Advances in Group Theory and Applications
© 2019 AGTA - www.advgrouptheory.com/journal
7 (2019), pp. 15–37
ISSN: 2499-1287
DOI: 10.32037/agta-2019-003

Problems on Skew Left Braces *

Leandro Vendramin

(*Received Aug. 7, 2018; Accepted Sep. 5, 2018 — Communicated by E. Jespers*)

Abstract

Braces were introduced by Rump as a generalization of Jacobson radical rings. It turns out that braces allow us to use ring-theoretic and group-theoretic methods for studying involutive solutions to the Yang–Baxter equation. If braces are replaced by skew braces, then one can use similar methods for studying not necessarily involutive solutions. Here we collect problems related to (skew) braces and set-theoretic solutions to the Yang-Baxter equation.

Mathematics Subject Classification (2010): 16T25, 81R50

Keywords: brace; skew brace; Yang-Baxter equation; radical ring; nil ring; regular subgroup; circle algebra

1 Introduction

In this paper I propose several problems in the theory of skew braces. I hope that these problems will help to strengthen the interest in the theory of skew braces and set-theoretic solutions to the Yang-Baxter equation. I have not attempted to review the general theory. I do not discuss problems related to homology of solutions (see [48]), semibraces (see [19]) or trusses (see [12]). I concentrate only on skew braces and the Yang-Baxter equation.

* This work is supported by PICT-2481-0147 and MATH-AmSud 17MATH-01. The author thanks F. Cedó, T. Gateva-Ivanova, E. Jespers, V. Lebed, K. Nejabati Zenouz, J. Okniński, A. Smoktunowicz, W. Rump, P. Zadunaisky for discussions, comments and problems.

In §9 of [32], Drinfeld wrote that maybe it would be interesting to study set-theoretical solutions to the equation

$$R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12}, \tag{1.1}$$

where X is a set, $R\colon X \times X \to X \times X$ and R_{ij} is the map acting like R on the two factors i and j and leaving the third factor alone. Writing $r = \tau \circ R$, where τ is the map $(x, y) \mapsto (y, x)$, Equation (1.1) becomes

$$r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23}, \tag{1.2}$$

where $r_{12} = r \times \mathrm{id}$ and $r_{23} = \mathrm{id} \times r$.

Let us say that a pair (X, r) is a *set-theoretic solution* to the Yang-Baxter equation (YBE) if X is a non-empty set and $r\colon X \times X \to X \times X$ is a bijective map satisfying (1.2). If (X, r) is a solution of the YBE we write

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

We say that the solution (X, r) is *involutive* if $r^2 = \mathrm{id}_{X\times X}$ and *non-degenerate* if $\sigma_x \in \mathbb{S}_X$ and $\tau_x \in \mathbb{S}_X$ for all $x \in X$, where $\mathbb{S}_X$ denotes the group of bijective maps $X \to X$. By convention, our *solutions* will always be non-degenerate solutions.

One tool to study set-theoretic solutions to the YBE is the theory of skew left braces. Braces were introduced by Rump in [59]. For a recent survey on braces we refer to [21]. Skew braces appeared later in [43]. A *skew left brace* is a triple $(A, +, \circ)$, where $(A, +)$ and $(A, \circ)$ are groups (not necessarily abelian) such that

$$a \circ (b + c) = a \circ b - a + a \circ c \tag{1.3}$$

for all $a, b, c \in A$. To define skew right braces one needs to replace (1.3) by

$$(a + b) \circ c = a \circ c - c + b \circ c. \tag{1.4}$$

The inverse of an element $a \in A$ with respect to the circle (or multiplicative) group of A will be denoted by a'. Examples of skew left braces can be found in [2],[25],[43],[61].

A skew *two-sided* brace is a skew left brace that is also a skew right brace with respect to the same pair of operations.

If $\mathcal{X}$ is a class of groups, a skew left brace will be called of type $\mathcal{X}$ if its additive group belongs to $\mathcal{X}$. Skew left braces of abelian type are those braces introduced by Rump in [59]. By convention, a *left brace* will always be a skew left brace of abelian type, i.e. with abelian additive group.

Braces and skew left braces have several interesting connections, see for example [61] and [67]. The connection between skew left braces and non-degenerate solutions of the YBE is given in the following theorem (see Theorem 3.1 of [43]):

Theorem *If A is a skew left brace, then the map*

$$r_A \colon A \times A \to A \times A, \quad r_A(a,b) = (-a + a \circ b, (-a + a \circ b)' \circ a \circ b),$$

is a non-degenerate set-theoretic solution of the YBE. Moreover, r_A is involutive if and only if A is of abelian type.

Solutions produced from skew left braces are universal. In a different language, one finds the following result in [36],[50],[68]:

Theorem *If (X,r) be a solution of the YBE, then there exists a unique skew left brace structure over the group*

$$G = G(X,r) = \langle X : x \circ y = u \circ v \text{ whenever } r(x,y) = (u,v) \rangle$$

such that the diagram

$$\begin{tikzcd} X \times X \arrow[r, "r"] \arrow[d, "\iota \times \iota"'] & X \times X \arrow[d, "\iota \times \iota"] \\ G \times G \arrow[r, "r_G"] & G \times G \end{tikzcd}$$

commutes, where $\iota \colon X \to G(X,r)$ is the canonical map.

One proves that the pair $(G(X,r), \iota)$ satisfies a universal property (see Proposition 3.9 of [43] and Theorem 3.5 of [67]). The group $G(X,r)$ is infinite since for example the degree map $X \to \mathbb{Z}$, $x \mapsto 1$, extends to a group homomorphism $G(X,r) \to \mathbb{Z}$. Several properties of $G(X,r)$ are discussed in [45]. If the set X of the solution (X,r) is finite, then one can realize this solution using a finite skew left brace (see [4] and [25]).

2 Problems

It was observed by Rump in [57] that non-degenerate involutive solutions are in bijective correspondence with non-degenerate cycle sets. A *cycle set* is a pair $(X, \cdot)$, where

$$X \times X \to X,\ (x, y) \mapsto x \cdot y,$$

is a map such that each $\varphi_x \colon X \to X$, $y \mapsto x \cdot y$, is bijective, and

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

for all $x, y, z \in X$.

A cycle set $(X, \cdot)$ is said to be *non-degenerate* if the map

$$x \mapsto x \cdot x$$

is bijective. Finite cycle sets are non-degenerate (see Theorem 2 of [57]). The correspondence between non-degenerate cycle sets and involutive solutions is given by

$$r(x, y) = ((y * x) \cdot y, y * x)$$

where $x * y = z$ if and only if $x \cdot z = y$. Homomorphisms of cycle sets are defined in the usual manner.

Problem 2.1 *Construct the free cycle set.*

It would be interesting to have a nice description of the free cycle set. This nice description could be used for example to compute homology.

In [36], Etingof, Schedler and Soloviev constructed all non-degenerate involutive solutions of cardinality $\leqslant 8$, see Table 2.1. To construct finite involutive solutions one needs to construct finite cycle sets.

Table 2.1: Involutive non-degenerate solutions of cardinality $\leqslant 8$

cardinality	1	2	3	4	5	6	7	8
solutions	1	2	5	23	88	595	3456	34528
square-free	1	1	2	5	17	68	336	2041
indecomposable	1	1	1	5	1	10	1	98

Problem 2.2 *Construct all cycle sets of small cardinality.*

One can try for example with the construction of cycle sets of cardinality nine. Of course Problem 2.2 refers to the construction of all isomorphism classes of cycle sets. It would also be interesting to construct all cycle sets (or involutive solutions) of small cardinality under particular assumptions. For example, a solution (X, r) of the YBE is said to be *square free* if $r(x, x) = (x, x)$ for all $x \in X$, this means that one needs cycle sets $(X, \cdot)$ such that $x \cdot x = x$ for all $x \in X$.

Problem 2.3 *Construct all square-free cycle sets of small cardinality.*

An involutive solution (X, r) is said to be *indecomposable* if the group $\mathcal{G}(X, r)$ defined as the subgroup of $\mathbb{S}_X$ generated by $\{\sigma_x : x \in X\}$ acts transitively on X. Similarly one defines indecomposable cycle sets. The classification of indecomposable solutions with a prime number of elements appears in [35] and [37].

Problem 2.4 *Construct all indecomposable cycle sets of small cardinality.*

Maybe Problems 2.2–2.4 and similar problems could be studied using constraint satisfaction methods.

The number of finite involutive solutions increases rapidly with the number of elements of the underlying set. Therefore it makes sense to ask for an estimation:

Problem 2.5 *Estimate the number of cycle sets of cardinality n for $n \to \infty$.*

Much less is known for non-involutive solutions. Before going into the general problem of constructing non-involutive solutions, one could start with injective solutions. A solution (X, r) is said to be *injective* if the canonical map $X \to G(X, r)$ is injective. As it was proved in [36], involutive solutions are always injective:

$$\{\text{involutive solutions}\} \subsetneq \{\text{injective solutions}\} \subsetneq \{\text{solutions}\}.$$

Problem 2.6 *Construct all injective non-involutive solutions of small cardinality.*

Problem 2.7 *Construct all solutions of small cardinality.*

Problem 2.7 is related to the construction of finite biquandles of small cardinality, see for example [10] and [38]. A different approach to construct all solutions could be based on skew left braces, see [4]; this method requires the classification of finite skew left braces.

Simple involutive solutions were defined in §2 of [69]. A surjective map

$$p\colon X \to Y$$

of involutive solutions is said to be a *covering* if all the fibers $p^{-1}(y)$ have the same cardinality. A covering $X \to Y$ is said to be *trivial* if either $|Y| = 1$ or $|Y| = |X|$. An involutive solution (X, r) is said to be *simple* if $|X| > 1$ and any covering $X \to Y$ is trivial.

Problem 2.8 *Classify finite simple involutive solutions.*

One could simply ask for examples of small involutive simple solutions:

Problem 2.9 *Construct finite simple involutive solutions of small cardinality.*

It would be interesting to understand the simplicity of an involutive solution in the language of left braces:

Problem 2.10 *Is it possible to read off the simplicity of an involutive solution* (X, r) *in terms of the left brace* $G(X, r)$*?*

It would be also interesting to develop the theory of non-involutive simple solutions. Some ideas could be obtained if one reads off the simplicity of a solution in terms of a skew left brace where it is realized.

Problem 2.11 *Let* (X, r) *be a solution to the YBE. When does the multiplicative group of* $G(X, r)$ *have torsion?*

Problem 2.11 was posed by Bachiller in [4]. Gateva-Ivanova and Van den Bergh proved in [42] that in the case of involutive solutions the multiplicative group of $G(X, r)$ is always torsion-free. It is easy to construct examples of non-involutive solutions (X, r) such that the multiplicative group of $G(X, r)$ has torsion.

Problem 2.12 *Construct the free (skew) left brace.*

Based on the work of Bachiller [3] and Catino and Rizzo [20] on regular subgroups, an algorithm to construct finite skew left braces was introduced in [43]. With some exceptions, this algorithm was used to construct small (skew) left braces. For $n \in \mathbb{N}$ let $s(n)$ be the number of non-isomorphic skew left braces of size n and let $b(n)$ be the number of non-isomorphic left braces of size n. Table 2.2 shows some values of $s(n)$ and $b(n)$ and several open cases. Maybe some of these open cases are fairly straightforward computational projects.

Table 2.2: The number of non-isomorphic left braces and skew left braces.

n	1	2	3	4	5	6	7	8	9	10	11	12
$b(n)$	1	1	1	4	1	2	1	27	4	2	1	10
$s(n)$	1	1	1	4	1	6	1	47	4	6	1	38
n	13	14	15	16	17	18	19	20	21	22	23	24
$b(n)$	1	2	1	357	1	8	1	11	2	2	1	96
$s(n)$	1	6	1	1605	1	49	1	43	8	6	1	855
n	25	26	27	28	29	30	31	32	33	34	35	36
$b(n)$	4	2	37	9	1	4	1	?	1	2	1	46
$s(n)$	4	6	101	29	1	36	1	?	1	6	1	400
n	37	38	39	40	41	42	43	44	45	46	47	48
$b(n)$	1	2	2	106	1	6	1	9	4	2	1	1708
$s(n)$	1	6	8	944	1	78	1	29	4	6	1	66209
n	49	50	51	52	53	54	55	56	57	58	59	60
$b(n)$	4	8	1	11	1	80	2	91	2	2	1	28
$s(n)$	4	51	1	43	1	?	12	815	2	6	1	418
n	61	62	63	64	65	66	67	68	69	70	71	72
$b(n)$	1	2	11	?	1	4	1	11	1	4	1	489
$s(n)$	1	6	11	?	1	36	1	43	1	36	1	17790
n	73	74	75	76	77	78	79	80	81	82	83	84
$b(n)$	1	2	5	9	1	6	1	1985	?	2	1	34
$s(n)$	1	6	14	29	1	78	1	?	?	6	1	606
n	85	86	87	88	89	90	91	92	93	94	95	96
$b(n)$	1	2	1	90	1	16	1	9	2	2	1	?
$s(n)$	1	6	1	800	1	294	1	29	8	6	1	?
n	97	98	99	100	101	102	103	104	105	106	107	108
$b(n)$	1	8	4	51	1	4	1	106	2	2	1	494
$s(n)$	1	53	4	711	1	36	1	944	8	6	1	?
n	109	110	111	112	113	114	115	116	117	118	119	120
$b(n)$	1	6	2	1671	1	6	1	11	11	2	1	395
$s(n)$	1	94	8	?	1	78	1	43	47	6	1	?
n	121	122	123	124	125	126	127	128	129	130	131	132
$b(n)$	4	2	1	9	49	36	1	?	2	4	1	24
$s(n)$	4	6	1	29	213	990	1	?	8	36	1	324
n	133	134	135	136	137	138	139	140	141	142	143	144
$b(n)$	1	2	37	108	1	4	1	27	1	2	1	?
$s(n)$	1	6	101	?	1	36	1	395	1	6	1	?
n	145	146	147	148	149	150	151	152	153	154	155	156
$b(n)$	1	2	9	11	1	19	1	90	4	4	2	40
$s(n)$	1	6	123	43	1	401	1	?	4	36	12	782
n	157	158	159	160	161	162	163	164	165	166	167	168
$b(n)$	1	2	1	?	1	?	1	11	2	2	1	443
$s(n)$	1	6	1	?	1	?	1	43	12	6	1	?

Problem 2.13 *Construct all left braces of size* 32.

Some results related to Problem 2.13 are shown in Table 2.3. According to these results, one needs to construct left braces of size 32 with additive group isomorphic to

$$C_2^5 = C_2 \times C_2 \times C_2 \times C_2 \times C_2,$$

where C_2 denotes the cyclic (multiplicative) group with two elements. Apparently, this particular case cannot be done in reasonable time with the techniques of [43]. The number of (skew) left braces of size 64, 96 or 128 seems to be extremely large and our computational methods are not strong enough to construct them all.

Table 2.3: Some calculations of braces of size 32.

additive group	number	time needed
C_{32}	9	0.1
$C_8 \times C_4$	1334	4 hours
$C_{16} \times C_2$	120	30 minutes
$C_4^2 \times C_2$	13512	13 days
$C_8 \times C_2^2$	1547	10 hours

Problem 2.14 *Let* p *be a prime number. Classify skew left braces of size* p^n.

Problem 2.14 is important because is the key step in the classification of skew left braces of nilpotent type.

Left braces of size p^2 and p^3, where p is a prime number, were classified by Bachiller in [2]. He proved that

$$b(p^2) = 4 \quad \text{and } b(p^3) = 6p + 19.$$

Since groups of order p^2 are abelian, it follows that $s(p^2) = 4$. Skew left braces of size p^3 were classified by Nejabati Zenouz in [52]. He proved that

$$s(p^3) = 6p^2 + 8p + 23$$

whenever $p > 3$. From Table 2.2 one gets $s(8) = 47$ and $s(27) = 101$.

Problem 2.15 *Let* p *and* q *be different prime numbers. Construct all skew left braces of size* pq.

It should be fairly easy to solve Problem 2.15 using the techniques of [14].

Problem 2.16 *Let* p *and* q *be different prime numbers. Consruct all skew left braces of size* p^2q.

Left braces of size p^2q for prime numbers p and q such that $q>p+1$ were classified by Dietzel in [31]. He proved that

$$b(4q) = \begin{cases} 9 & \text{if } 4 \nmid q-1, \\ 11 & \text{if } 4 \mid q-1, \end{cases}$$

if $q > 3$, and that

$$b(p^2q) = \begin{cases} 4 & \text{if } p \nmid q-1, \\ p+8 & \text{if } p \mid q-1 \text{ and } p^2 \nmid q-1, \\ 2p+8 & \text{if } p^2 \mid q-1, \end{cases}$$

if $q > p+1 > 3$.

Problem 2.17 *Estimate the number of (skew) left braces of size* n *for* $n \to \infty$.

The following problem appears in [21]:

Problem 2.18 *Compute automorphism groups of skew left braces of size* p^n.

Automorphism groups of skew left braces of size p^3 were computed in [53].

In 2.28 (I) of [39], Gateva-Ivanova made the following conjecture: for each finite involutive square-free solution (X, r) there exist $x, y \in X$ such that $x \neq y$ and $\sigma_x = \sigma_y$. It was proved by Cedó, Jespers and Okniński in [24] that the conjecture is true if the group $\mathcal{G}(X, r)$ generated by $\{\sigma_x : x \in X\}$ is abelian. Later in [41] and in [25] it was shown using other methods that the result is also valid if $\mathcal{G}(X, r)$ is infinite abelian. In full generality, the conjecture is now known to be false. The first counterexample appeared in [69]; other counterexamples were later constructed in [6] and [17]. It would be interesting to find essentially new counterexamples.

Problem 2.19 *Construct counterexamples to Gateva-Ivanova conjecture.*

One could ask, for example, for counterexamples of size nine. Computer calculations show that there is only one counterexample to Gateva-Ivanova conjecture among the 38698 involutive solutions of size $\leqslant 8$. It could be enlightening to attack Problem 2.19 using the theory of braces. Let A be a brace and X be a subset of A such that the restriction

$$r_X = r_A|_{X \times X}$$

of r_A to $X \times X$ is a solution to the YBE. We say that (A, X) is a *Gateva-Ivanova pair* if the solution (X, r_X) is a counterexample to Gateva-Ivanova conjecture.

Problem 2.20 *Find Gateva-Ivanova pairs.*

One could start studying Problem 2.20 by inspecting the database of small braces. I should remark that counterexamples to Gateva-Ivanova conjecture might provide new examples of Artin-Schelter regular algebras with global dimension > 3 with interesting properties to study. Gateva-Ivanova conjecture motivated a deeper study of the structure of braces and related objects (see, for example, [25],[40], [59]).

Gateva-Ivanova conjecture is of course related with the retractability of involutive solutions, introduced in [36]. For an involutive solution (X, r), consider the equivalence relation on X given by $x \sim y$ if and only if $\sigma_x = \sigma_y$. Denoting by Y the set of equivalence classes of X, the map r induces a function

$$\bar{r}\colon Y \times Y \to Y \times Y.$$

The pair $(Y, \bar{r})$ is a solution to the YBE which will be denoted by $\operatorname{Ret}(X, r)$. One defines inductively

$$\operatorname{Ret}^{m+1}(X, r) = \operatorname{Ret}(\operatorname{Ret}^m(X, r))$$

for all $m \geqslant 1$. The solution (X, r) is said to be a *multipermutation solution* if there is a positive integer m such that $\operatorname{Ret}^m(X, r)$ has only one element. The solution (X, r) is said to be *irretractable* if

$$\operatorname{Ret}(X, r) = (X, r).$$

A group G admits a *left ordering* if it admits a total ordering $<$ such that if $x < y$ then $zx < zy$ for all $x, y, z \in G$. In [9] it is proved that a finite involutive set-theoretic solution (X,r) of the YBE is a multipermutation solution if and only if its structure group $G(X,r)$ admits a left ordering. One of the implications was proved in [30] and [44].

Problem 2.21 *Let* (X,r) *be an injective non-involutive solution of the YBE. When does the multiplicative group of* $G(X,r)$ *admit a left ordering?*

Problem 2.21 appears in [49].

A group G satisfies the *unique product property* if for every finite non-empty subsets A and B of G there is an element x which can be written uniquely as $x = ab$ with $a \in A$ and $b \in B$.

Problem 2.22 *Let* (X,r) *be an involutive irretractable solution of the YBE. Can* $G(X,r)$ *satisfy the unique product property?*

In Example 8.2.14 of [45], Jespers and Oknińksi proved that the structure group $G(X,r)$ of a certain involutive irretractable solution (X,r) of cardinality four does not satisfy the unique product property. They showed that this structure group contains a subgroup isomorphic to the celebrated Promislow group [56].

A group G is said to be *diffuse* if for every finite non-empty subset A of G there exists $a \in A$ such that for all $g \in G \setminus \{1\}$, either $ga \notin A$ or $g^{-1}a \notin A$. Diffuse groups satisfy the unique product property. However, the precise relation between diffuseness and unique products is not clear at the moment. In [49] it is proved that the structure group $G(X,r)$ of an involutive solution (X,r) is diffuse if and only if (X,r) is a multipermutation solution. Therefore a positive answer to Problem 2.22 would give an example of a non-diffuse group with the unique product property.

Problem 2.23 *Study non-involutive multipermutation solutions.*

Some work related to Problem 2.23 can be found in [49] and [67].

As it was observed by Rump, two-sided braces are equivalent to radical rings. The multiplication of this radical ring is the operation

$$a * b = -a + a \circ b - b.$$

It makes sense to consider this operation for all skew left braces, although in general it will not be associative. The following problem appears in [22].

Problem 2.24 *Let A be a left brace such that the operation $*$ is associative. Is A a two-sided brace?*

It is proved in Proposition 2.2 of [22] that the answer is positive if the additive group of the left brace has no elements of order two. For skew braces, Problem 2.24 can be answered in the negative (see §1 of [46]).

A *left ideal* of a skew left brace A is a subgroup L of the additive group of A such that $A * L \subseteq L$. An *ideal* of A is a left ideal I such that

$$a + I = I + a \quad \text{and} \quad a \circ I = I \circ a$$

for all $a \in A$. A skew left brace A is said to be *simple* if it has no ideals different from $\{0\}$ and A.

Problem 2.25 *Classify finite simple skew left braces.*

Problem 2.25 is intensively studied for finite left braces (see for example [5],[8],[7]). However, not much is known about finite simple skew left braces that are not of abelian type.

Problem 2.26 *Study representation theory of skew left braces.*

Rump defined modules over right braces in [58].

Left braces such that either the additive or the multiplicative group is isomorphic to $\mathbb{Z}$ were classified in [28]. It is not clear how to extend some of these results to skew left braces. The operations

$$g^k + g^l = g^{k+(-1)^k l} \quad \text{and} \quad g^k \circ g^l = g^{k+l}$$

turn the set $\{g^k : k \in \mathbb{Z}\}$ into a skew left brace with multiplicative group isomorphic to $\mathbb{Z}$ and additive group isomorphic to the infinite dihedral group. It seems that there are no other non-trivial skew left braces with multiplicative group isomorphic to $\mathbb{Z}$.

Problem 2.27 *Classify isomorphism classes of skew left braces with multiplicative group isomorphic to $\mathbb{Z}$.*

Problem 2.27 could be studied using techniques from factorizable groups (see for example [1]). Similarly one could also ask for the classification of skew left braces where one of its groups is isomorphic to the infinite dihedral group.

Finite skew left braces with cyclic additive groups were classified by Rump in [60] and [62]. In the same vein, it would be interesting to know the classification of skew left braces with multiplicative group isomorphic to the quaternion group. This problem is not even solved for left braces. Such left braces are called *quaternion left braces*. For $m \in \mathbb{N}$ let $q(4m)$ be the number of isomorphism classes of quaternion left braces of size $4m$.

Problem 2.28 *Prove that*

$$q(4m) = \begin{cases} 2 & \text{if } m \text{ is odd,} \\ 7 & \text{if } m \equiv 0 \bmod 8, \\ 9 & \text{if } m \equiv 4 \bmod 8, \\ 6 & \text{if } m \equiv 2 \bmod 8 \text{ or } m \equiv 6 \bmod 8. \end{cases}$$

The conjectural formula for $q(4m)$ of Problem 2.28 was verified by computer for all $m \leqslant 128$.

Problem 2.29 *Which finite abelian groups appear as the additive group of a quaternion left brace?*

For $m \in \{2, \dots, 128\}$ the additive group of a quaternion left brace of order $4m$ is isomorphic to one of the following groups:

$$C_{4m},\ C_{2m} \times C_2,\ C_m \times C_2 \times C_2,\ C_m \times C_4,\ C_{m/2} \times C_2 \times C_2 \times C_2.$$

By inspection, $C_m \times C_2^2$ appears if $m \equiv 2, 4, 6 \bmod 8$ and $C_m \times C_4$ and $C_{m/2} \times C_2^3$ appear if $m \equiv 4 \bmod 8$.

Problem 2.30 *Is it true that there are seven classes of isomorphism of quaternion left braces of size 2^k for $k > 4$?*

It is interesting to study properties of groups appearing as the multiplicative groups of skew left braces. Let us start with the case of left braces. A finite group G is said to be an *involutive Yang-Baxter* group (or simply a IYB group) if it is isomorphic to the multiplicative group of a finite left brace. In [36], Etingof, Schedler and Soloviev proved that IYB groups are always solvable. A natural problem arises: Is every finite solvable group the multiplicative group of a left brace? The answer is negative, as it was shown by Bachiller (see [3]) following the ideas of Rump (see [61]). However, it would be interesting to find other counterexamples.

Problem 2.31 *Which is the minimal cardinality of a solvable group that is not a IYB group?*

Some results related to IYB-groups can be found in [11],[23],[25],[26],[33]. Related problems are the following ones.

Problem 2.32 *Is every nilpotent group of nilpotecy class two the multiplicative group of a left brace?*

Problem 2.33 *Is every nilpotent group of nilpotecy class two the multiplicative group of a two-sided brace?*

Problem 2.34 *Which finite nilpotent groups are multiplicative groups of a two-sided (or left) brace?*

Problems 2.32–2.34 appeared in the survey [21]. Problem 2.34 is interesting even in the particular case of groups of nilpotency class $\leqslant 3$.

I learned the following related problem from Rump.

Problem 2.35 *Is there an example of a non-IYB finite group where all the Sylow subgroups are IYB groups?*

The solution to the YBE one obtains from a skew left brace is always a biquandle. Biquandles are non-associative structures useful in combinatorial knot theory. We refer to [34],[54],[55] for nice introductions to the subject.

Problem 2.36 *Study knot invariants produced from skew left braces.*

As biquandles produce combinatorial knot invariants and these invariants can be strengthened by using quandle and biquandle homology, it is then natural to ask if the homology of braces of [47] can be used in combinatorial knot theory.

Problem 2.37 *Is it possible to strengthen invariants produced from skew left braces by using brace homology?*

Left and right nilpotent left (and right) braces were defined by Rump in [59]. Strongly nilpotent left braces were defined by Smoktunowicz in [65]. These definitions extend to skew left braces, see [28]. A skew brace A is said to be *left nilpotent* if there exists $n \geqslant 1$ such that $A^n = 0$, where

$$A^1 = A \quad \text{and} \quad A^{n+1}$$

is defined as the subgroup $A * A^n$ of $(A, +)$ generated by

$$\{a * x : a \in A, x \in A^n\}.$$

Similarly A is said to be *right nilpotent* if there exists $n \geqslant 1$ such that $A^{(n)} = 0$, where

$$A^{(1)} = A \quad \text{and} \quad A^{(n+1)}$$

is defined as the subgroup $A^{(n)} * A$ of $(A, +)$ generated by

$$\{x * a : x \in A^{(n)}, a \in A\}.$$

The following problem of Smoktunowicz appears in [64] in an equivalent formulation.

Problem 2.38 *Let* G *be a finite group which is the multiplicative group of some left brace. Is* G *is the multipicative group of a right nilpotent left brace?*

Problem 2.38 also makes sense for skew left braces of nilpotent type.

Problem 2.39 *Are there simple two-sided skew braces of nilpotent type?*

A skew brace A is said to be *prime* if for all non-zero ideals I and J, the subgroup $I * J$ of $(A, +)$ generated by $\{u * v : u \in I, v \in J\}$ is non-zero.

Problem 2.40 *Is every finite prime skew left brace of nilpotent type a simple skew left brace?*

Problem 2.41 *Is every finite prime left brace a simple left brace?*

In §5 of [27], Cedó, Jespers and Okniński found a prime non-simple finite left brace. This example solves Problems 2.40 and 2.41.

Problem 2.42 *Are there prime two-sided skew braces of nilpotent type?*

A skew left brace is said to be *strongly nilpotent* if it is right and left nilpotent. A skew left brace A is said to be *strongly nil* if for every element $a \in A$ there is a positive integer $n = n(a)$ such that any $*$-product of n copies of a is zero.

Problem 2.43 *Is every finite strongly nil skew left brace a strongly nilpotent skew left brace?*

For a skew left brace A let $\rho_1(a) = a$ and $\rho_{k+1}(a) = \rho_k(a) * a$ for $n \geqslant 1$. The skew left brace A is said to be *right nil* if there exists a positive integer n such that $\rho_n(a) = 0$ for all $a \in A$.

Problem 2.44 *Is every finite right nil skew left brace a right nilpotent skew left brace?*

Radical rings are the source of several other problems for skew left braces. For example, it might make sense to discuss an analog of the Köthe conjecture in the context of skew left braces. For rings one of the formulations of the conjecture is the following: the sum of two nil left ideals in a ring is a left nil ideal. The conjecture was formulated around 1930 and it is still open (see [29] and [63]).

Problem 2.45 *Is there an analog of the Köthe conjecture for skew left braces?*

Problems 2.39, 2.40, 2.41, 2.42, 2.43 and 2.44 appear in [28] and [46].

Köthe conjecture has been shown to be true for various classes of rings such as polynomial identity rings, right Noetherian rings and radical rings.

Bachiller observed the connection between skew braces and Hopf-Galois extensions. This connection is precisely described in the appendix of [67]. In the theory of Hopf-Galois extensions the following problems are natural, see [16].

Problem 2.46 *Is there a skew left brace with solvable additive group but non-solvable multiplicative group?*

Problem 2.47 *Is there a skew left brace with non-solvable additive group but nilpotent multiplicative group?*

Problems 2.46 and 2.47 also appeared in [67] and Problem 19.90 of [51]. In general, it is interesting to know relations between the multiplicative and the additive group of a skew left brace. Several results in this direction can be found in the theory of Hopf-Galois extensions (see for example [13],[15],[16]). The following problem is mentioned in [49] and Problem 19.49 of [51].

Problem 2.48 *Let A be a skew left brace with left-orderable multiplicative group. Is the additive group of A left-orderable?*

Timur Nasybullov constructed an example of a left brace that answers Problem 2.48 negatively (private communication). Another example that answers Problem 2.48 appears in [28].

In [28] it is proved that skew left braces generated (as a skew left brace) by a single element yield indecomposable solutions of the YBE. It is then natural to ask if all finite indecomposable solutions are of the following type.

Problem 2.49 *Is it true that for each indecomposable involutive solution* (X, r) *there exists a one-generator left brace* A *generated by* x *such that* X *is of the form* $X = \{ax + x : a \in A\}$*?*

Problem 2.49 appears in [66] for left braces.

Rump proved that braces are equivalent to linear cycle sets. A *linear cycle set* is a triple $(A, +, \cdot)$, where $(A, +)$ is an abelian group and $(A, \cdot)$ is a cycle set such that

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{and } (a + b) \cdot c = (a \cdot b) \cdot (a \cdot c)$$

hold for all $a, b, c \in A$.

A theory of dynamical extensions of cycle sets was used in [69] to produce a counterexample to Gateva-Ivanova conjecture.

Problem 2.50 *Develop the theory of dynamical extensions of linear cycle sets.*

To study non-involutive solutions one replaces cycle sets by skew cycle sets. According to §6 of [67], a skew cycle set is defined as a linear cycle set but where the commutativity of the group $(A, +)$ is not assumed. Problem 2.50 can be stated for skew braces and skew cycle sets.

Almost all of the questions for skew left braces make sense in the particular and highly interesting case of k-linear left braces, which are left braces where the additive group is a k-vector space compatible with the multiplicative group. Those braces were introduced by Catino and Rizzo in [20] as *circle algebras*.

There are also several questions on one-generator skew left braces, as those skew left braces are maybe easier to study than skew left braces. In particular, one could also ask most of the previous questions on skew left braces for one-generator skew left braces.

REFERENCES

[1] B. Amberg – S. Franciosi – F. de Giovanni: "Products of Groups", *Clarendon*, Oxford (1992).

[2] D. Bachiller: "Classification of braces of order p^3", *J. Pure Appl. Algebra* 219 (2015), 3568–3603.

[3] D. Bachiller: "Counterexample to a conjecture about braces", *J. Algebra* 453 (2016), 160–176.

[4] D. Bachiller: "Solutions of the Yang-Baxter equation associated to skew left braces, with applications to racks", *J. Knot Theory Ramifications* 27 (2018), n.8, 36pp.

[5] D. Bachiller: "Extensions, matched products, and simple braces", *J. Pure Appl. Algebra* 222 (2018), 1670–1691.

[6] D. Bachiller – F. Cedó – E. Jespers – J. Okniński: "A family of irretractable square-free solutions of the Yang-Baxter equation" *Forum Math.* 29 (2017), 1291–1306.

[7] D. Bachiller – F. Cedó – E. Jespers – J. Okniński: "Iterated matched products of finite braces and simplicity; new solutions of the Yang-Baxter equation", *Trans. Amer. Math. Soc.* 370 (2018), 4881–4907.

[8] D. Bachiller – F. Cedó – E. Jespers – J. Okniński: "Asymmetric product of left braces and simplicity; new solutions of the Yang-Baxter equation", *Commun. Contemp. Math.*, to appear.

[9] D. Bachiller – F. Cedó – L. Vendramin: "A characterization of finite multipermutation solutions of the Yang-Baxter equation", *Publ. Mat.*, 62 (2018), 641–649.

[10] A. Bartholomew – R. Fenn: "Biquandles of small size and some invariants of virtual and welded knots", *J. Knot Theory Ramifications* 20 (2011), 943–954.

[11] N. Ben David – Y. Ginosar: "On groups of I-type and involutive Yang-Baxter groups", *J. Algebra* 458 (2016), 197–206.

[12] T. Brzeziński: "Trusses: between braces and rings", *Trans. Amer. Math. Soc.*, to appear; doi:10.1090/tran/7705.

[13] N.P. Byott: "Hopf-Galois structures on field extensions with simple Galois groups", *Bull. London Math. Soc.* 36 (2004), 23–29.

[14] N.P. Byott: "Hopf-Galois structures on Galois field extensions of degree pq", *J. Pure Appl. Algebra* 188 (2004), 45–57.

[15] N.P. Byott: "Nilpotent and abelian Hopf-Galois structures on field extensions", *J. Algebra* 381 (2013), 131–139.

[16] N.P. Byott: "Solubility criteria for Hopf-Galois structures", *New York J. Math.* 21 (2015), 883–903.

[17] M. Castelli – F. Catino – G. Pinto: "A new family of set-theoretic solutions of the Yang-Baxter equation", *Comm. Algebra* 46 (2018), 1622–1629.

[18] F. Catino – I. Colazzo – P. Stefanelli: "Regular subgroups of the affine group and asymmetric product of radical braces", *J. Algebra* 455 (2016), 164–182.

[19] F. Catino – I. Colazzo – P. Stefanelli: "Semi-braces and the Yang-Baxter equation", *J. Algebra* 483 (2017), 163–187.

[20] F. Catino – R. Rizzo: "Regular subgroups of the affine group and radical circle algebras", *Bull. Austral. Math. Soc.* 79 (2009), 103–107.

[21] F. Cedó: "Left braces: solutions of the Yang-Baxter equation", *Adv. Group Theory Appl.* 5 (2018), 33–90.

[22] F. Cedó – T. Gateva-Ivanova – A. Smoktunowicz: "Braces and symmetric groups with special conditions", *J. Pure Appl. Algebra*, 222 (2018), 3877–3890.

[23] F. Cedó – E. Jespers – Á. del Río: "Involutive Yang-Baxter groups", *Trans. Amer. Math. Soc.* 362 (2010), 2541–2558.

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

[25] F. Cedó – E. Jespers – J. Okniński: "Braces and the Yang-Baxter equation", *Comm. Math. Phys.* 327 (2014), 101–116.

[26] F. Cedó – E. Jespers – J. Okniński: "Nilpotent groups of class three and braces", *Publ. Mat.* 60 (2016), 55–79.

[27] F. Cedó – E. Jespers – J. Okniński: "An abundance of simple left braces with abelian multiplicative Sylow subgroups"; *arXiv*:1807.06408.

[28] F. Cedó – A. Smoktunowicz – L. Vendramin: "Skew left braces of nilpotent type", *Proc. London Math. Soc.*, to appear; doi:10.1112/plms.12209.

[29] M.A. Chebotar – P.H. Lee – E.R. Puczyłowski: "On some questions related to Koethe's nil ideal problem", *Proc. Edinburgh Math. Soc. (2)* 59 (2016), 57–64.

[30] F. Chouraqui: "Left orders in Garside groups", *Int. J. Algebra Comput.* 26 (2016), 1349–1359.

[31] C. Dietzel: "Braces of order p^2q"; *arXiv*:1801.06911.

[32] V.G. Drinfel′d: "On some unsolved problems in quantum group theory" in Quantum groups (Leningrad, 1990), *Lecture Notes in Math.* 1510 (1992), 1–8.

[33] F. Eisele: "On the IYB-property in some solvable groups" *Arch. Math. (Basel)* 101 (2013), 309–318.

[34] M. Elhamdadi – S. Nelson: "Quandles — An Introduction to the Algebra of Knots", *Student Mathematical Library* 74, American Mathematical Society, Providence (2015).

[35] P. Etingof – S. Gelaki – R. Guralnick – J. Saxl: "Biperfect Hopf algebras", *J. Algebra* 232 (2000), 331–335.

[36] P. Etingof – T. Schedler – A. Soloviev: "Set-theoretical solutions to the quantum Yang-Baxter equation", *Duke Math. J.* 100 (1999), 169–209.

[37] 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), 709–719.

[38] R.A. Fenn – A. Bartholomew: "Erratum: Biquandles of small size and some invariants of virtual and welded knots [MR2819176]", *J. Knot Theory Ramifications* 26(8):1792002, 11, 2017.

[39] T. Gateva-Ivanova: "A combinatorial approach to the set-theoretic solutions of the Yang-Baxter equation", *J. Math. Phys.* 45 (2004), 3828–3858.

[40] T. Gateva-Ivanova: "Set-theoretic solutions of the Yang-Baxter equation, braces, and symmetric groups", *Adv. Math.* 338 (2018), 649–701.

[41] T. Gateva-Ivanova – P. Cameron: "Multipermutation solutions of the Yang-Baxter equation", *Comm. Math. Phys.* 309 (2012), 583–621.

[42] T. Gateva-Ivanova – M. Van den Bergh: "Semigroups of I-type", *J. Algebra* 206 (1998), 97–112.

[43] L. Guarnieri – L. Vendramin: "Skew braces and the Yang-Baxter equation", *Math. Comp.* 86 (2017), 2519–2534.

[44] E. Jespers – J. Okniński: "Monoids and groups of I-type", *Alg. Rep. Theory* 8 (2005), 709–729.

[45] E. Jespers – J. Okniński: "Noetherian Semigroup Algebras", Springer, Berlin (2007).

[46] A. Konovalov – A. Smoktunowicz – L. Vendramin: "On skew braces and their ideals", *Exp. Math.*, to appear.

[47] V. Lebed – L. Vendramin: "Cohomology and extensions of braces", *Pacific J. Math.* 284 (2016), 191–212.

[48] V. Lebed – L. Vendramin: "Homology of left non-degenerate set-theoretic solutions to the Yang-Baxter equation", *Adv. Math.* 304 (2017), 1219–1261.

[49] V. Lebed – L. Vendramin: "On structure groups of set-theoretic solutions to the Yang-Baxter equation", *Proc. Edinburgh Math. Soc.*, to appear; doi:10.1017/S0013091518000548.

[50] J.-H. Lu – M. Yan – Y.-C. Zhu: "On the set-theoretical Yang-Baxter equation", *Duke Math. J.* 104 (2000), 1–18.

[51] V.D. Mazurov – E.I. Khukhro (editors): "The Kourovka Notebook — Unsolved Problems in Group Theory", 19th edition (2019).

[52] K. Nejabati Zenouz: "On Hopf-Galois Structures and Skew Braces of Order p^3", *PhD thesis*, The University of Exeter, UK (2018).

[53] K. Nejabati Zenouz: "Skew braces and Hopf-Galois structures of Heisenberg type", *J. Algebra* 524 (2019), 187–225.

[54] S. Nelson: "The combinatorial revolution in knot theory", *Notices Amer. Math. Soc.* 58 (2011), 1553–1561.

[55] S. Nelson: "What is ... a quandle?", *Notices Amer. Math. Soc.* 63 (2016), 378–380.

[56] S.D. Promislow: "A simple example of a torsion-free, nonunique product group", *Bull. London Math. Soc.* 20 (1988), 302–304.

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

[58] W. Rump: "Modules over braces", *Algebra Discrete Math.* 2 (2006), 127–137.

[59] W. Rump: "Braces, radical rings, and the quantum Yang-Baxter equation", *J. Algebra* 307 (2007), 153–170.

[60] W. Rump: "Classification of cyclic braces", *J. Pure Appl. Algebra* 209 (2007), 671–685.

[61] W. Rump: "The brace of a classical group", *Note Mat.* 34 (2014), 115–144.

[62] W. Rump: "Classification of cyclic braces, II", *Trans. Amer. Math. Soc.*, to appear; doi:10.1090/tran/7569.

[63] A. Smoktunowicz: "On some results related to Köthe's conjecture", *Serdica Math. J.* 27 (2001), 159–170.

[64] A. Smoktunowicz: "A note on set-theoretic solutions of the Yang-Baxter equation", *J. Algebra* 500 (2018), 3–18.

[65] A. Smoktunowicz: "On Engel groups, nilpotent groups, rings, braces and the Yang-Baxter equation", *Trans. Amer. Math. Soc.* 370 (2018), 6535–6564.

[66] A. Smoktunowicz – A. Smoktunowicz: "Set-theoretic solutions of the Yang-Baxter equation and new classes of R-matrices", *Linear Algebra Appl.* 546 (2018), 86–114.

[67] A. Smoktunowicz – L. Vendramin: "On skew braces (with an appendix by N. Byott and L. Vendramin)", *J. Comb. Algebra* 2 (2018), 47–86.

[68] A. Soloviev: "Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation", *Math. Res. Lett.* 7 (2000), 577–596.

[69] 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.

Leandro Vendramin
Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
(1428) Pabellón I, Ciudad Universitaria
Buenos Aires (Argentina)
e-mail: lvendramin@dm.uba.ar