.

# COCYCLIC BRACES AND INDECOMPOSABLE COCYCLIC SOLUTIONS OF THE YANG-BAXTER EQUATION

PŘEMYSL JEDLIČKA, AGATA PILITOWSKA, AND ANNA ZAMOJSKA-DZIENIO

ABSTRACT. We study indecomposable involutive set-theoretic solutions of the Yang-Baxter equation with cyclic permutation groups (cocyclic solutions). In particular, we show that there is no one-to-one correspondence between indecomposable cocyclic solutions and cocyclic braces which contradicts recent results in [19].

## 1. INTRODUCTION

The Yang-Baxter equation is a fundamental equation occurring in integrable models in statistical mechanics and quantum field theory [13]. 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. [9]).

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 $(X, \sigma, \tau)$ is a *set-theoretic 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*:

$$(1.1) \qquad (id \times r)(r \times id)(id \times r) = (r \times id)(id \times r)(r \times id).$$

A solution is called *non-degenerate* if the mappings $\sigma_x := \sigma(x, \_)$ and $\tau_y := \tau(\_, y)$ are bijections, for all $x, y \in X$. A solution $(X, \sigma, \tau)$ is *involutive* if $r^2 = \mathrm{id}_{X^2}$. In the involutive case, the operation $\tau$ can be expressed by means of the operation $\sigma$ (see [16, Proposition 1]).

**Convention 1.1.** All solutions, we study in this paper, are set-theoretic, non-degenerate and involutive so we will call them simply *solutions*.

*The permutation group* $\mathcal{G}(X) = \langle \sigma_x \colon x \in X \rangle$ of a solution $(X, \sigma, \tau)$ is the subgroup of the symmetric group $S(X)$ generated by mappings $\sigma_x$, with $x \in X$. The group $\mathcal{G}(X)$ is also called *the involutive Yang-Baxter group* (IYB group) associated to the solution $(X, \sigma, \tau)$. A solution $(X, \sigma, \tau)$ is *indecomposable* if the permutation group $\mathcal{G}(X)$ acts transitively on $X$.

It was already observed in [10] that indecomposable solutions form an important class of all solutions. Since then, many articles on indecomposable solutions appeared, for instance (e.g. [22, Problem 4], [2, 4, 12, 20]).

Solutions $(X, \sigma, \tau)$ with $\mathcal{G}(X)$ cyclic are called *cocyclic*. A classification of such solutions was recently given by Rump [19]. In this paper we focus on indecomposable cocyclic solutions. Among the others, we reformulate the main result [19, Theorem 1] here as Theorem 2.8. According to Rump's classification, a complete system of invariants are: the size of the solution and the index of a subgroup of $\mathcal{G}(X)$. In particular, this classification claims that there exist, for each prime $p$,

exactly two non-isomorphic indecomposable solutions with their permutation groups isomorphic to $\mathbb{Z}_{p^2}$.

However, there is an earlier classification by Castelli, Pinto and Rump [4] of all the indecomposable solutions of size $p^2$ with abelian permutation groups. For each prime $p$, there exist $p+1$ such solutions up to isomorphism, among which one has its permutation group isomorphic to $\mathbb{Z}_p^2$ and the other $p$ solutions have their permutation groups isomorphic to $\mathbb{Z}_{p^2}$. This result has been confirmed by the authors in [12] using a different technique.

The main motivation for this paper was therefore to investigate the discrepancy between those two results cited above. We analyzed several results about indecomposable solutions from the point of view of their permutation groups and this has lead us to a final conclusion: our results are summarized in Theorem 3.15. For an indecomposable cocyclic solution, to constitute a complete system of invariants one needs three parameters not two and, as a consequence, there is no one-to-one correspondence between cocyclic braces and indecomposable cocyclic solutions. This shows that Theorem 1 and its Corollary in [19] are incorrect.

The paper is organized as follows: in Section 2 we give basic definitions used in contemporary studies of involutive set-theoretic solutions of Yang-Baxter equation. We also investigate all the 9-element indecomposable solutions, as the smallest example where the two theories mentioned above differ. This investigation will eventually bring us to a trail of a mistake in [19]. In Section 3 we present a construction by Bachiller, Cedó and Jespers [1] that allows one to construct all the solutions with a given permutation group. We first analyze prime power size solutions and then we use Chinese remainder theorem to capture all finite sizes. At the end, in Section 4, we use this construction to enumerate all the indecomposable solutions with their permutation group cyclic.

## 2. Preliminaries

In this section we give all the necessary notions that we need to analyse both papers [19] and [4]. We give also an example where the results of both the papers differ.

Rump in [17, Definition 2] introduced the notion of a brace and showed the correspondence between such structures and solutions. Here we use an equivalent definition formulated by Cedó, Jespers and Okniński.

**Definition 2.1.** [7, Definition 2.2] An algebra $(B, +, \circ)$ is called a *left brace* if $(B, +)$ is an abelian group, $(B, \circ)$ is a group and the operations satisfy, for all $a, b, c \in B$,

$$(2.1) \qquad a \circ b + a \circ c = a \circ (b + c) + a.$$

The inverse element to $a$ in the group $(B, \circ)$ shall be denoted by $\bar{a}$. Notice that identity elements in both groups $(B, +)$ and $(B, \circ)$ coincide so we will indicate them by 0.

A left brace $(B, +, \circ)$ is said to be *abelian* if its adjoint (or *multiplicative*) group $(B, \circ)$ is abelian, *cyclic* if the additive group $(B, +)$ is cyclic and it is called *cocyclic* if its adjoint group $(B, \circ)$ is cyclic. In case that both groups are cyclic, the brace is then called *bicyclic*.

For a left brace $(B, +, \circ)$ there is an action $\lambda \colon (B, \circ) \to \operatorname{Aut}(B, +)$, where $\lambda(a) = \lambda_a$ and for all $b \in B$, $\lambda_a(b) = a \circ b - a$. The kernel of the group homomorphism $\lambda$ is called the *socle* of the left brace $(B, +, \circ)$ and denoted by $\operatorname{Soc}(B)$, i.e.

$$\operatorname{Soc}(B) = \operatorname{Ker}(\lambda) = \{a \in B \colon \lambda_a = \operatorname{id}\} = \{a \in B \colon a \circ b = a + b \text{ for all } b \in B\}.$$

$\operatorname{Soc}(B)$ is a normal subgroup of the group $(B, \circ)$ and is an ideal of the left brace. Hence the quotient $(B, \circ)/\operatorname{Soc}(B)$ of the multiplicative group is also the quotient of the additive group $(B, +)$ and the factor brace $B/\operatorname{Soc}(B) := (B, +, \circ)/\operatorname{Soc}(B)$ by the ideal $\operatorname{Soc}(B)$ is well defined.

A right brace is defined similarly, replacing Property (2.1) by $b \circ a + c \circ a = (b + c) \circ a + a$. If $(B, +, \circ)$ is both a left and a right brace then one says that it is a (*two-sided*) brace. A brace is called *trivial* if $a + b = a \circ b$, for all $a, b \in B$.

For a left brace $(B, +, \circ)$ one can define another operation $*$ as follows

$$a * b = a \circ b - a - b,$$

for $a, b \in B$. A brace $(B, +, \circ)$ is two-sided if and only if $(B, +, *)$ is a radical ring [7, Proposition 1]. In particular, every abelian left brace is two-sided.

The *associated solution* $(B, \sigma, \tau)$ to a left brace $(B, +, \circ)$ is defined on a set $B$ as follows: $\sigma_x(y) := \lambda_x(y)$ and $\tau_y(x) := \lambda_{\lambda_x(y)}^{-1}(x)$ for $x, y \in B$.

In [10, Section 3.2] Etingof, Schedler and Soloviev introduced, for each solution $(X, \sigma, \tau)$, the equivalence relation $\sim$ on the set $X$: for each $x, y \in X$

$$x \sim y \quad \Leftrightarrow \quad \sigma_x = \sigma_y.$$

They showed that the quotient set $X/{\sim}$ can be again endowed with a structure of a solution. They call such a solution the *retraction* of the solution $(X, \sigma, \tau)$ and denote it by $\mathrm{Ret}(X)$. One can also define *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 $(X, \sigma, \tau)$ 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 such case, we will also say that a solution is *of a multipermutational level $m$*.

**Proposition 2.2.** [17, Proposition 7] *(see also* [7, Lemma 3]*) Let $(B, +, \circ)$ be a nonzero left brace. The solution associated to the factor left brace $B/\mathrm{Soc}(B)$ is equal to the retraction of the solution associated to $(B, +, \circ)$.*

There are many different methods to construct braces. Etingof, Schedler and Soloviev in [10, Appendix] introduced the notion of a *T-structure* on an abelian group $A$. By [10, Theorem A7] one can deduce that cyclic braces correspond to $T$-structures on cyclic groups. Rump in [18] used this result to obtain a wide family of cyclic braces constructed on rings with an identity and with a cyclic additive group. See [18, Proposition 1] and [18, Theorem 1] for the particular case of the ring $(\mathbb{Z}_n, +, \cdot) = \mathbb{Z}/(n)$.

By results of [10, Example 3, Appendix] Rump's construction can be easily generalized. The ring multiplication in any ring $(R, +, \cdot)$ will be consequently indicated by juxtaposition.

**Proposition 2.3.** *Let $(R, +, \cdot)$ be a ring with identity $1$, $J(R)$ be the Jacobson radical of the ring and $r \in J(R)$. Let for $a, b \in R$,*

(2.2)
$$a \circ b := a + b + arb.$$

*Then $(R, +, \circ)$ is a two-sided brace with $\mathrm{Soc}(R) = \mathrm{Ann}(r)$.*

*Proof.* Directly by Etingof, Schedler and Soloviev [10], $(R, \circ)$ is a group with $0$ as the unit and $\bar{a} := -a(1 + ra)^{-1}$ as the inverse of an element $a$.

Straightforward calculations show that $(R, +, \circ)$ is a two-sided brace:

$$a \circ (b + c) + a = a + b + c + ar(b + c) + a = a + b + arb + a + c + arc = a \circ b + a \circ c,$$

and

$$(b + c) \circ a + a = b + c + a + (b + c)ra + a = b + a + bra + c + a + cra = b \circ a + c \circ a.$$

Now, for all $b \in R$,

$$a \in \mathrm{Soc}(R) \Leftrightarrow \lambda_a(b) = b \Leftrightarrow a + b = a \circ b \Leftrightarrow arb = 0 \Leftrightarrow a \in \mathrm{Ann}(r). \qquad \square$$

Note that the construction from Proposition 2.3 is valid for any nilpotent element $r \in R$ (see e.g. [14, Lemma 4.4]).

**Definition 2.4.** [5] Let $(B, +, \circ)$ be a left brace. It is *left nilpotent* if $B^n = 0$ for some positive integer $n$, where $B^{n+1} = B * B^n$ and it is *right nilpotent* if $B^{(m)} = 0$ for some $m \in \mathbb{Z}^+$, where $B^{(1)} = B$ and $B^{(m+1)} = B^{(m)} * B$.

The least $n \in \mathbb{Z}^+$ such that $B^{n+1} = 0$ is called *the left nilpotency degree* of a left brace $(B, +, \circ)$ or one shortly says that $(B, +, \circ)$ is a *left n-nilpotent* left brace. Similarly, if $m \in \mathbb{Z}^+$ is the least number such that $B^{(m+1)} = 0$, then $(B, +, \circ)$ is a *right m-nilpotent* left brace or a left brace of the right nilpotency degree equal to $m$. There is a direct connection between the right nilpotency degree of a left brace and the multipermutational level of its associated solution.

**Proposition 2.5.** [5, Proposition 6] *Let $(B, +, \circ)$ be a nonzero left brace and let $(B, \sigma, \tau)$ be its associated solution. Then $(B, \sigma, \tau)$ is a solution of a multipermutational level $m$ if and only if $(B, +, \circ)$ is right m-nilpotent.*

If a left brace is abelian, then the left nilpotency and the right nilpotency are the same notions and we speak simply of *nilpotency*. In the finite case, every abelian left brace is nilpotent ([7, Proposition 3]).

Let $(R, +, \cdot)$ be a commutative ring with identity 1 and $J(R)$ the Jacobson radical of the ring. Let $(R, +, \circ)$ be the two-sided brace defined in Proposition 2.3 for some $r \in J(R)$. Then, for $a, b \in R$ we have $a * b = rab$. Since the operation $*$ is commutative and associative this implies, for arbitrary $k \in \mathbb{N}$

$$R^k = R^{(k)} = r^{k-1}R.$$

We then immediately obtain:

**Proposition 2.6.** *Let $(R, +, \cdot)$ be a commutative ring with identity 1 and $J(R)$ the Jacobson radical of the ring. Let $(R, +, \circ)$ be the brace defined in Proposition 2.3, for some $r \in J(R)$. Then,*

  (1) *The brace $(R, +, \circ)$ is nilpotent if and only if the element $r$ is nilpotent.*
     *In such a case the nilpotency degrees of $r$ and $(R, +, \circ)$ are equal.*
  (2) *The associated solution to the brace $(R, +, \circ)$ is a multipermutation solution if and only if the element $r$ is nilpotent. The multipermutational level is equal to degree of nilpotency of $r$.*

Our work focuses on finite cocyclic solutions that are closely connected to the following example of cyclic braces.

**Example 2.7.** (See also [15, 4.1].) Let $n = p_1^{k_1} \cdots p_s^{k_s}$ for some prime pairwise distinct numbers $p_1, \ldots, p_s$ and positive integers $k_1, \ldots, k_s$. The nilradical $\mathrm{nil}(\mathbb{Z}_n)$ of the ring $(\mathbb{Z}_n, +, \cdot)$ consists precisely of the elements of the form $rp_1^{t_1} \cdots p_s^{t_s}$, for $1 \le t_1 \le k_1, \ldots, 1 \le t_s \le k_s$ and $r \in \mathbb{Z}_n^*$.

Let $t \in \mathbb{Z}$ be such that $t \bmod n \in \mathrm{nil}(\mathbb{Z}_n)$. By Proposition 2.3, $(\mathbb{Z}_n, +, \circ)$ with

$$a \circ b = a + b + tab$$

is a two-sided brace with $\mathrm{Soc}(\mathbb{Z}_n) = \frac{n}{t}\mathbb{Z}_n \cong \mathbb{Z}_t$.

By Proposition 2.6, the associated solution to such brace is a solution of a multipermutational level equal to $\max(\lceil \frac{k_1}{t_1} \rceil, \lceil \frac{k_2}{t_2} \rceil, \ldots, \lceil \frac{k_s}{t_s} \rceil)$.

We will denote the brace $(\mathbb{Z}_n, +, \circ)$, obtained as described above, by $B_t(n)$.
Note that braces constructed for $t = p_1^{t_1} \cdots p_s^{t_s}$ and $rt$, for $r \in \mathbb{Z}_n^*$, are isomorphic via the mapping $f(x) = r^{-1}x$. This justifies the introduction of the notation:

$$\mathcal{N}(\mathbb{Z}_n) := \{p_1^{t_1} \cdots p_s^{t_s} : t_i \in \{1, \ldots k_i\} \text{ for } i \in \{1, \ldots s\}\},$$

which we use in the following sections.

Braces of the form $B_t(n)$ are actually the only finite abelian cyclic braces [18, Theorem 1]. By [18, Proposition 6] this class contains almost all finite cocyclic braces.

For each solution $(X, \sigma, \tau)$, Etingof, Schedler and Soloviev [10, Section 2] introduced its *structure group* $(G(X), \cdot)$ generated by elements of $X$ with defining relations $x \cdot y = \sigma_x(y) \cdot \tau_y(x)$. $G(X)$ has also a natural structure of a left brace with an additive group being a free abelian group with basis $X$ (see e.g [7, 6]). This left brace is denoted by $A_X$. Furthemore, let $A(X)$ be the factor brace $A_X/\mathrm{Soc}(A_X)$.

Cocyclic solutions have been recently studied in [19]. By construction, the adjoint group of $A(X)$ is isomorphic to the permutation group $\mathcal{G}(X)$. Then, knowing the permutation group of a solution and using an algorithm described in [19, Section 1], one is able to reconstruct the solution $(X, \sigma, \tau)$ from the brace $A(X)$. This leads to the following classification:

**Theorem 2.8.** [19, Theorem 1] *For the isomorphism class of an indecomposable cocyclic solution $(X, \sigma, \tau)$, the order $n$ and the socle index $s = |A(X)/\mathrm{Soc}(A(X))|$ form a complete system of invariants. For a given order $n$, the possible socle indices are the divisors $s$ of $n$ which satisfy $p \mid n \Rightarrow ps \mid n$, for all primes $p$ and $8 \mid n \Rightarrow 4s \mid n$.*

An immediate consequence of the theorem is

**Corollary 2.9.** [19] *Up to isomorphism, there is a one-to-one correspondence between finite indecomposable cocyclic solutions and finite cocyclic braces.*

This corollary was quite unexpected, as Rump himself admits in the introduction of [19]. Nevertheless, as we already announced in the introduction of this paper, both of the results are incorrect. We illustrate it on the smallest counterexample.

**Example 2.10.** Consider the ring $(\mathbb{Z}_9, +, \cdot)$. According to [4, Corollary 22] and [12, Corollary 4.8], there exist three indecomposable 9-element solutions $(X, \sigma, \tau)$ with their permutation group cyclic, namely for $r \in \{0, 3, 6\}$, the set $X = \{0, 1, \ldots, 8\}$ with

$$\sigma_x(y) = rx + y + 1 \qquad \text{and} \qquad \tau_y(x) = x - 1 - r(y + 1).$$

They are not isomorphic since, for each $x \in X$, $\sigma_{\sigma_x(x)} = \sigma_x^{r+1}$.

It can be computed that the brace $A(X)$ is then isomorphic to the brace $B_{9-r}(9)$ described in Example 2.7. Of course, for $r = 0$, it is a trivial brace $B_9(9)$, whereas for $r \in \{3, 6\}$ one obtains the brace $B_3(9) \cong B_6(9)$ (see also Example 4.2).

This example indicates (a thorough proof comes in the next section though) that there is a mistake in the proof of Theorem 2.8. Indeed, there is one, a very subtle one: on page 473 the autor correctly supposes that the multiplicative group can be identified with $\mathbb{Z}_n$. But then the proof of the main theorem on page 475 starts with: "*Up to isomorphism, the solution $X$ is determined by the cocyclic brace $A(X)$*" (which is unique up to isomorphism). However, we cannot use the "*up to isomorphism*" argument anymore since we have already chosen an isomorphism by identifying the elements of $A(X)$ with the elements of the group $\mathbb{Z}_n$.

The rest of the proof is correct. Therefore we can say that a cocyclic solution is uniquely determined by the brace $A(X)$ and by the choice of the isomorphism $(A(X), \circ) \cong \mathbb{Z}_n$, that means by the choice of a generator of $(A(X), \circ)$. Nevertheless, different choices of the generators may still yield isomorphic solutions. Finding a correct answer for the isomorphism question using the tools of [19] does not seem to be straightforward and therefore, in the next section, we introduce results from yet another paper.

## 3. Cocyclic braces and solutions

In this Section our aim is to construct all finite indecomposable solutions with cyclic permutation group. In [1] Bachiller, Cedó and Jespers present the construction of all finite solutions $(X, \sigma, \tau)$ of

the YBE such that the permutation group $\mathcal{G}(X)$ is isomorphic, as a left brace, to a given finite left brace $(B, +, \circ)$. We shall not repeat their construction here, as our case is much less complicated than the general one. If the permutation group $\mathcal{G}(X)$ is abelian and acts on $X$ transitively, then it acts regularly on $X$ and therefore its order is equal to $|X|$ and, simultaneously, to $|B|$.

By [21, Theorem 19], a finite left brace of cardinality $n = p_1^{k_1} \ldots p_s^{k_s}$, for some pairwise distinct prime numbers $p_1, \ldots, p_s$ and $k_1, \ldots, k_s \in \mathbb{Z}^+$, with multiplicative group isomorphic to an abelian group $\mathbb{Z}_n$ is a direct product of left braces whose cardinalities are powers of prime numbers. By [18, Section 5], every cyclic brace of a cardinality equal to a power of some odd prime is bicyclic. On the other hand, by [1, Proposition 5.4], every cocyclic left brace $(B, +, \circ)$ of order $4 \neq n = p^k$, for some prime $p$ and $k \geq 1$, has a cyclic additive group $\mathbb{Z}_{p^k}$. According to Rump's classification [18, Theorem 1] (see also [1, Section 5]), such braces are equal to $B_t(p^k)$ (up to isomorphism), for $t \in \mathcal{N}(\mathbb{Z}_{p^k})$ with assumption that $t \neq 2$ when $p^k = 4$. Four-element left braces form an exception in the classification: there exist two trivial ones, one cyclic which is not cocyclic and one cocyclic which is not cyclic [19]. See also a clasification of commutative radical rings given in [15, Proposition 4.1.7].

This implies (see [1, Remark 5.5]) that a cocyclic left brace of cardinality $n = 2^{k_1} \cdot p_2^{k_2} \ldots p_s^{k_s}$ with $0 \leq k_1 \neq 2$ is isomorphic to the following direct product

$$B_{t_1}(2^{k_1}) \times B_{t_2}(p_2^{k_2}) \times \ldots \times B_{t_s}(p_s^{k_s}),$$

with some $t_i \in \mathcal{N}(\mathbb{Z}_{p_i^{k_i}})$, for $1 \leq i \leq s$, where $t_1 \neq 2$ or $k_1 = 1$.

Any such direct product is isomorphic to the brace described in Example 2.7.

**Lemma 3.1.** *Let $n = p_1^{k_1} \cdots p_s^{k_s}$ for some pairwise distinct prime numbers $p_1, \ldots, p_s$ and $k_1, \ldots, k_s \in \mathbb{Z}^+$. Let $1 < t_i \leq p_i^{k_i}$ be a power of $p_i$, for $1 \leq i \leq s$, and let $t = t_1 \cdots t_s$. Then the braces $B_t(n)$ and $B_{t_1}(p_1^{k_1}) \times B_{t_2}(p_2^{k_2}) \times \ldots \times B_{t_s}(p_s^{k_s})$ are isomorphic.*

*Proof.* Indeed, let $f : \mathbb{Z}_n \to \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \ldots \times \mathbb{Z}_{p_s^{k_s}}$ be such that

$$a \mapsto (a\frac{t}{t_1} \pmod{p_1^{k_1}}, \ldots, a\frac{t}{t_i} \pmod{p_i^{k_i}}, \ldots, a\frac{t}{t_s} \pmod{p_s^{k_s}}).$$

Since for each $1 \leq i \leq s$, the element $\frac{t}{t_i}$ is a generator of the group $\mathbb{Z}_{p_i^{k_i}}$, the mapping $f$ is a homomorphism of additive groups. Next, for $a, b \in \mathbb{Z}_n$

$$f(a) \circ f(b) = (a\frac{t}{t_1} \pmod{p_1^{k_1}}, \ldots, a\frac{t}{t_s} \pmod{p_s^{k_s}}) \circ (b\frac{t}{t_1} \pmod{p_1^{k_1}}, \ldots, b\frac{t}{t_s} \pmod{p_s^{k_s}}) =$$

$$(a\frac{t}{t_1} \pmod{p_1^{k_1}} \circ b\frac{t}{t_1} \pmod{p_1^{k_1}}, \ldots, a\frac{t}{t_s} \pmod{p_s^{k_s}} \circ b\frac{t}{t_s} \pmod{p_s^{k_s}}) =$$

$$(a\frac{t}{t_1} + b\frac{t}{t_1} + t_1 \cdot a\frac{t}{t_1} \cdot b\frac{t}{t_1} \pmod{p_1^{k_1}}, \ldots, a\frac{t}{t_s} + b\frac{t}{t_s} + t_s \cdot a\frac{t}{t_s} \cdot b\frac{t}{t_s} \pmod{p_s^{k_s}}) =$$

$$((a + b + tab)\frac{t}{t_1} \pmod{p_1^{k_1}}, \ldots, (a + b + tab)\frac{t}{t_s} \pmod{p_s^{k_s}}) = f(a + b + tab) = f(a \circ b).$$

Hence, $f$ is a homomorphism of braces, too. Finally, if

$$f(a) = (a\frac{t}{t_1} \pmod{p_1^{k_1}}, \ldots, a\frac{t}{t_s} \pmod{p_s^{k_s}}) = (b\frac{t}{t_1} \pmod{p_1^{k_1}}, \ldots, b\frac{t}{t_s} \pmod{p_s^{k_s}}) = f(b)$$

we have

$$\forall (1 \leq i \leq s) \quad p_i^{k_i}|(a - b) \quad \Rightarrow \quad n|(a - b) \quad \Rightarrow \quad a = b,$$

and $f$ is a bijection. $\square$

As a corollary one obtains generalization of [1, Proposition 5.4] (see also [18, Proposition 6]).

**Corollary 3.2.** *Let $n \in \mathbb{Z}^+$ and $t \in \mathcal{N}(\mathbb{Z}_n)$ be such that $4|t$ whenever $4|n$. Then the brace $B_t(n)$ is bicyclic.*

**Remark 3.3.** The multiplicative group of the brace $B_2(2^{k+1})$, for $k \in \mathbb{Z}^+$, is isomorphic to the (non-cyclic) group $\mathbb{Z}_2 \times \mathbb{Z}_{2^k}$.

A cocyclic left brace of cardinality $n = 2^2 \cdot p_2^{k_2} \ldots p_s^{k_s}$ also splits as a direct product, namely

$$\tilde{B}_{t_1}(4) \times B_{t_2}(p_2^{k_2}) \times \ldots \times B_{t_s}(p_s^{k_s}),$$

with some $t_i \in \mathcal{N}(\mathbb{Z}_{p_i^{k_i}})$, for $1 \leq i \leq s$, where $\tilde{B}_{t_1}(4)$ is a cocyclic brace obtained from $B_{t_1}(4)$ by swapping the operations $+$ and $\circ$.

To construct solutions with the permutation group isomorphic to the associated group of a given left brace, it is enough to find two special mappings: $\eta \colon X \to B$ and $\varrho \colon B \to S(X)$ as described in [1, Section 2]. In the case when the left brace $(B, +, \circ)$ is cocyclic of order $p^k$, for some prime $p$ with $k \in \mathbb{Z}^+$, and solutions are indecomposable, this construction can be significantly simplified.

3.1. **Indecomposable cocyclic solutions of order $p^k$.** First of all, the construction in [1], Section 3, involves an intersection of subgroups $\bigcap_I \bigcap_{J_i} \bigcap_b bK_{i,j}b^{-1} = \{0\}$. Since any subgroup $K$ of the abelian group $(B_t(p^k), \circ)$ is normal we of course have $bK_{i,j}b^{-1} = K_{i,j}$, for any $b \in B$. Furthermore, to obtain the trivial intersection of a family of subgroups of the cyclic group $(B_t(p^k), \circ)$, we have to assume that at least one $K_{i,j}$ is equal to $\{0\}$.

Moreover, in [1], Theorem 3.1 starts with $X = \sqcup_I \sqcup_{J_i} B/K_{i,j}$. Given the equality $|B| = |\mathcal{G}(X)| = |X|$ and the fact $K_{i,j} = \{0\}$, for some $i \in I$ and some $j \in J_i$, we necessarily have $|I| = |J_i| = 1$. Since $(B, +)$ has to be generated by $\bigcup \bigcup I$, there exists some $a \in \mathbb{Z}_{p^k}^*$ such that

$$\eta \colon \mathbb{Z}_{p^k} \to \mathbb{Z}_{p^k}; \quad \eta(b) = \lambda_b(a),$$

and

$$\varrho \colon \mathbb{Z}_{p^k} \to S(\mathbb{Z}_{p^k}); \quad \varrho(c) \colon \mathbb{Z}_{p^k} \to \mathbb{Z}_{p^k}; \quad \varrho(c)(b) = c \circ b.$$

Hence

$$\varrho(\eta(b))(c) = \varrho(\lambda_b(a))(c) = \lambda_b(a) \circ c = (b \circ a - b) \circ c =$$
$$(b + a + tab - b) + c + t(a + tab)c = a + tab + c + t(a + tab)c.$$

This implies the following reformulation of [1, Theorem 3.1].

**Theorem 3.4.** *Let $p$ be a prime number and $k \in \mathbb{Z}^+$. Let $t \in \mathbb{Z}$ such that $t \mod p^k \in \mathrm{nil}(\mathbb{Z}_{p^k})$ and $(B_t(p^k), +, \circ)$ be a cocyclic brace of order $p^k$.*

*For any indecomposable solution $(X, \sigma, \tau)$ with the permutation group $\mathcal{G}(X)$ isomorphic, as left braces, to $(B_t(p^k), +, \circ)$, there exists $a \in \mathbb{Z}_{p^k}^*$, so that $(X, \sigma, \tau)$ is isomorphic to the solution defined on the set $\mathbb{Z}_{p^k}$ with*

$$\sigma_b(c) := a + c + tab + tac + t^2abc$$

*for all $b, c \in \mathbb{Z}_{p^k}$.*

Let us denote such a solution by $\mathcal{K}(p^k, t, a)$.

**Remark 3.5.**   (1) For $k = 1$ one obtains [10, Theorem 2.13]: the indecomposable solution with a prime number of elements is a cyclic permutation solution, i.e. a multipermutation solution of level 1 with $\sigma_x$ being a cycle. There is only one (up to isomorphism) such solution for each prime.

(2) If $t \in \mathcal{N}(\mathbb{Z}_{p^k})$ and $r \in \mathbb{Z}_{p^k}^*$ then, similarly as for braces in Example 2.7, we obtain an isomorphic solutions $\mathcal{K}(p^k, t, a)$ and $\mathcal{K}(p^k, rt, ar^{-1})$ via the mapping $\Phi(x) = r^{-1}x$. Thus we usually restrain our focus to $t \in \mathcal{N}(\mathbb{Z}_{p^k})$.

[1, Theorem 4.1] characterizes when two solutions, with their permutation groups isomorphic to the same brace, are isomorphic. Again, the assumptions $|I| = 1$ and $K_{i,j} = \{0\}$ simplify the theorem substantially.

**Theorem 3.6.** *Let $a, a' \in \mathbb{Z}_{p^k}^*$. The solutions $\mathcal{K}(p^k, t, a)$ and $\mathcal{K}(p^k, t, a')$ are isomorphic if and only if there exist an automorphism $\Psi$ of the left brace $(B_t(p^k), +, \circ)$ and an element $z \in \mathbb{Z}_{p^k}$ such that*

$$\Psi(a) = \lambda_z(a').$$

Each automorphism $\Psi$ of the cyclic group $\mathbb{Z}_{p^k}$ is of the form $\Psi(x) = \alpha x$, where $\alpha \in \mathbb{Z}_{p^k}^*$. Moreover, each automorphism $\Psi$ of the left brace $(B_t(p^k), +, \circ)$ must satisfy additionally, for every $x, y \in \mathbb{Z}_{p^k}$, the following:

$$\alpha x + \alpha y + \alpha^2 t x y = \alpha x \circ \alpha y = \Psi(x) \circ \Psi(y) =$$
$$\Psi(x \circ y) = \alpha(x \circ y) = \alpha(x + y + t x y) = \alpha x + \alpha y + \alpha t x y.$$

This implies that, for any $x, y \in \mathbb{Z}_{p^k}$, $\alpha t x y \equiv \alpha^2 t x y \pmod{p^k}$ or equivalently, $p^k \mid t x y \alpha(\alpha - 1)$. Hence, for $x = y = 1$ and remembering that $t = p^w$ for some $w \in \{1, \ldots, k\}$, $p^{k-w} \mid \alpha(\alpha - 1)$. Since $\gcd(\alpha, p) = 1$ we obtain $p^{k-w} \mid (\alpha - 1)$ which means that $\alpha \equiv 1 \pmod{p^{k-w}}$. Finally, we obtain that

$$\exists (h \in \operatorname{Soc}(B_t(p^k))) \; \alpha = 1 + h.$$

Summarizing,

**Corollary 3.7.** *The solutions $\mathcal{K}(p^k, t, a)$ and $\mathcal{K}(p^k, t, a')$ are isomorphic if and only if there exist $h \in \operatorname{Soc}(B_t(p^k))$ and $z \in \mathbb{Z}_{p^k}$ such that*

$$(3.1) \qquad\qquad\qquad (1 + h)a = a'(1 + zt).$$

In particular, for $h = 0$, $a$ and $a'$ are in the same orbit of the action $\lambda$. Thus all solutions $\mathcal{K}(p^k, t, a)$ and $\mathcal{K}(p^k, t, a')$ with $a$ and $a'$ in the same orbit of the action $\lambda$ are isomorphic.

**Corollary 3.8.** *The solutions $\mathcal{K}(p^k, p^w, a)$ and $\mathcal{K}(p^k, p^w, a')$ are isomorphic if and only if*
   (1) $a \equiv a' \pmod{p^w}$, *for $k \geq 2w$;*
   (2) $a \equiv a' \pmod{p^{k-w}}$, *for $2w > k > w$,*
   (3) $a$ *and* $a'$ *are any, for* $w = k$.

*Proof.* Recall that, for the brace $B_{p^w}(p^k)$, the socle $\operatorname{Soc}(\mathbb{Z}_{p^k}) = p^{k-w}\mathbb{Z}_{p^k}$ and note that the equation (3.1) is equivalent to the following one

$$a - a' \equiv a' p^w z - a p^{k-w} h \pmod{p^k},$$

for some $h, z \in \mathbb{Z}_{p^k}$.

Let $a - a' = p^w r$, for some $r \in \mathbb{Z}$. Then, by choosing $h = 0$ and $z = r(a')^{-1}$, we obtain

$$a' p^w z - a p^{k-w} h = a' p^w r(a')^{-1} = p^w r = a - a'$$

and $\mathcal{K}(p^k, p^w, a) \cong \mathcal{K}(p^k, p^w, a')$.

Let $a - a' = p^{k-w} r$, for some $r \in \mathbb{Z}$. Then, by choosing $h = -r a^{-1}$ and $z = 0$, we obtain

$$a' p^w z - a p^{k-w} h = a p^{k-w} r a^{-1} = p^{k-w} r = a - a'$$

and $\mathcal{K}(p^k, p^w, a) \cong \mathcal{K}(p^k, p^w, a')$ as well.

Now assume that solutions $\mathcal{K}(p^k, p^w, a)$ and $\mathcal{K}(p^k, p^w, a')$ are isomorphic. Then

$$a - a' \equiv a' p^w z - a p^{k-w} h \pmod{p^k}$$

for some $h, z \in \mathbb{Z}_{p^k}$.

Thus if $k - w \geq w$ we have $p^w \mid (a - a')$. Otherwise, $p^{k-w} \mid (a - a')$. $\qquad\square$

It is known that finite cocyclic solutions are multipermutation solutions. In general it is difficult to describe the retraction of the solution. But in the case of indecomposable cocyclic solutions of the form $\mathcal{K}(p^k, p^w, a)$ we are able to give a precise description and also to compute their level.

**Theorem 3.9.** *Let $p$ be a prime number, $k, w \in \mathbb{N}$ and $a \in \mathbb{Z}_{p^k}^*$. For arbitrary $m \in \mathbb{N}$, the $m$-th retraction $\mathrm{Ret}^m(X)$ of the solution $(X, \sigma, \tau) = \mathcal{K}(p^k, p^w, a)$ is isomorphic to the solution:*

$$\mathcal{K}(p^{\max(k-mw, 0)}, p^w, a).$$

*Proof.* Suppose first $k \leq w$. Then $p^w \equiv 0 \pmod{p^k}$ and the solution $\mathcal{K}(p^k, p^w, a)$ is a permutation solution. Hence $\mathrm{Ret}^m(\mathcal{K}(p^k, p^w, a))$ is, for all $m > 0$, the trivial solution $\mathcal{K}(1, 0, 0)$.

Suppose now $k \geq w$. At first we want to prove that $\mathrm{Ret}(X) \cong \mathcal{K}(p^{k-w}, p^w, a)$. The relation $\sim$ on $X = \mathbb{Z}_{p^k}$ is defined as follows:

$$b \sim c \quad \Leftrightarrow \quad \sigma_b = \sigma_c \quad \Leftrightarrow \quad b \equiv c \pmod{p^{k-w}}.$$

Our planned isomorphism $\Phi : \mathrm{Ret}(X) \to \mathcal{K}(p^{k-w}, p^w, a)$ simply sends $[b]_\sim$ to $b \bmod p^{k-w}$. Such a mapping is clearly a bijection. Moreover, it is actually an identity on $\mathbb{Z}_{p^{k-w}}$ and both the operations $\sigma$ (in $\mathrm{Ret}(X)$ and in $\mathcal{K}(p^{k-w}, p^w, a)$) are defined using the same $[a]_\sim$ and the same $[p^w]_\sim$ and therefore $\Phi$ is a homomorphism.

The rest of the proof goes easily by an induction on $m$. $\qquad\square$

**Corollary 3.10.** *The solution $\mathcal{K}(p^k, p^w, a)$ is a multipermutation solution of level $\lceil k/w \rceil$.*

*Proof.* By Theorem 3.9, the size of the retract $\mathrm{Ret}^m(X)$ is $\max(1, p^{k-mw})$. And the smallest number $m$ such that $k - mw \leq 0$ is $m = \lceil \frac{k}{w} \rceil$. $\qquad\square$

**Question 3.11.** *We have presented two different solutions based on the brace $B_t(p^k)$, namely an indecomposable solution $\mathcal{K}(p^k, t, a)$ and the (decomposable) associated solution. Nevertheless, according to Proposition 2.6, both the solutions have the same multipermutational level. We wonder whether this is a coincidence or there is a more general mechanism hidden behind.*

What remains is a description of indecomposable cocyclic solutions of size 4. According to [4] or [12] there are only two such solutions: one of multipermutational level 1 and one of multipermutational level 2. The latter one $(X, \tilde{\sigma}, \tilde{\tau})$ can be constructed on the ring $(\mathbb{Z}_4, +, \cdot)$ using the operation

$$\tilde{\sigma}_b(c) = a + c + 2ab,$$

for any chosen $a \in \{1, 3\}$. We will denote such a solution by $\tilde{\mathcal{K}}(4, 2, a)$. Similarly as in Remark 3.5, $\tilde{\mathcal{K}}(4, 2, 1)$ and $\tilde{\mathcal{K}}(4, 2, 3)$ are isomorphic via the mapping $\Phi(x) = 3^{-1}x = 3x$.

**3.2. Indecomposable cocyclic solutions of order $n = p_1^{k_1} \ldots p_s^{k_s}$.** To obtain finite indecomposable solutions with the permutation group $\mathcal{G}(X)$ isomorphic, as a left brace, to a finite left brace $(B_t(n), \circ)$, for some pairwise distinct prime numbers $p_1, \ldots, p_s$, $k_1, \ldots, k_s \in \mathbb{Z}^+$ and $2 < t \in \mathcal{N}(\mathbb{Z}_n)$, we can proceed exactly in the same way as in Subsection 3.1. There is one difference however—to get a trivial intersection of a family of subgroups of $(B_t(n), \circ)$ it is not necessary to assume that at least one of them is equal to $\{0\}$. But let us make such an assumption. In consequence, we obtain some indecomposable cocyclic solutions $(X, \sigma, \tau)$ defined on the set $X = \mathbb{Z}_n$ and being of the form

$$\sigma_b(c) := a + c + tab + tac + t^2abc$$

for $b, c \in \mathbb{Z}_n$, $t \in \mathcal{N}(\mathbb{Z}_n)$ and $a \in \mathbb{Z}_n^*$. We will denote them by $\mathcal{K}(n, t, a)$.

On the other hand by [3, Corollary 12] each indecomposable solution $(X, \sigma, \tau)$ of order $n = p_1^{k_1} \ldots p_s^{k_s}$ and with cyclic permutation group $\mathcal{G}(X)$ is isomorphic to the product of indecomposable solutions $\mathcal{K}(p_i^{k_i}, t_i, a_i)$, for $i = 1, \ldots, s$. A precise description of the isomorphism is given as follows:

**Theorem 3.12.** *Let* $n = p_1^{k_1} \cdots p_s^{k_s}$ *for some pairwise distinct prime numbers* $p_1, \ldots, p_s$ *and* $k_1, \ldots, k_s \in \mathbb{Z}^+$. *Let* $t = t_1 \cdots t_s \in \mathcal{N}(\mathbb{Z}_n)$, *for* $t_i \in \mathcal{N}(\mathbb{Z}_{p_i^{k_i}})$. *Let* $a \in \mathbb{Z}_n^*$ *and let* $a_i \in \mathbb{Z}_{p_i^{k_i}}^*$ *be such that* $a_i \equiv \frac{t}{t_i} a \pmod{p_i^{k_i}}$, *for* $1 \le i \le s$. *Then the solutions* $\mathcal{K}(n, t, a)$ *and* $\mathcal{K}(p_1^{k_1}, t_1, a_1) \times \mathcal{K}(p_2^{k_2}, t_2, a_2) \times \ldots \times \mathcal{K}(p_s^{k_s}, t_s, a_s)$ *are isomorphic.*

*Proof.* We show that the mapping $\Phi \colon \mathbb{Z}_n \to \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \ldots \times \mathbb{Z}_{p_s^{k_s}}$ given by

$$x \mapsto (\frac{t}{t_1} x \pmod{p_1^{k_1}}, \ldots, \frac{t}{t_i} x \pmod{p_i^{k_i}}, \ldots, \frac{t}{t_s} x \pmod{p_s^{k_s}})$$

is a homomorphism of the solutions. By Chinese Remainder Theorem it is also an isomorphism.

$$\sigma_{\Phi(b)} \Phi(c) = \sigma_{(b\frac{t}{t_1} \pmod{p_1^{k_1}}, \ldots, b\frac{t}{t_s} \pmod{p_s^{k_s}})}(c\frac{t}{t_1} \pmod{p_1^{k_1}}, \ldots, c\frac{t}{t_s} \pmod{p_s^{k_s}}) =$$

$$(\sigma_{b\frac{t}{t_1} \pmod{p_1^{k_1}}}(c\frac{t}{t_1} \pmod{p_1^{k_1}}), \ldots, \sigma_{b\frac{t}{t_s} \pmod{p_s^{k_s}}}(c\frac{t}{t_s} \pmod{p_s^{k_s}})) =$$

$$(a_1 + \frac{t}{t_1}c + t_1 \cdot a_1 \cdot \frac{t}{t_1}b + t_1 \cdot a_1 \cdot \frac{t}{t_1}c + t_1^2 \cdot a_1 \cdot b\frac{t}{t_1} \cdot c\frac{t}{t_1} \pmod{p_1^{k_1}}, \ldots) =$$

$$(\frac{t}{t_1}a + \frac{t}{t_1}c + t \cdot a \cdot \frac{t}{t_1}b + t \cdot a \cdot \frac{t}{t_1}c + t_1 \cdot a \cdot b \cdot c\frac{t^3}{t_1^2} \pmod{p_1^{k_1}}, \ldots) =$$

$$((a + c + tab + tac + t^2abc)\frac{t}{t_1} \pmod{p_1^{k_1}}, \ldots, (a + c + tab + tac + t^2abc)\frac{t}{t_s} \pmod{p_s^{k_s}}) =$$

$$\Phi(a + c + tab + tac + t^2abc) = \Phi(\sigma_b(c)). \qquad \square$$

**Corollary 3.13.** *Let* $d := gcd(t, \frac{n}{t})$. *The solutions* $\mathcal{K}(n, t, a)$ *and* $\mathcal{K}(n, t, a')$ *are isomorphic if and only if*

$$a \equiv a' \pmod{d}.$$

*Proof.* We use here the notation of Theorem 3.12. According to Corollary 3.8 and Theorem 3.12, the solutions $\mathcal{K}(n, t, a)$ and $\mathcal{K}(n, t, a')$ are isomorphic if and only if, for each $1 \le i \le s$, the numbers $a_i = \frac{t}{t_i}a$ and $a_i' = \frac{t}{t_i}a'$, are congruent modulo $\min(t_i, p_i^{k_i}/t_i)$. Since $\frac{t}{t_i}$ is coprime to $p_i$ and since $\min(t_i, p_i^{k_i}/t_i) = \gcd(t, \frac{n}{t}, p_i^{k_i})$, this is equivalent to $a_i \equiv a_i' \pmod{\gcd(d, p_i^{k_i})}$, for each $1 \le i \le s$. According to Chinese Remainder Theorem, this means $a \equiv a' \pmod{d}$. $\qquad \square$

Theorem 3.12 describes all finite indecomposable cocyclic solutions except for some non-trivial ones of size $4n$, with $n$ odd. In this case we need to consider the four element solution which does not originate from a bicyclic brace. In the following proposition we give an explicit construction of the remaining solutions of size $4n$. We are not able to apply the map $\Phi \colon \mathbb{Z}_{4n} \to \mathbb{Z}_4 \times \mathbb{Z}_n$ (from the proof of Theorem 3.12) directly since there is that four element cocyclic brace which is not cyclic. But we use a similar formula.

**Proposition 3.14.** *Let* $n$ *be an odd number and* $\bar{2}$ *be a number such that* $2 \cdot \bar{2} \equiv 1 \pmod{n}$. *Let* $t \in \mathcal{N}(\mathbb{Z}_n)$ *and* $a \in \mathbb{Z}_{4n}^*$. *Then* $(\mathbb{Z}_{4n}, \bar{\sigma}, \bar{\tau})$ *with*

$$\bar{\sigma}_b(c) = a + c + 2tab + 4t\bar{2}ac + 4t^2abc \pmod{4n}$$

*yields an indecomposable solution with its permutation group isomorphic to* $\mathbb{Z}_{4n}$.

*Proof.* We will show that $(\mathbb{Z}_{4n}, \bar{\sigma}, \bar{\tau})$ is isomorphic to the product of two solutions: one defined on the set $\mathbb{Z}_4$ and the second one on $\mathbb{Z}_n$.

The mapping

$$\Phi \colon \mathbb{Z}_{4n} \to \mathbb{Z}_4 \times \mathbb{Z}_n; \quad \Phi : x \mapsto (tx \pmod 4, 2x \pmod n)$$

gives for $b, c \in \mathbb{Z}_{4n}$

$$\Phi(\overline{\sigma}_b(c)) = (t(a+c+2tab+4t\overline{2}ac+4t^2abc) \pmod 4, 2(a+c+2tab+4t\overline{2}ac+4t^2abc) \pmod n) =$$
$$(ta + tc + 2t^2ab \pmod 4, 2a + 2c + 4tab + 4tac + 8t^2abc \pmod n) =$$
$$(ta + \Phi(c) + 2ta\Phi(b) \pmod 4, 2a + \Phi(c) + t2a\Phi(b) + t2a\Phi(c) + t^2 2a\Phi(b)\Phi(c) \pmod n).$$

Since for any $t \in \mathcal{N}(\mathbb{Z}_n)$ and $a \in \mathbb{Z}_{4n}^*$, $ta \in \{1,3\} \pmod 4$ we obtain that $\Phi$ is a homomorphism between the solution $(\mathbb{Z}_{4n}, \overline{\sigma}, \overline{\tau})$ and a product of solutions $\tilde{\mathcal{K}}(4, 2, ta \pmod 4)$ and $\mathcal{K}(n, t, 2a \pmod n)$. Clearly, $\Phi$ is a bijection. $\qquad \square$

**Theorem 3.15.** *A complete set of invariants for finite cocyclic indecomposable solutions are*

- $n \in \mathbb{N}$;
- $t \in \mathbb{N}$ *such that*
  - $t$ *divides* $n$,
  - *every prime* $p$ *divides* $t$ *whenever* $p$ *divides* $n$,
  - *if* $8$ *divides* $n$ *then* $4$ *divides* $t$;
- $a \in \{1, \ldots, \gcd(t, n/t)\}$ *coprime to* $n$.

*Proof.* Existence of such solutions is given in Theorem 3.12 and Proposition 3.14. Moreover, we know that such a solution splits as a product of prime-power size solutions. If $n \equiv 4 \pmod 8$ then there are two possibilities for the 2-primary component and they depend on $t$ only, not on $a$. Otherwise we use Corollary 3.13. $\qquad \square$

**Remark 3.16.** Let $n$, $t$, $a$ be invariants described in Theorem 3.15. Similar proof as in Theorem 3.9 shows that $\mathrm{Ret}(\mathcal{K}(n,t,a)) \cong \mathcal{K}(n/t,t,a)$. In particular, the solution $\mathcal{K}(n,t,a)$ is then a multi-permutation solution of level $s$, where $s$ is the smallest number such that $n$ divides $t^s$. Moreover, the solution $(\mathbb{Z}_{4n}, \overline{\sigma}, \overline{\tau})$ is of multipermutational level equal to $\max(2, s)$.

## 4. ENUMERATION AND EXAMPLES

In the last section we compute the number of non-isomorphic indecomposable cocyclic solutions. We give exact numbers for prime powers only as for composed numbers the enumeration is straightforward using the splitting onto their prime components. We, of course, omit the case $n = p$ where we have exactly one solution and the case $n = 4$ where we have two solutions.

**Proposition 4.1.** *Let $p$ be a prime number and $k \in \mathbb{Z}^+$. Then the number $N$ of indecomposable solutions of order $p^k$ and with the cyclic permutation group is equal to:*

- $N = p^r + p^{r-1} - 1$, *for* $p \neq 2$ *and* $k = 2r \geq 2$
- $N = 2p^r - 1$, *for* $p \neq 2$ *and* $k = 2r + 1 \geq 3$
- $N = 2^r + 2^{r-1} - 2$, *for* $p = 2$ *and* $k = 2r \geq 4$
- $N = 2^{r+1} - 2$, *for* $p = 2$ *and* $k = 2r + 1 \geq 3$

*Proof.* Directly by Corollary 3.8, for $p \neq 2$, we have

$$N = \sum_{w=1}^{\lfloor \frac{k}{2} \rfloor} (p^w - p^{w-1}) + \sum_{w=\lfloor \frac{k}{2} \rfloor + 1}^{k-1} (p^{k-w} - p^{k-w-1}) + 1 =$$
$$p^{\lfloor \frac{k}{2} \rfloor} - 1 + p^{k - \lfloor \frac{k}{2} \rfloor - 1} - 1 + 1 = p^{\lfloor \frac{k}{2} \rfloor} + p^{k - \lfloor \frac{k}{2} \rfloor - 1} - 1.$$

Moreover, for $p = 2$

$$N = \sum_{w=2}^{\lfloor \frac{k}{2} \rfloor} (2^w - 2^{w-1}) + \sum_{w=\lfloor \frac{k}{2} \rfloor+1}^{k-1} (2^{k-w} - 2^{k-w-1}) + 1 =$$

$$2^{\lfloor \frac{k}{2} \rfloor} - 2 + 2^{k-\lfloor \frac{k}{2} \rfloor-1} - 1 + 1 = 2^{\lfloor \frac{k}{2} \rfloor} + 2^{k-\lfloor \frac{k}{2} \rfloor-1} - 2. \qquad \square$$

At the end we give some examples to illustrate Theorem 3.4.

**Example 4.2.** For $p = 3$ and $k = 2$ we have two non-isomorphic braces: $(B_3(9), +, \circ)$ and $(B_9(9), +, \circ)$.

Let us consider the brace $(B_3(9), +, \circ)$ with the multiplication

$$x \circ y = x + y + 3xy.$$

In this case $\mathrm{Soc}(B_3(9)) = \{0, 3, 6\}$. Since $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ then using the construction described in Theorem 3.4 we obtain six indecomposable solutions:

$$\mathcal{K}(9, 3, 1), \text{ with } \sigma_b(c) = 1 + 3b + 4c, \qquad \mathcal{K}(9, 3, 2), \text{ with } \sigma_b(c) = 2 + 6b + 7c,$$
$$\mathcal{K}(9, 3, 4), \text{ with } \sigma_b(c) = 4 + 3b + 4c, \qquad \mathcal{K}(9, 3, 5), \text{ with } \sigma_b(c) = 5 + 6b + 7c,$$
$$\mathcal{K}(9, 3, 7), \text{ with } \sigma_b(c) = 7 + 3b + 4c, \qquad \mathcal{K}(9, 3, 8), \text{ with } \sigma_b(c) = 8 + 6b + 7c.$$

By Corollary 3.8, the solutions $\mathcal{K}(9, 3, 1)$, $\mathcal{K}(9, 3, 4)$ and $\mathcal{K}(9, 3, 7)$ are isomorphic. In particular, the solutions $\mathcal{K}(9, 3, 1)$ and $\mathcal{K}(9, 3, 4)$ are isomorphic by the mapping $\Phi(x) = 7^{-1}x = 4x$, i.e. by the permutation $(147)(285)$. Similarly, the solutions $\mathcal{K}(9, 3, 2)$, $\mathcal{K}(9, 3, 5)$ and $\mathcal{K}(9, 3, 8)$ are also isomorphic. Finally, again by Corollary 3.8 solutions $\mathcal{K}(9, 3, 1)$ and $\mathcal{K}(9, 3, 2)$ are non-isomorphic. Note that they are isomorphic to solutions from Example 2.10 for $r = 3$ and $r = 6$, respectively. The isomorphisms are given by permutations: $(285)$ and $(184572)(36)$, respectively.

For the trivial brace $(B_9(9), +, \circ)$ we have six isomorphic indecomposable solutions of multipermutational level 1: $\mathcal{K}(9, 0, a)$, with $\sigma_b(c) = a + c$, for $a \in \{1, 2, 4, 5, 7, 8\}$.

By Corollary 3.10 and Proposition 4.1 one can easily check how many indecomposable cocyclic solutions of each multipermutational level one can define on a set $X$ of cardinality $p^k$. Note that the highest possible level in this case does not exceed $k$. In particular, for each $2 \neq p$ there exists at least one solution of level $k$, but for $p = 2$ and $k > 2$ there is none. Then the smallest example of the indecomposable solution of multipermutational level 3 with cyclic permutation group can be constructed for $|X| = 27$.

**Example 4.3.** There are five non-isomorphic indecomposable solutions with $|X| = 27$ – two of multipermutational level 3: $\mathcal{K}(27, 3, 1)$ and $\mathcal{K}(27, 3, 2)$ which originate from the brace $B_3(27)$, two of multipermutational level 2: $\mathcal{K}(27, 9, 1)$ and $\mathcal{K}(27, 9, 2)$ which are obtained from the brace $B_9(27)$ and one of multipermutational level 1: $\mathcal{K}(27, 0, 1)$ constructed from the trivial brace $B_{27}(27)$.

Using Corollary 3.13 and Remark 3.16 we can quickly calculate the number of solutions and their permutational level in the case $n$ is product of powers of two primes.

**Remark 4.4.** Let $p$ and $q$ be two distinct prime numbers, $k, l \in \mathbb{Z}^+$ and $n = p^k q^l$. For $t = p^{k'} q^{l'}$ with $1 \leq k' \leq k$, $1 \leq l' \leq l$ there are

$$(p^{\min(k', k-k')} - p^{\min(k', k-k')-1})(q^{\min(l', l-l')} - p^{\min(l', l-l')-1})$$

non-isomorphic solutions $\mathcal{K}(p^k q^l, p^{k'} q^{l'}, a)$ with $a \in \mathbb{Z}_d^*$ and $d = p^{\min(k', k-k')} q^{\min(l', l-l')}$.

By Remark 3.16 they are of multipermutational level equal to $\max(\lceil \frac{k}{k'} \rceil, \lceil \frac{l}{l'} \rceil)$.

**Example 4.5.** Consider a set $X$ with $|X| = 3^3 \cdot 5^2 = 675$. All indecomposable cocyclic solutions constructed on $X$ originate from bicyclic braces. By Lemma 3.1 there are 6 such braces (up to isomorphism). By Remark 4.4 there are 25 indecomposable cocyclic solutions and they are of multipermutational level at most 3.

We focus now on multipermutation solutions of level 3 since there are not many examples in the literature. We have 10 non-isomorphic such solutions: $\mathcal{K}(675, 3 \cdot 5, a)$ for $a \in \{1, 2, 4, 7, 8, 11, 13, 14\}$ and $\mathcal{K}(675, 3 \cdot 5^2, b)$ for $b \in \{1, 2\}$.

In particular, by Theorem 3.12 combined with Corollary 3.8 we obtain the following sequence of isomorphisms:

$$\mathcal{K}(27 \cdot 25, 3 \cdot 5, 1) \cong \mathcal{K}(27, 3, 5) \times \mathcal{K}(25, 5, 3) \cong \mathcal{K}(27, 3, 2) \times \mathcal{K}(25, 5, 3) \cong \mathcal{K}(27 \cdot 25, 3 \cdot 5, 76).$$

By Remark 3.16 we can describe now the retracts of $\mathcal{K}(27 \cdot 25, 3 \cdot 5, 1)$ in each step, i.e.
$\mathrm{Ret}(\mathcal{K}(27 \cdot 25, 3 \cdot 5, 1)) \cong \mathcal{K}(45, 15, 1)$, $\mathrm{Ret}(\mathcal{K}(45, 15, 1)) \cong \mathcal{K}(3, 0, 1)$ and $|\mathrm{Ret}(\mathcal{K}(3, 0, 1))| = 1$.

Moreover we have 14 non-isomorphic solutions of multipermutational level 2: $\mathcal{K}(675, 3^2 \cdot 5, a)$ for $a \in \{1, 2, 4, 7, 8, 11, 13, 14\}$, $\mathcal{K}(675, 3^2 \cdot 5^2, b)$ for $b \in \{1, 2\}$, $\mathcal{K}(675, 3^3 \cdot 5, c)$ for $c \in \{1, 2, 3, 4\}$ and one solution $\mathcal{K}(675, 0, 1)$ of multipermutational level 1.

**Example 4.6.** We construct all (up to isomorphism) indecomposable cocyclic solutions on set $X$ of cardinality $|X| = 36 = 4 \cdot 9$. By Remark 3.16 they are multipermutation solutions of level at most 2. By [12, Corollary 4.8] there are 6 such solutions. Using Theorem 3.12 we obtain 3 of them - those originating from bicyclic braces. There will be 1 of multipermutational level 1: $\mathcal{K}(36, 0, 1) \cong \mathcal{K}(4, 0, 1) \times \mathcal{K}(9, 0, 4) \cong \mathcal{K}(4, 0, 1) \times \mathcal{K}(9, 0, 1)$. Note that $\mathcal{K}(36, 0, 1) \cong \mathcal{K}(36, 0, a)$ for any $a \in \mathbb{Z}_{36}^*$. We also have 2 non-isomorphic solutions of multipermutational level 2:

(1) for $a \in \{1, 7, 13, 19, 25, 31\}$: $\mathcal{K}(36, 12, a) \cong \mathcal{K}(4, 0, 1) \times \mathcal{K}(9, 3, 1)$;
(2) for $a \in \{5, 11, 17, 23, 29, 35\}$: $\mathcal{K}(36, 12, a) \cong \mathcal{K}(4, 0, 1) \times \mathcal{K}(9, 3, 2)$.

By Proposition 3.14 we obtain 3 non-isomorphic solutions with cyclic permutation group but not originating from the construction presented in Theorem 3.4. They are of multipermutational level 2.

(1) for $t = 9$ and any $a \in \mathbb{Z}_{36}^*$ we have a solution with $\overline{\sigma}_b(c) = a + c + 18b \pmod{36}$. It is isomorphic to $\tilde{\mathcal{K}}(4, 2, 1) \times \mathcal{K}(9, 0, 1)$;
(2) for $t = 3$ and $a \in \{1, 7, 13, 19, 25, 31\}$ we have a solution with $\overline{\sigma}_b(c) = a + 25c + 6b \pmod{36}$. It is isomorphic to $\tilde{\mathcal{K}}(4, 2, 1) \times \mathcal{K}(9, 3, 2)$;
(3) for $t = 3$ and $a \in \{5, 11, 17, 23, 29, 35\}$ we have a solution with $\overline{\sigma}_b(c) = a + 13c + 30b \pmod{36}$. It is isomorphic to $\tilde{\mathcal{K}}(4, 2, 1) \times \mathcal{K}(9, 3, 1)$.

Proposition 4.1 together with Theorem 3.12 and Proposition 3.14 allow us to compute the precise number of all non-isomorphic indecomposable cocyclic solutions of arbitrary size $n$. Table 1 shows that this number grows rapidly as $n$ increases. Comparing even with the number of all non-isomorphic left braces (see [11, Table 5.4] for example for $n = 25$ or $n = 49$) one can see that these computations confirm Theorem 3.15.

| $k$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $p = 2$ | 2 | 2 | 4 | 6 | 10 | 14 | 22 | 30 | 46 | 62 | 94 | 126 | 190 | 254 |
| $p = 3$ | 3 | 5 | 11 | 17 | 35 | 53 | 107 | 161 | 323 | 485 | 971 | 1457 | 2915 | 4373 |
| $p = 5$ | 5 | 9 | 29 | 49 | 149 | 249 | 749 | 1249 | 3749 | 6249 | 18749 | 31249 | 93749 | 156249 |
| $p = 7$ | 7 | 13 | 55 | 97 | 391 | 685 | 2743 | 4801 | 19207 | 33613 | 134455 | 235297 | 941191 | 1647085 |

TABLE 1. The number of indecomposable cocyclic solutions of order $p^k$, up to isomorphism.

Finally, let us mention the infinite indecomposable solutions $(X, \sigma, \tau)$ with $\mathcal{G}(X) \cong \mathbb{Z}$. By [8, Theorem 5.5] a left brace with multiplicative group isomorphic to the group $\mathbb{Z}$ is trivial. Then,

by [3, Theorem 14] there is, up to isomorphism, unique cocyclic infinite indecomposable solution $(\mathbb{Z}, \sigma, \tau)$ of multipermutational level 1 such that $\sigma_x(y) = y + 1$. (See also [12, Proposition 2].)

## References

[1] D. Bachiller, F. Cedó, E. Jespers, *Solutions of the Yang-Baxter equation associated with a left brace*, J. Algebra **463** (2016), 80–102.

[2] M. Castelli, F. Catino, G. Pinto, *Indecomposable involutive set-theoretic solutions of the Yang-Baxter equation*, J. Pure Appl. Algebra **223** (2019), 4477–4493.

[3] M. Castelli, F. Catino, P. Stefanelli, *Indecomposable involutive set-theoretic solutions of the Yang-Baxter equation and orthogonal dynamical extensions of cycle sets*, available at http://arxiv.org/abs/2011.10083

[4] M. Castelli, G. Pinto, W. Rump, *On the indecomposable involutive set-theoretic solutions of the Yang-Baxter equation of prime-power size*, Comm. Algebra **48** (2020), 1941–1955.

[5] F. Cedó, T. Gateva-Ivanova, A. Smoktunowicz, *On the Yang–Baxter equation and left nilpotent left braces*, J. Pure Appl. Algebra **221** (2017), 751–756.

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

[7] F. Cedó, E. Jespers, J. Okniński, *Braces and the Yang-Baxter equation*, Comm. Math. Phys. **327** (2014), 101–116. Extended version arXiv:1205.3587.

[8] F. Cedó, A. Smoktunowicz, L. Vendramin, *Skew left braces of nilpotent type*, Proc. Lond. Math. Soc. **(3) 118(6)** (2019), 1367–1392.

[9] V.G. Drinfeld, *On some unsolved problems in quantum group theory*, In: P.P. Kulish (ed.) Quantum groups, in: Lecture Notes in Math., vol. 1510, Springer-Verlag, Berlin, (1992), pp. 1–8.

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

[11] L. Guarnieri, L. Vendramin, *Skew braces and the Yang-Baxter equation*, Math. Comp. **86** (307) (2017), 2519—2534.

[12] P. Jedlička, A. Pilitowska, A. Zamojska-Dzienio, *Indecomposable involutive solutions of the Yang-Baxter equation of multipermutational level 2 with abelian permutation group*, available at http://arxiv.org/abs/2011.00229

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

[14] T. Kepka, P. Němec, *Commutative radical rings I*, Acta Univ. Carolinae Math. Phys. **48** (2007), 11–41.

[15] T. Kepka, P. Němec, *Commutative radical rings II*, Acta Univ. Carolinae Math. Phys. **49** (2008), 53–73.

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

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

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

[19] W. Rump, *Cocyclic solutions to the Yang-Baxter equation*, Proc. Amer. Math. Soc. **149** (2021), 471–479.

[20] W. Rump, *Classification of indecomposable involutive set-theoretic solutions to the Yang–Baxter equation*, Forum Math. **32** (2020), 891–903.

[21] A. Smoktunowicz, *On Engel groups, nilpotent groups, rings, braces and the Yang-Baxter equatiuon*, Trans. Am. Math. Soc. **370**(9) (2018), 6535–6564.

[22] L. Vendramin, *Problems on skew left braces*, Adv. Group Theory Appl. **7** (2019), 15–37.

(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@mini.pw.edu.pl