y/(x{\cdot}y)$, we obtain that the operations of the right multiplication $\cdot$ and the left multiplication $*$ of an involutive birack are expressed by the operations of the left $\backslash$ and right $/$ divisions. Since α is a congruence with respect to divisions, the relation α is also a congruence due to the additional operation $*$. This exactly means that satisfying the condition (4.6) by a right cyclic left quasigroup $(X, \backslash, *)$ is sufficient for the relation α to be a congruence of $(X, \backslash, *)$.

4.3. **Groupoid modes.** Romanowska and Smith investigated in [19, Section 8.4] *groupoid modes* – idempotent and medial groupoids. A groupoid $(X, *)$ is *medial* if, for every $x, y, z, t \in X$,

$$(x * y) * (z * t) = (x * z) * (y * t) \quad \Leftrightarrow \quad L_{x*y}L_z = L_{x*z}L_y.$$

For each natural number k they defined the following equivalence relation on a mode $(X, *)$. For $a, b \in X$,

$$a\varrho_k b \quad \Leftrightarrow \quad \forall x \in X \; ax^k := (((a * \underbrace{x) * x) * \ldots) * x}_{k-\text{times}} = (((b * \underbrace{x) * x) * \ldots) * x}_{k-\text{times}} =: bx^k.$$

They proved that each of the relations ϱ_k is a congruence of any mode $(A, *)$. Clearly, $\varrho_1 = \sim$.

They also showed that each ϱ_k-class $(a^{\varrho_k}, *)$ is k-reductive. A groupoid $(X, *)$ is *k-reductive* if for every $x, y \in X$,

$$xy^k = y. \tag{4.9}$$

1-reductive groupoid is usually called a *right zero (right trivial) semigroup or a* (right) projection groupoid. Romanowska and Smith proved that if a mode $(X, *)$ is n-reductive then the congruences ϱ_k form an increasing chain of relations

$$id_X = \varrho_0 \leq \varrho_1 \leq \ldots \leq \varrho_{n-1} \leq \varrho_n = X \times X.$$

Additionally, if $k < n$ then a quotient $(A^{\varrho_k}, *)$ is $(n-k)$-reductive. This means ([19, Theorem 5.7.4]) that the variety of n-reductive binary modes coincides with the Mal'cev product of the varieties of k-reductive and $(n-k)$-reductive groupoid modes. In particular, this gives a recursive method of constructing n-reductive binary modes from right zero semigroups.

4.4. **The strong retraction.** Cedó, Jespers and Okniński introduced in [4] a stronger version of retractability of an involutive solution (X, σ, τ). They defined a relation ρ on X as follows:

$$x \rho y \quad \Leftrightarrow \quad L_x = L_y \quad \text{and} \quad x \text{ and } y \text{ are in the same orbit under the action of } \mathrm{LMlt}(X) \text{ on } X.$$

The *strong retraction* of (X, σ, τ) is taken then as the induced solution $(X^\rho, \overline{\sigma}, \overline{\tau})$. Cedo et al. applied the relation ρ to solve a problem of Gateva-Ivanova and showed that each involutive square free solution of the Yang-Baxter equation with abelian left multiplication group $\mathrm{LMlt}(X)$ is strongly retractable [4, Corollary 2.9].

In particular, they showed [4, Theorem 2.5] that in a non trivial involutive square free solution (X, σ, τ) with abelian left multiplication group $\mathrm{LMlt}(X)$, there exists an orbit X_k, under the action of $\mathrm{LMlt}(X)$ on X, with at least two different elements $x, y \in X_k$ such that $x \sim y$.

Independently, in [13, Definition 6.3] a quandle with such property of orbits was called *quasi-reductive*. Recall, an idempotent left quasigroup $(X, *, \backslash_*)$ is called a *quandle* if it is *left distributive*, i.e. for every $x, y, z \in X$

$$L_x(y * z) = L_x(y) * L_x(z) \quad \Leftrightarrow \quad x * (y * z) = (x * y) * (x * z).$$

Note that quandles are closely related to solutions of the Yang-Baxter equation — any injective derived solution is a quandle [8]. In knot theory biquandles were introduced as generalization of quandles.

Jedlička, Pilitowska and Zamojska-Dzienio in [13] classified subdirectly irreducible medial quandles. A quandle is *subdirectly irreducible* if and only if the intersection of all its non-trivial congruences, called the *monolith congruence*, is non-trivial. In particular, they showed [13, Main Theorem 6.4] that every subdirectly irreducible medial quandle with more than two elements is either a quasigroup or it is quasi-reductive. In finite case this characterization is even more readable since a subdirectly irreducible finite medial quandle is either quasigroup or it is k-reductive for some natural k. For reductive case, the congruence ρ plays the role of the monolith. However, the group $\mathrm{LMlt}(X)$ for a quandle, needn't be abelian.

References

[1] V. D. Belousov, *Fundamentals of the theory of quasigroups and loops*, (Russian), Nauka, Moskva (1967).

[2] A. Bartholomew, R. Fenn, *Biquandles of small size and some invariants of virtual and welded knots*, J. Knot Theory Ramifications **20/7** (2011) 943—954; erratum: J. Knot Theory Ramifications **26/8** (2017) 1792002 (11 pages).

[3] C. Bergman, *Universal algebra: Fundamentals and selected topics*, Chapman & Hall/CRC Press, 2011.

[4] F. Cedó, E. Jespers, J. Okniński, *Retractability of set theoretic solutions of the Yang-Baxter equation*, Adv. Math. **224** (2010), 2472–2484.

[5] P. Dehornoy, *Set-theoretic solutions of the Yang-Baxter equation, RC-calculus, and Garside germs*, Adv. Math. **282** (2015), 93–127.

[6] V. G. Drinfeld, *On some unsolved problems in quantum group theory*, Quantum groups (Leningrad, 1990), 1992, pp. 1.8.
[7] M. Elhamdadi, S. Nelson, *Quandles: An introduction to the algebra of knots*, American Mathematical Society, Providence, 2015.
[8] P. Etingof, A. Soloviev, R. Guralnick, *Indecomposable set-theoretical solutions to the quantum Yang-Baxter equation on a set with a prime number of elements*, J. Algebra **242** (2001), no. **2**, 709–719.
[9] P. Etingof, T. Schedler, A. Soloviev, *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. **100** (1999), 169–209.
[10] R. Fenn, M. Jordan-Santana, L. Kauffman, *Biquandles and virtual links*, Topology and its Appl. **145** (2004), 157–175.
[11] T. Gateva-Ivanova, P. Cameron, *Multipermutation solutions of the Yang-Baxter equation*, Commun. Math. Phys. **309** (2012), 583—621.
[12] T. Gateva-Ivanova, S. Majid, *Matched pairs approach to set theoretic solutions of the Yang-Baxter equation*, J. Algebra **319** (2008), 1462–1529.
[13] P. Jedlička, A. Pilitowska, A. Zamojska-Dzienio, *Subdirectly irreducible medial quandles*, Comm. Algebra **46** (2018), 4803–4829.
[14] M. Jimbo, *Introduction to the Yang-Baxter equation*, Int. J. Modern Physics A, 4-15 (1989), 3759–3777.
[15] V. Lebed, L. Vendramin, *On structure groups of set-theoretical solutions to the Yang-Baxter equation*, available at `https://arxiv.org/pdf/1707.00633`, accepted in Proc. Edinburgh Math. Soc.
[16] W. W. McCune, *Prover9 and Mace4,* `http://www.cs.unm.edu/~mccune/prover9/`, 2005–2010.
[17] S. Nelson, *Link invariants from finite biracks*, Banach Center Publ. **100**, Polish Acad. Sci. Inst. Math., Warsaw (2014), 197–212.
[18] H.O. Pflugfelder, *Quasigroups and Loops: Introduction*, Heldermann Verlag, Berlin, 1990.
[19] A. Romanowska, J.D.H. Smith, *Modes*, World Scientific, 2002.
[20] W. Rump, *A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation*, Adv. Math. **193** (2005), 40–55.
[21] V.A. Shcherbacov, *Elements of Quasigroup Theory and Applications*, Chapman & Hall/CRC Press, 2017.
[22] A. Smoktunowicz, L. Vendramin, *On skew braces* (with an appendix by N. Byott and L. Vendramin), J. Comb. Algebra **2** (2018), 47—86.
[23] D. Stanovský, *On axioms of biquandles*, J. Knot Theory Ramifications **15/7** (2006) 931–933.
[24] L. Vendramin, *Extensions of set-theoretic solutions of the Yang-Baxter equation and a conjecture of Gateva-Ivanova*, J. Pure Appl. Algebra **220** (2016), 2064—2076.

(P.J.) Department of Mathematics, Faculty of Engineering, Czech University of Life Sciences, Kamýcká 129, 16521 Praha 6, Czech Republic

(A.P., A.Z.) Faculty of Mathematics and Information Science, Warsaw University of Technology, Koszykowa 75, 00-662 Warsaw, Poland

Email address: `(P.J.) jedlickap@tf.czu.cz`
Email address: `(A.P.) A.Pilitowska@mini.pw.edu.pl`
Email address: `(A.Z.) A.Zamojska-Dzienio@mini.pw.edu.pl`