Classification of uniconnected involutive solutions of the Yang-Baxter equation with odd size and a Z-group permutation group

M. CASTELLI

Lecce (Italy)

Abstract
In the first part of this paper, we investigate the retraction of finite uniconnected involutive non-degenerate set-theoretic solutions of the Yang-Baxter equation by means of left braces, giving a precise description in some cases. In the core of the paper, we also use left braces to classify all the uniconnected involutive non-degenerate set-theoretic solutions having odd size and a Z-group permutation group. As an application, we classify all the uniconnected involutive non-degenerate solutions having odd square-free size.

Keywords: set-theoretic solution, Yang-Baxter equation, brace, cycle set

2020 MSC: 16T25, 81R50, 20N02, 20E22

Introduction

A set-theoretic solution of the Yang-Baxter equation on a non-empty set $X$ is a pair $(X, r)$, where $r : X \times X \to X \times X$ is a map such that the relation

$$(r \times \text{id}_X) (\text{id}_X \times r) (r \times \text{id}_X) = (\text{id}_X \times r) (r \times \text{id}_X) (\text{id}_X \times r)$$

is satisfied. The paper by Drinfel’d $^7$ moved the interest of several researchers for finding and classifying solutions of this equation in the last thirty years. Writing a solution $(X, r)$ as $r(x, y) = (\lambda_x(y) \rho_y(x))$, with $\lambda_x, \rho_x$ maps from $X$ into itself, for every $x \in X$, we say that $(X, r)$ is non-degenerate if $\lambda_x, \rho_x \in \text{Sym}_X$, for every $x \in X$, and involutive if $r^2 = \text{id}_{X \times X}$. Over the years, the involutive non-degenerate solutions have been widely studied starting from the seminal papers by Gateva-Ivanova and Van den Bergh $^{10}$, Gateva-Ivanova and Majid $^2$, and Etingov, Schedler, and Soloviev $^3$. In particular, in $^3$, Section 2 the class of indecomposable solutions was introduced. Technically, an involutive non-degenerate solution $(X, r)$ is said to be decomposable if there exists a non-trivial partition $\{Y, Z\}$ such that $(Y, r|_{Y \times Y})$ and $(Z, r|_{Z \times Z})$ are again solutions; otherwise, $(X, r)$ is called indecomposable. In the same paper, the authors studied these solutions by means of some associated algebraic structures, such as the structure...
group and the associated permutation group (see [3] for more details). In this context, a remarkable result gives a complete classification of the involutive non-degenerate solutions having a prime number of elements (see [3, Theorem 2.13]). The paper of Etingof, Scheidler and Soloviev stimulated the study of this class of solutions and in the last years several results were obtained in the classification of indecomposable solutions. In [3] and [22] a first attempt to construct examples of indecomposable involutive solutions was given by using cycle sets and left braces, an algebraic structures strictly related to involutive solutions (see [16, 17] for more details). In [4] some results involving the concrete classifications of indecomposable solutions were given: indeed, the authors completely classified the indecomposable involutive solutions having size \( pq \) (where \( p \) and \( q \) are not necessarily distinct prime numbers) and abelian permutation group. This result was extended some months later by Jedlička, Pilitowska and Zamojska-Dzenio in [12], where they classified all the indecomposable involutive solutions having multipermutation level 2 and abelian permutation group. In the last year, the classification obtained in [4] was extended by Rump in [21] and by Jedlička, Pilitowska and Zamojska-Dzenio in [13] in an other direction: indeed, a complete classification of the indecomposable solutions with cyclic permutation group (without restriction on the cardinality and the multipermutation level) was exhibited. In particular, in [13] Theorem 3.9 and Corollary 3.10, the authors provided the precise structure of the retraction of such a solutions and give a formula to compute their multipermutation level. At the same time, using different tools, in [6] Cedó, Jespers and Okniński classified the indecomposable involutive solutions having primitive permutation group, showing that they coincide with the ones having a prime number of elements.

In this paper, we study the indecomposable involutive solutions with regular permutation group. This is also motivated by a recent paper due by Rump, in which he developed a machinery (see [20, Theorems 2-3]) to classify all the indecomposable involutive solutions for which the classification of the ones with regular permutation group is the first fundamental step. Following Rump’s terminology, we will call these solutions unconnected. In the first part, we take advantage of the results obtained in [13, 21] to study the retraction of unconnected solutions by means of left braces, giving special attention on the solutions associated to cyclic left braces and the ones having abelian permutation group. In particular, we show that the retractions of these solutions can be completely understood in terms of the retraction of the associated left braces. As applications of these results, we answer to [13, Question 3.11] and we extend a result on retractability of solutions obtained in [4, Proposition 2].

In the core of the paper, we study unconnected involutive solutions having odd size and a Z-group permutation group by means of their associated left braces. Recall that a finite group is said to be a Z-group if all its Sylow subgroups are cyclic. We use the classification of cyclic left braces given in [18, 19] together with [20, Theorem 1] to develop a concrete construction of these solutions and we cut the isomorphism classes using a theorem due by Bachiller, Cedó and Jespers [2, Theorem 4.1]. In analogy to the results obtained in [13, Theorem 3.15] and [13, Corollary 3.10] for involutive solutions with cyclic permutation group, we exhibit a set of invariants for unconnected solutions having odd size and a Z-group permutation group and a formula to compute their multipermutation levels. As an application, we provide a complete classification of unconnected involutive non-degenerate solutions having square-free odd order.
1. Cycle sets: basic definitions and results

In this section we give the background informations involving cycle sets that will be useful in the following. In [16], a one-to-one correspondence between solutions and a special class of cycle sets, i.e., non-degenerate cycle sets, was established. To illustrate this correspondence, let us firstly recall the following definition.

**Definition 1.1** *(p. 45, [16])* A pair \((X, \cdot)\) is said to be a cycle set if each left multiplication \(\sigma_x : X \rightarrow X, y \mapsto x \cdot y\) is invertible and

\[(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z),\]

for all \(x, y, z \in X\). Moreover, a cycle set \((X, \cdot)\) is called non-degenerate if the squaring map \(x \mapsto x \cdot x\) is bijective.

From now on, for a cycle set we mean a non-degenerate cycle set.

**Proposition 1.2** *(Propositions 1-2, [16])* Let \((X, \cdot)\) be a cycle set. Then the pair \((X, r)\), where

\[r(x, y) := (\sigma_x^{-1}(y), \sigma_x^{-1}(y) \cdot x),\]

for all \(x, y \in X\), is a solution of the Yang-Baxter equation which we call the associated solution to \((X, \cdot)\). Moreover, this correspondence is one-to-one.

In [8], Etingof, Schedler and Soloviev introduced the so-called retract relation, an equivalence relation on \(X\) which we denote by \(\sim_r\). If \((X, r)\) is a solution, then \(x \sim_r y\) if and only if \(\lambda_x = \lambda_y\), for all \(x, y \in X\). In this way, we can define canonically another solution, having the quotient \(X/\sim_r\) as underlying set, which is named retraction of \((X, r)\) and is indicated by \(\text{Ret}(X, r)\). As one can expect, the retraction of a solution corresponds to the retraction of a cycle set. Technically, in [16] Rump defined the binary relation \(\sim_{\sigma}\) on \(X\) by \(x \sim_{\sigma} y :\Leftrightarrow \sigma_x = \sigma_y\) for all \(x, y \in X\), and he showed that it is a congruence of \((X, \cdot)\). Moreover, he proved that the quotient \(X/\sim_{\sigma}\), which we denote by \(\text{Ret}(X)\), is a cycle set whenever \(X\) is non-degenerate and he called it the retraction of \((X, \cdot)\). As the name suggests, if \((X, \cdot)\) is the cycle set associated to a solution \((X, r)\), then the retraction \(\text{Ret}(X)\) is the cycle set associated to \(\text{Ret}(X, r)\). Besides, a cycle set \(X\) is said to be irretractable if \(\text{Ret}(X) = X\), otherwise it is called retractable.

To study cycle sets (and hence involutive solutions), one can consider the retraction-process. Therefore the following definition is of crucial importance.

**Definition 1.3** A cycle set \(X\) has multipermutation level \(n\) if \(n\) is the minimal non-negative integer such that \(\text{Ret}^n(X)\) has cardinality one, where

\[\text{Ret}^0(X) := X \quad \text{and} \quad \text{Ret}^i(X) := \text{Ret}(\text{Ret}^{i-1}(X)), \quad \text{for } i > 0.\]

From now on, we will write \(\text{mpl}(X) = n\) to indicate that \(X\) has multipermutation level \(n\).

A standard subgroup associated to a cycle set \(X\) is the permutation group generated by the set \(\{\sigma_x \mid x \in X\}\). It will be denoted by \(G(X)\) and we call it the associated permutation group. Obviously, in terms of solutions, the associated permutation group is exactly the permutation group generated by the set \(\{\lambda_x \mid x \in X\}\).

In this paper, we focus our attention on cycle sets that are indecomposable. In particular, among these cycle sets, we will consider the uniconnected ones.
Definition 1.4. A cycle set \((X, \cdot)\) is said to be indecomposable if the permutation group \(G(X)\) acts transitively on \(X\), otherwise it is said to be decomposable. Moreover, \(X\) is said to be uniconnected if \(G(X)\) acts regularly on \(X\).

Clearly, an uniconnected cycle set is indecomposable, but the converse is not necessarily true.

Remark 1.5. In the rest of the paper, we will study indecomposable solutions by their associated cycle sets. In every case, all the results involving cycle sets can be translated in terms of solutions by Proposition 1.2.

2. Left braces: basic definitions and results

Now, we give the backgroud informations of left braces. We start giving the definition of these algebraic structures using the formulation contained in [5]. For the original formulation, we refer the reader to [17].

Definition 2.1 ([5], Definition 1). A set \(A\) endowed of two operations + and \(\circ\) is said to be a left brace if \((A, +)\) is an abelian group, \((A, \circ)\) a group, and the equality \(a \circ (b + c) = a \circ b - a + a \circ c\) follows, for all \(a, b, c \in A\).

From now on, if \((A, +, \circ)\) is a left brace, the group \((A, +)\) will be called the additive group and the group \((A, \circ)\) will be called the multiplicative group. An example of left brace can be constructed taking and abelian group \((A, +)\) and setting \(a \circ b := a + b\) for all \(a, b \in A\). Through the paper, we call these left braces trivial. Left braces \((A, +, \circ)\) with cyclic multiplicative group are intensively studied (see for example [18, 19]).

Example 1. Let \(p\) be a prime number, \(k, t\) natural numbers such that \(t \leq k\), \((A, +) = (\mathbb{Z}/p^k\mathbb{Z}, +)\) and the binary operation \(\circ\) on \(A\) by \(a \circ b := a + b + ab^t\) for all \(a, b \in A\). Then the triple \((A, +, \circ)\) is a left brace and \((A, \circ)\) is a cyclic group.

In [18], Rump showed that every left brace with prime-power size, for some odd prime number, and cyclic multiplicative group can be constructed as in the previous example: for this reason, we will indicate this left brace as \(B(p, k, t)\). Moreover, it is well-known that every left brace with odd size and cyclic multiplicative group is isomorphic to the direct product of left braces having prime-power size and cyclic multiplicative group (for more details, see [18, 19]).

A simple way to construct other left braces, which will be useful in the next sections, is the semidirect product of left braces. Given a left brace \((A, +, \circ)\), an automorphism of the left brace \(A\) is a bijective function \(\alpha\) from \(A\) to itself such that \(\alpha \in \text{Aut}(A, +) \cap \text{Aut}(A, \circ)\). Of course, the set consisting of all the automorphisms of \((A, +, \circ)\) is a subgroup of the permutations group on \(A\) and we indicate it by \(\text{Aut}(A, +, \circ)\). If \(A_1\) and \(A_2\) are left braces and \(\alpha\) a homomorphism from \((A_2, \circ)\) to \(\text{Aut}(A_1, +, \circ)\), the semidirect product of the left braces \(A_1\) and \(A_2\) via \(\alpha\) is the left brace \((A_1 \times A_2, +, \circ)\) such that \((A_1 \times A_2, +)\) is the direct product of the additive groups \((A_1, +)\) and \((A_2, +)\) and \((A_1 \times A_2, \circ)\) is the semidirect product of the multiplicative groups \((A_1, \circ)\) and \((A_2, \circ)\) via \(\alpha\). In this way, the operations + and \(\circ\) of the semidirect product are given by

\[ (a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2) \]

\[ a_1 \circ (b_1, b_2) := (a_1 \circ b_1, \alpha_{b_1}(a_2)) \]
Let $(a_1, a_2) \diamond (b_1, b_2) := (a_1 \circ b_1^{a_2}, a_2 \circ b_2)$ for all $(a_1, a_2), (b_1, b_2) \in A_1 \times A_2$, where $b_1^{a_2}$ simply means $\alpha(a_2)(b_1)$, as the function $\alpha$ is clear from the context.

Given a left brace $A$ and $a \in A$, let us denote by $\lambda_a : A \rightarrow A$ the map from $A$ into itself defined by $\lambda_a(b) := -a + a \circ b$, for all $b \in A$. As shown in [17, Proposition 2] and [3, Lemma 1], these maps have special properties. We recall them in the following proposition.

**Proposition 2.2.** Let $A$ be a left brace. Then, the following are satisfied:

1) $\lambda_a \in \text{Aut}(A, +)$, for every $a \in A$;

2) the map $\lambda : A \rightarrow \text{Aut}(A, +)$, $a \mapsto \lambda_a$ is a group homomorphism from $(A, \circ)$ into $\text{Aut}(A, +)$.

The map $\lambda$ is of crucial importance to construct cycle sets (and hence involutive solutions) using left braces, as one can see in the following propositions.

**Proposition 2.3** (Lemma 2, [5]). Let $A$ be a left brace and $\cdot$ the binary operation on $A$ given by

$$a \cdot b := \lambda_a^{-1}(b)$$

for all $a, b \in A$. Then, $(A, \cdot)$ is a decomposable cycle set.

Before giving the following result, recall that a subset $X$ of a left brace $(A, +, \circ)$ is said to be a *cycle base* if $X$ is a union of orbits respect to the action $\lambda$ and generates the additive group $(A, +)$. Moreover, a cycle base that is a single orbit is called *transitive cycle base*.

**Proposition 2.4** (Theorem 2, [20]). Let $A$ be a left brace, $X$ a transitive cycle base and $g \in X$. Define on $A$ the binary operation $\ast$

$$a \ast b := (\lambda_a(g))^{-1} \circ b,$$

for all $a, b \in A$. Then, $(A, \ast)$ is an uniconnected cycle set such that $\mathcal{G}(A) \cong (A, \circ)$. Conversely, every uniconnected cycle set can be constructed in this way.

In the two previous propositions, we saw that a left brace $A$ provide a decomposable cycle set and several indecomposable cycle sets, which in full generality are not isomorphic. The cycle set provided by Proposition 2.3 will be called the *decomposable associated cycle set*, and similarly a cycle set provided by Proposition 2.4 will be called an *uniconnected associated cycle set*.

Similarly to rings, the notion of ideal of a left brace was introduced in [17] and reformulated in [3, Definition 3].

**Definition 2.5.** Let $A$ be a left brace. A subset $I$ of $A$ is said to be a *left ideal* if it is a subgroup of the multiplicative group and $\lambda_a(I) \subseteq I$, for every $a \in A$. Moreover, a left ideal is an *ideal* if it is a normal subgroup of the multiplicative group.
Given an ideal $I$, it holds that the structure $A/I$ is a left brace called the quotient left brace of $A$ modulo $I$. A special ideal of a left brace, introduced in [17], is the socle. In the terms of [5, Section 4], it is the following.

**Definition 2.6.** Let $A$ be a left brace. Then, the set
\[
\text{Soc}(A) := \{ a \in A \mid \forall b \in A \quad a + b = a \circ b \}
\]
is named socle of $A$.

Clearly, $\text{Soc}(A) := \{ a \in A \mid \lambda_a = \text{id}_A \}$. It is well-known that $\text{Soc}(A)$ is an ideal of $A$ and it is strongly related to the retraction of its decomposable associated cycle set. The following proposition is implicitly contained in [17, Proposition 7] and [5, Lemma 3].

**Proposition 2.7.** Let $A$ be a left brace and $(A, \cdot)$ the decomposable associated cycle set. If $(A/\text{Soc}(A), \cdot)$ is the decomposable associated cycle set of the left brace $A/\text{Soc}(A)$, then $(A/\text{Soc}(A), \cdot)$ coincides with the retraction $\text{Ret}(A, \cdot)$ of $(A, \cdot)$.

**Definition 2.8.** A left brace $A$ has finite multipermutation level if the decomposable associated cycle set $(A, \cdot)$ has finite multipermutation level. If $n$ is a natural number and a left brace $A$ is such that the decomposable associated cycle set $(A, \cdot)$ has multipermutation level equal to $n$, then $A$ is said to be of multipermutation level $n$.

**Example 2.** Let $A$ be the left brace $B(p, k, t)$ given in Example [1]. Then, the multipermutation level of $A$ is $\lceil \frac{k}{t} \rceil$, where, if $z$ is a real number, $\lceil z \rceil$ is the greatest integer part of $z$ (see [13, Corollary 3.10]). Therefore, if $C$ is a left brace isomorphic to the direct product $B(p_1, k_1, t_1) \times \ldots \times B(p_n, k_n, t_n)$, for some distinct prime numbers $p_1, \ldots, p_n$, then the multipermutation level is equal to $\max\{\lceil \frac{k_1}{t_1} \rceil, \ldots, \lceil \frac{k_n}{t_n} \rceil\}$.

We conclude the section focusing our attention on Proposition 2.4. Note that the cycle sets obtained using this results can be also obtained using a construction developed in [2]. Indeed, if in Theorem 3.1 of [2] we take $I := \{i\}$ as a set of size one given by a transitive cycle base $i$, $a_1$ an element of $i$, $J_i := \{j\}$ a set of size one and $K_{i,j} := \{0\}$ the trivial subgroup of the stabilizer of $a_i$ under the action $\lambda$, we can construct all the cycle sets provided in Proposition 2.4. Moreover, in [2, Theorem 4.1] a method to verify when two cycle sets, having permutation groups isomorphic as left braces, are isomorphic is provided. In the following we reformulate the result in our case.

**Proposition 2.9 (Theorem 4.1, [2]).** Let $A$ be a left brace, $X_1$ and $X_2$ a transitive cycle bases, $g_1 \in X_1$ and $g_2 \in X_2$. Let $A_1$ (resp. $A_2$) be the cycle set constructed as in Proposition 2.4 starting from $g_1$ and $X_1$ (resp. $g_2$ and $X_2$). Then, $A_1$ and $A_2$ are isomorphic if and only if there exist $z \in A$ and $\psi \in \text{Aut}(A, +, \circ)$ such that $\psi(x_1) = \lambda_z(x_2)$.

### 3. Retraction of uniconnected cycle sets

In this section, we study the retraction of uniconnected cycle sets by means of left braces. We show that, in some cases, the underlying set of the retraction of these cycle sets is the quotient of the associated left brace by its socle and we use these facts to give an answer to [13, Question 3.11]. The control of the retraction-structure of these cycle sets will be useful in the last part of the section, in which we extend the results obtained in [3] on the retractability of indecomposable cycle sets with abelian permutation group.
Lemma 3.1. Let $A$ be a left brace. Suppose that $A$ has a transitive cycle base and let $(A, \bullet)$ be an uniconnected associated cycle set. Moreover, let $g \in A$ be an element of a transitive cycle base such that $a \bullet b = \lambda_a(g)^- \circ b$ for all $a, b \in A$. Then, $\text{Ret}(A, \bullet)$ coincides with the set of the left cosets $A/H$, where $H$ is equal to the subgroup of $(A, \circ)$ given by $H := \{ h \mid h \in A, \lambda_h(g) = g \}$. Moreover, the socle of $A$ is contained in $H$.

Proof. By a standard calculation, one can show that $H$ is a subgroup of $(A, \circ)$ containing $\text{Soc}(A)$. Since $\lambda$ is a homomorphism from $(A, \circ)$ to $\text{Aut}(A, +)$, it follows that $\sigma_a = \sigma_b$ if and only if $\lambda_a^{- \circ b}(g) = \lambda_a^{- \circ b}(g) = g$, therefore the retract relation coincides with the equivalence relation induced by $H$.

In general, we are not able to state if for a left brace $A$ the subgroup $H$ of the previous proposition is equal to $\text{Soc}(A)$. However, this surely happens in some cases, which we see in the following results. At first, we need a lemma. Recall that if $A$ is a cyclic left brace, i.e. a left brace with cyclic additive group, then it surely has a transitive cycle base: it is sufficient to consider the orbit of a generator $a$ of the additive group respect to the action $\lambda$.

Lemma 3.2. Let $(A, +, \circ)$ be a finite cyclic left brace, $X$ a transitive cycle base and $g \in X$. Then, $g$ is a generator of the additive group $(A, +)$.

Proof. If $g$ has order $n < |A|$, since the maps $\lambda_a$ preserve the order in the additive group, it follows that all the elements of $X$ have additive order equal to $n$ and therefore all the elements of $A$ have additive order that divides $n$, a contradiction.

Proposition 3.3. Let $A$ be a finite cyclic left brace and $(A, \bullet)$ an uniconnected associated cycle set. Moreover, let $g \in A$ be an element of a transitive cycle base such that $a \bullet b = \lambda_a(g)^- \circ b$ for all $a, b \in A$ and $H$ the subgroup of $(A, \circ)$ such that $\text{Ret}(A, \bullet) = A/H$. Then $H$ is equal to $\text{Soc}(A)$.

Proof. The inclusion $\text{Soc}(A) \subseteq H$ follows by Lemma 3.1. By Lemma 3.2 if $h$ is an element of $H$ the equality $\lambda_h(g) = g$ implies $\lambda_h = \text{id}_A$, therefore $H \subseteq \text{Soc}(A)$.

Proposition 3.4. Let $A$ be a finite left brace. Suppose that $A$ has a transitive cycle base and let $(A, \bullet)$ be an uniconnected associated cycle set. Moreover, let $g \in A$ be an element of a transitive cycle base $X$ such that $a \bullet b = \lambda_a(g)^- \circ b$ for all $a, b \in A$ and let $H$ be the subgroup of $(A, \circ)$ such that $\text{Ret}(A, \bullet) = A/H$. If $H$ is a normal subgroup of $(A, \circ)$, the subgroup $H$ is equal to $\text{Soc}(A)$.

Proof. The inclusion $\text{Soc}(A) \subseteq H$ follows by Lemma 3.1. Now, all the elements of $X$ are in the same orbit under the action $\lambda$, hence their stabilizers are conjugated in $(A, \circ)$. Since the stabilizer of $g$, which is equal to $H$, is a normal subgroup of $(A, \circ)$, it follows that $H$ fixes all the elements of $X$. The thesis follows since the additive group generated by $X$ is $A$.

The previous propositions are useful to understand, in some cases, the relation between the retraction-process of the decomposable associated cycle set $(A, \cdot)$ and an uniconnected associated cycle set $(A, \bullet)$. 

7
Theorem 3.5. Let $A$ be a finite cyclic left brace, $(A, \cdot)$ the decomposable associated cycle set and $(A, \ast)$ an unconnected associated cycle set. Moreover, let $g \in A$ an element of a transitive cycle base such that $a \ast b = \lambda_a(g)^{-1} \circ b$ for all $a, b \in A$. Then, $(A, \cdot)$ and $(A, \ast)$ are multipermutation cycle sets and $mpl(A, \cdot) = mpl(A, \ast)$. Moreover, the underlying sets of $Ret^n(A, \cdot)$ and $Ret^n(A, \ast)$ coincide, for every $n \in \mathbb{N}$.

Proof. Since $(A, \cdot)$ has regular permutation group, by [14, Corollary 3.3] it is retractable, hence the subgroup $H$ of $(A, \circ)$ such that $Ret(A, \bullet) = A/H$ is not trivial. Moreover, by Proposition 3.3 and Proposition 2.7 $H$ is equal to $Soc(A)$ and $Ret(A, \cdot)$ and $Ret(A, \ast)$ have as underlying set the quotient $A/Soc(A)$. By standard calculation, if we indicate by $(A/Soc(A), \bullet)$ the uniconnected cycle set associated to the left brace $A/Soc(A)$ given by

$$(a + Soc(A)) \ast (b + Soc(A)) := \lambda_{a+Soc(A)}(g + Soc(A))^{-1} \circ (b + Soc(A)),$$

it follows that $Ret(A, \bullet) = (A/Soc(A), \bullet)$. Moreover, the quotient left brace $A/Soc(A)$ is again a cyclic left brace. Therefore, the thesis follows by an easy induction on $|A|$. □

In [10] Rump used the classification of cyclic left braces to show that they have not trivial socle. Here, we use the previous theorem to show this result in a different way.

Corollary 3.6 (pg. 319, [10]). Let $A$ be a finite cyclic left brace. Then, the socle of $A$ is not trivial.

Proof. By the previous theorem, the decomposable associated cycle set is retractable hence the thesis follows by Proposition 2.7. □

In the following, we consider left braces $A$ whose multiplicative group is a so-called Dedekind group, i.e., a group in which every subgroup is normal (see [15, pg. 143]).

Theorem 3.7. Let $A$ be a finite left brace such that $(A, \circ)$ is a Dedekind group and $(A, \cdot)$ the decomposable associated cycle set. Suppose that $A$ has a transitive cycle base and let $(A, \ast)$ be an unconnected associated cycle set. Moreover, let $g \in A$ be an element of a transitive cycle base such that $a \ast b = \lambda_a(g)^{-1} \circ b$ for all $a, b \in A$. Then, $(A, \ast)$ and $(A, \cdot)$ are multipermutation cycle sets and $mpl(A, \cdot) = mpl(A, \ast)$. Moreover, the underlying sets of $Ret^n(A, \cdot)$ and $Ret^n(A, \ast)$ coincide, for every $n \in \mathbb{N}$.

Proof. Since $(A, \ast)$ has regular permutation group, by [14, Corollary 3.3] it is retractable, hence the subgroup $H$ of $(A, \circ)$ such that $Ret(A, \bullet) = A/H$ is not trivial. By Proposition 3.3 and Proposition 2.7 $H$ is equal to $Soc(A)$ and $Ret(A, \cdot)$ and $Ret(A, \ast)$ have as underlying set the quotient $A/Soc(A)$. Similarly to the previous corollary, if we indicate by $(A/Soc(A), \bullet)$ the uniconnected cycle set associated to the left brace $A/Soc(A)$ given by

$$(a + Soc(A)) \ast (b + Soc(A)) := \lambda_{a+Soc(A)}(g + Soc(A))^{-1} \circ (b + Soc(A)),$$

it follows that $Ret(A, \bullet) = (A/Soc(A), \bullet)$. Moreover, $\{\lambda_x(g) + Soc(A) \mid x \in A\}$ is a transitive cycle base of $(A/Soc(A), \cdot)$ and $(A/Soc(A), \circ)$ is again a Dedekind group. Therefore, the thesis follows by an easy induction on $|A|$. □

Remark 3.8. 1) In [13, Question 3.11], the authors noted that, given a cyclic left brace $A$ having prime-power size and abelian multiplicative group, the multipermutation level of the decomposable associated cycle set coincides with the one of
an uniconnected associated cycle set and they asked if this is a coincidence or there is a more general mechanism hidden behind. Theorems 3.5 and 3.7 show that this is not a mere coincidence.

2) Theorems 3.5 and 3.7 also show that the retraction of the cycle sets belonging to these classes can be simply obtained considering the quotient module the socle by the associated left brace. By an iteration-process, this idea allow to obtain the \(m\)-th retraction, for all \(m \in \mathbb{N}\). In this way, one can obtain [13, Theorem 3.9] as a corollary.

We close the section extending the result on retractability obtained in [4, Proposition 2] for indecomposable cycle sets with abelian permutation group.

**Theorem 3.9.** Let \(X\) be an uniconnected cycle set and suppose that the permutation group \(\mathcal{G}(X)\) is a Dedekind group. Then, \(X\) is a multipermutation cycle set.

**Proof.** Let \(A\) be the left brace constructed as in Proposition 2.4 such that an indecomposable associated cycle set \((A, \bullet)\) is isomorphic to \(X\). Then, the group \((A, \circ)\) is isomorphic to \(\mathcal{G}(X)\), hence the thesis follows by Theorem 3.7 applied to the left brace \(A\).

The following example, which closes the section, ensures the existence of an uniconnected cycle set having permutation group isomorphic to a non-abelian Dedekind group.

**Example 3.** Let \((A, +, \circ)\) the left brace of size 8 given by \((A, +):= (\mathbb{Z}/8\mathbb{Z}, +)\) and \((A, \circ)\) the group structure on \(\mathbb{Z}/8\mathbb{Z}\) given by

\[
a_1 \circ a_2 := a_1 + 3^{a_1} a_2
\]

for all \(a_1, a_2 \in A\). Then, by [13, Theorem 3.1] \((A, +, \circ)\) is a left brace such that \((A, \circ)\) is isomorphic to the quaternion group of size 8. Since \((A, +)\) is cyclic, the left brace has a transitive cycle base. Therefore, if \((A, \bullet)\) is an uniconnected associated cycle set, by Proposition 2.4 we have that \(\mathcal{G}(A)\) is isomorphic to \((A, \circ)\).

4. The cyclic left braces with odd size and a Z-group permutation group

This small section, which does not contains new "genuine" results, aims to show that cyclic left braces with odd size and a Z-group permutation group can be constructed as a particular semidirect product of left braces. The results contained in this section are implicitly contained in [19], but we exhibit them in a comfortable form for our scopes.

We start recalling that in [19] Rump showed that a cyclic left brace \(A\) is isomorphic to an iterated semidirect product of cyclic left braces \((... \times B_m \times B_{m-1} \times ... \times B_2) \times B_1\), where the left braces \(B_i\) are constructed on a Sylow basis of the multiplicative group \((A, \circ)\). Given the left braces \(B_1, ..., B_m\) having respectively size \(p_1^{a_1}, ..., p_m^{a_m}\) with \(p_i < p_{i+1}\), the whole cyclic left brace \(A\) is completely determined by the action of \(B_i\) on \(B_j\) (see [19, Sections 3-4]), which we denote by \(\alpha_{i,j}\), for all \(i, j \in \{1, ..., m\}\) with \(j > i\). By [19, Proposition 5] we have that if \(B_j\) is not trivial as left brace, then the action \(\alpha_{i,j}\) must be trivial for all \(i \in \{1, ..., m\}\) with \(j > i\). Moreover, in [19, Proposition 14] it was shown that the socle of \((... \times B_m \times B_{m-1} \times ... \times B_2) \times B_1\) is the ideal \(S_m \times ... \times S_1\), where \(S_i = Soc(B_i) \cap C_{B_i}(B_{i+1} \times ... \times B_m, \circ)\) and \(C_{B_i}(B_{i+1} \times ... \times B_m, \circ)\) is the set
of the elements of \((B_i, \circ)\) which commutes with the subgroup \((B_{i+1} \times \ldots \times B_m, \circ)\), for all \(i \in \{1, \ldots, m\}\). The following proposition is useful to construct a family of cyclic left braces.

**Proposition 4.1.** Let \(r, m, v \in \mathbb{N} \cup \{0\}\) such that \(m \leq r\). Moreover, let \(\alpha_1, \ldots, \alpha_r, \gamma_1, \ldots, \gamma_v\) be natural numbers and \(P : = \{p_1, \ldots, p_r, q_1, \ldots, q_v\}\) a set of distinct odd prime numbers such that \(p_i < p_{i+1}\), for all \(i = 1, \ldots, r - 1\). Suppose that \(A_1, \ldots, A_v\) are cyclic left braces and that \(|A_i| = q_i^\alpha_i\) for all \(i = 1, \ldots, v\). Let \(B_1, \ldots, B_r\) be cyclic left braces of size respectively \(p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}\) such that \(B_i\) has multipermutation level 1 for all \(i = 1, \ldots, r\) and suppose that \(\alpha\) is a homomorphism from \((B_1 \times \ldots \times B_m, \circ)\) to \(\text{Aut}(B_{m+1} \times \ldots \times B_r, +)\) such that \(\alpha_{i|m_i}\) is not trivial for all \(i \in \{1, \ldots, m\}\) and \(|\alpha(B_1 \times \ldots \times B_m) \cap \text{Aut}(B_i)| > 1\), for all \(i \in \{m + 1, \ldots, r\}\).

Denote by \(A\) the direct product of left braces \((A_1 \times \ldots \times A_v)\) and by \(B\) the semidirect product of groups \((B_{m+1} \times \ldots \times B_r) \rtimes_{\alpha} (B_1 \times \ldots \times B_m)\). Then, \(\alpha\) makes the structure \(A \times B\) onto a cyclic left brace.

**Proof.** Since \(B_{m+1} \times \ldots \times B_r\) is a trivial left brace, \(\alpha\) is a homomorphism from \((B_1 \times \ldots \times B_m, \circ)\) to \(\text{Aut}(B_{m+1} \times \ldots \times B_r, +)\), therefore it makes \(A := A \times B\) onto a left brace structure with cyclic additive group.

As a weaker converse of Proposition 4.1, we provide the following result.

**Proposition 4.2.** Let \((A, +, \circ)\) be a cyclic left brace having odd size and such that \((A, \circ)\) is a Z-group. Then, \(A\) can be constructed as in Proposition 4.1.

**Proof.** By Chapter 9, \((A, \circ)\) is isomorphic to a semidirect product of two cyclic groups \(C_1\) and \(C_2\) having coprime order. Let \(r, m, \alpha_1, \ldots, \alpha_r, \in \mathbb{N}, p_1, \ldots, p_r\) distinct prime numbers such that \(m \leq r\), \(C_2 \cong \mathbb{Z}/p_1^{\alpha_1} \mathbb{Z} \times \ldots \mathbb{Z}/p_r^{\alpha_r} \mathbb{Z}\) and \(C_1 \cong \mathbb{Z}/p_{m+1}^{\gamma_1} \mathbb{Z} \times \ldots \mathbb{Z}/p_r^{\gamma_v} \mathbb{Z}\). Then, \((A, \circ)\) is isomorphic to \(C_1 \rtimes_{\beta} C_2\) for some homomorphism \(\beta\) from \(C_2\) to \(\text{Aut}(C_1)\).

If \(B_{m+1}, \ldots, B_r\) are the Sylow subgroups of \(C_1\) and \(B_1, \ldots, B_m\) are the ones of \(C_2\), the set \(\{B_1, \ldots, B_r\}\) can be identified with a Sylow basis of \(A\), hence by Sections 3-4 the whole left brace is determined by \(\beta\) and we can suppose that \(p_i < p_j\) for all \(i \in \{1, \ldots, m\}\) and \(j \in \{m + 1, \ldots, r\}\) whenever the induced action of \(B_i\) on \(B_j\) is not trivial. Let \(S\) be the subset of \(\{B_1, \ldots, B_r\}\) given by the elements \(B_j\) such that \(B_j \subseteq \ker(\beta)\) if \(j \in \{1, \ldots, m\}\) or \(|\beta(A) \cap \text{Aut}(B_j)| = 1\) if \(j \in \{m + 1, \ldots, r\}\). Define \(\hat{A}\) as the subgroup of \((A, \circ)\) given by \(\hat{A} := \Pi_{B_i \in \hat{S}} B_i\) and \(\hat{B}\) the subgroup of \((A, \circ)\) given by \(\hat{B} := (\Pi_{B_i \in \{B_{m+1}, \ldots, B_r\}} S B_j) \rtimes_{\alpha} (\Pi_{B_i \in \{B_1, \ldots, B_m\}} S B_i)\), where \(\alpha\) is the restriction of \(\beta\) onto \(\Pi_{B_i \in \{B_1, \ldots, B_m\}} S B_i\). By Proposition 2 \(B_j\) must be a trivial left brace for all \(B_j \in \{B_{m+1}, \ldots, B_r\}\). Then, as left brace, \(A\) is isomorphic to \(\hat{A} \times \hat{B}\). By a standard verification, one can check that \(\hat{A}, \hat{B}\) and \(\alpha\) are the same as in Proposition 4.1.

5. Classification of uniconnected cycle sets with odd size and a Z-group permutation group

In this section we construct and classify, by means of left braces, the uniconnected cycle sets with odd size and a Z-group permutation group. Moreover, we also use left braces to provide a formula useful to compute the multipermutation level of these cycle sets. In that regard, we start showing that the multipermutation level is always finite.
Corollary 5.1. Every uniconnected cycle set having odd size and with a Z-group permutation group has finite multipermutation level, which is equal to the one of its associated left brace.

Proof. Let $X$ be an uniconnected cycle set having odd size and with a Z-group permutation group. By [19, Corollary 2] the associated left brace has cyclic additive group, hence the thesis follows by [10, Corollary at pg. 319] and Theorem 3.5. □

Convention 1. In order to give the following results, we fix some notations. If $(A, +, \circ)$ is a cyclic left brace as in Proposition 4.1 we indicate by $\bar{A}$ and $\bar{B}$ the left braces constructed as in Proposition 4.2, such that $A = \bar{A} \times \bar{B}$. In this way, $\bar{B}$ can be written as a semidirect product of left braces $(B_{m+1} \times \ldots \times B_r) \rtimes_{\alpha} (B_1 \times \ldots \times B_m)$, where $\alpha, B_1, \ldots, B_r$ clearly are as in Proposition 4.1. Following the same proposition, $\bar{A}$ can be written as direct product of the left braces $A_1, \ldots, A_v$. Moreover, there exist a prime numbers, which we indicate by $q_1, \ldots, q_v, p_1, \ldots, p_r$, and a natural numbers, which we indicate by $\gamma_1, \ldots, \gamma_v, \beta_1, \ldots, \beta_r$, such that $|A_i| = q_i^{\gamma_i}$ for all $i \in \{1, \ldots, v\}$ and $|B_i| = p_i^{\beta_i}$ for all $i \in \{1, \ldots, r\}$.

We indicate by $I_j$ the subgroup of the left brace $B_j$ given by $I_j := \text{Soc}(B_j) \cap \text{Ker}(\alpha)$, for all $j \in \{1, \ldots, m\}$. Finally, we will indicate by $d_i$ the natural number such that $|\text{Soc}(A_i)| = q_i^{d_i}$, for all $i \in \{1, \ldots, v\}$, and similarly we indicate by $f_i$ the natural number such that $|\text{Soc}(B_i)| = p_i^{f_i}$, for all $i \in \{1, \ldots, m\}$, and by $\beta_i$ the natural number such that $|I_i| = p_i^{\beta_i}$, for all $i \in \{1, \ldots, m\}$.

By Corollary 5.1 every uniconnected cycle set having odd size and with a Z-group permutation group has finite multipermutation level: in the following, we provide a formula to compute this number. At first, we show a corollary useful for this scope.

Corollary 5.2. The socle of $A$ is equal to $\text{Soc}(\bar{A}) \times (B_{m+1} \times \ldots B_r \times I_1 \times \ldots \times I_m)$. In particular, $A/\text{Soc}(A)$ has cyclic multipermutative group.

Proof. Since $A$ is equal to the direct product of left braces $\bar{A} \times \bar{B}$, the socle of $A$ is equal to the direct product $\text{Soc}(\bar{A}) \times \text{Soc}(\bar{B})$. By [19, Proposition 14], we have that $\text{Soc}(\bar{B})$ is equal to $B_{m+1} \times \ldots B_r \times I_1 \times \ldots \times I_m$. In this way, the quotient $(A/\text{Soc}(A), \circ)$ is the group $(\bar{A}/\text{Soc}(\bar{A}) \times B_1/I_1 \times \ldots \times B_m/I_m, \circ)$, hence it is cyclic. □

Theorem 5.3. The following equalities hold:

$$mpl(X) = mpl(A) = \max\{\max_{j \in \{1, \ldots, v\}}\left\lfloor \frac{\gamma_j - d_j}{d_j} \right\rfloor, \left\lfloor \frac{\beta_1 - f_1}{f_1} \right\rfloor, \ldots, \left\lfloor \frac{\beta_m - f_m}{f_m} \right\rfloor\} + 1,$$

where $X$ is an uniconnected associated cycle set of $A$.

Proof. Clearly $mpl(A)$ is equal to $1 + mpl(A/\text{Soc}(A))$. Now, $A_1, \ldots, A_v, B_1, \ldots, B_m$ have distinct prime-power orders; moreover, $|A_i/\text{Soc}(A_i)| = q_i^{\gamma_i - d_i}$ for all $i \in \{1, \ldots, v\}$ and $|B_i/\text{Soc}(B_i)| = p_i^{\beta_i - f_i}$ for all $i \in \{1, \ldots, m\}$. Since $A/\text{Soc}(A)$ has cyclic multipermutation group, by the previous proposition and Example 2 it follows that $mpl(A/\text{Soc}(A))$ is the number

$$\max\{\max_{j \in \{1, \ldots, v\}}\left\lfloor \frac{\gamma_j - d_j}{d_j} \right\rfloor, \left\lfloor \frac{\beta_1 - f_1}{f_1} \right\rfloor, \ldots, \left\lfloor \frac{\beta_m - f_m}{f_m} \right\rfloor\},$$

hence the second equality of the statement follows. The first equality follows by Theorem 3.5. □
Clearly, if $A$ as cyclic group, i.e. $B$ is the trivial left brace $\{0\}$, the multipermutation level of $A$ is equal to $\max_{j \in \{1, \ldots, v\}} \lceil \frac{a_j - d_j}{d_j} \rceil + 1$: this is consistent with [13, Corollary 3.10].

**Example 4.** Let $p_1, p_2$ be distinct odd prime numbers, with $p_1 < p_2$ and suppose that $p_1$ divides $p_2 - 1$. Suppose that $m = 1$, $r = 2$, $A = \{0\}$ and $B$ is the non-abelian semidirect product of the two trivial left braces $B_1$ and $B_2$ having size $p_1$ and $p_2$, respectively. Then, $\beta_1 = \beta_2 = 1$, $f_1 = 1$, $f_1 = 0$ and $I_1 = \{0\}$, therefore $A = B$ and $mpl(A) = \lceil \frac{21 - f_1}{f_1} \rceil + 1 = 2$.

Now, in the rest of the section we want to classify all the uniconnected cycle set having odd size and with a $Z$-group permutation group, that can be obtained by using the results contained in [14, 20].

**Corollary 5.4.** Let $(A, +, \circ)$ be a cyclic left brace as in Proposition 4.2. Then, an uniconnected associated cycle set $X$ has odd size and $G(X)$ is a $Z$-group. Conversely, every uniconnected cycle set having odd size and with a $Z$-group permutation group can be constructed in this way.

**Proof.** The first part is a consequence of Proposition 2.4. Conversely, let $X$ be an uniconnected cycle set of odd size and with a $Z$-group permutation group. Let $A$ be the left brace, as in Proposition 2.3, such that $X$ is an indecomposable associated cycle set of $A$. Then, by Proposition 2.3, $A$ has a $Z$-group multiplicative group, it has odd size and by [13, Corollary 2], $A$ is a cyclic left brace, hence it can be constructed as in Proposition 1.2.

The previous corollary states that, if we know all the cyclic left braces with $Z$-group multiplicative group, we can construct all the uniconnected cycle set having odd size and with a $Z$-group permutation group. Hence, we have to cut all the isomorphic cycle sets obtained by the same cyclic left braces. In this direction we exhibit three preliminary results.

**Lemma 5.5.** Let $a_1$ be an element of $A$ and $(a_2, a_3)$ an element of $B = (B_{m+1} \times \cdots \times B_r) \times_\alpha (B_1 \times \cdots \times B_m)$, where $a_2 \in B_{m+1} \times \cdots \times B_r$ and $a_3 \in B_1 \times \cdots \times B_m$. Then, $\lambda_{(a_1, a_2, a_3)}(b_1, b_2, b_3)$ is equal to $(\lambda_{a_1}(b_1), \alpha(a_2)(b_2), \lambda_{a_3}(b_3))$.

**Proof.** It follows by a standard calculation, using the fact that $B_{m+1} \times \cdots \times B_r$ is a trivial left brace.

**Lemma 5.6.** A permutation $\psi$ of $\text{Sym}(A \times B)$ is an automorphism of the left brace $A \times B$ if and only if it is of the form $(\psi_1, \psi_2, \psi_3)$, where $\psi_1$ acts on the $j$th-component of an elements belonging to $A_1 \times \cdots \times A_v$ as the ring multiplication by an invertible element of the form $1 + s_j$ with $s_j \in \text{Soc}(A_j)$, for every $j \in \{1, \ldots, v\}$, $\psi_2 \in \text{Aut}(B_{m+1} \times \cdots \times B_r)$, hence acts on the $j$th-component of an elements belonging to $B_{m+1} \times \cdots \times B_r$ as the ring multiplication by an invertible element of $B_{j+m}$, for every $j \in \{1, \ldots, r - m\}$, and $\psi_3$ acts on the $j$th-component of an elements belonging to $B_1 \times \cdots \times B_m$ as the ring multiplication by an invertible element of the form $1 + s_j$ with $s_j \in I_j$, for every $j \in \{1, \ldots, m\}$.

**Proof.** It follows by Propositions 1 and 14 of [10].
Recall that an element of the left brace $A = \bar{A} \times \bar{B}$ can be uniquely written as a triple $(a, b, c)$ where $a \in \bar{A}$, $b \in B_{m+1} \times \ldots \times B_r$ and $c \in B_1 \times \ldots \times B_m$. Moreover, $a$ can be written as $(a_1, \ldots, a_v) \in A_1 \times \ldots \times A_v$, $b$ can be written as $(b_{m+1}, \ldots, b_r) \in B_{m+1} \times \ldots \times B_r$ and $c$ can be written as $(c_1, \ldots, c_m) \in B_1 \times \ldots \times B_m$. Using this notation, we give a further lemma.

**Lemma 5.7.** Let $(a, b, c), (a', b', c')$ be elements of $\bar{A} \times \bar{B}$ belonging to some transitive cycle bases and let $X_1$ (resp. $X_2$) be the uniconnected cycle set associated to $(a, b, c)$ (resp. $(a', b', c')$). Then $X_1$ and $X_2$ are isomorphic if and only if the following conditions hold:

1) $a_j' = (1 + s_j)(1 + q^{d_j}a_j'j') \mod q$ for all $j \in \{1, \ldots, v\}$ and $a_j' \in A_j$, for all $j \in \{1, \ldots, v\}$

2) $c_j' = (1 + s_j)(1 + p^{d_j}a_j')j' \mod q$ for some $s_j \in I_j$ and $a_j' \in B_j$, for all $j \in \{1, \ldots, m\}$

**Proof.** At first, note that by Lemma 3.2, $X_1$ and $X_2$ are isomorphic if and only if there exist $\psi \in Aut(A)$ and $\alpha \in A$ such that $\psi \lambda c(a, b, c) = (a', b', c')$. Now, since by Proposition 5, $\lambda c(a, b, c)$ is a trivial left brace, $b$ and $b'$ are in the same orbit respect to $Aut(A)$. Hence, by the Lemmas 5.3 and 5.4, $X_1$ and $X_2$ are isomorphic if and only if conditions 1) and 2) of the statement hold.

Using the previous lemma we can classify all the uniconnected cycle sets with odd size, a $\mathbb{Z}$-group permutation group and having a fixed associated left brace.

**Theorem 5.8.** Let $(a, b, c), (a', b', c')$ be elements of $\bar{A} \times \bar{B}$ belonging to some transitive cycle bases and let $X_1$ (resp. $X_2$) be the uniconnected cycle set associated to $(a, b, c)$ (resp. $(a', b', c')$). Then $X_1$ and $X_2$ are isomorphic if and only if the following conditions hold:

1) $a_j' \equiv a_j \mod q^{z_1}$ where $z_1 = \min\{\gamma_j - d_j, d_j\}$, for all $j \in \{1, \ldots, v\}$ and $a_j$ and $a_j'$ are any if $d_j = \gamma_j$;

2) $c_j' \equiv c_j \mod q^{z_2}$ where $z_2 = \min\{\beta_j - f_j, f_j\}$, for all $j \in \{1, \ldots, m\}$

**Proof.** If 1) and 2) hold, then $a_j' = a_j + r_jq^{z_1} = a_j(1 + q^{-\gamma_j}r_j)$ for some $r_j \in A_j$ and $c_j' = c_j + p^{z_2}s_j = c_j(1 + (c_j^{-1}p^{z_2}s_j)$ for some $s_j \in B_j$ and this fact implies 1) and 2) of the previous proposition, hence $X_1$ and $X_2$ are isomorphic. Conversely, if $X_1$ and $X_2$ are isomorphic by the previous proposition we have that $a_j' = a_j + q^{d_j}a_j'j' + s_ja_j + s_jq^{d_j}a_j'j$ for some $s_j \in Soc(A_j)$ and $a_j' \in A_j$, for all $j \in \{1, \ldots, v\}$ and $c_j' = c_j + p^{d_j}a_j'j + s_jc_j + s_jp^{d_j}a_j'j$ for some $s_j \in I_j$ and $a_j' \in B_j$, for all $j \in \{1, \ldots, m\}$. Using the last equalities conditions 1) and 2) follow, hence the thesis.

**Example 5.** Suppose that $\bar{A} = \{0\}$, $r = 2$, $m = 1$, $\bar{B} = p_1^{\alpha_1}p_2^{\alpha_2}$ with $p_1 < p_2$ and $\alpha$ isjective. Then, the left brace $B$ is the semidirect product $B_2 \times_\alpha B_1$ of two left braces $B_1$ having size $p_1^{\alpha_1}$ and $B_2$ having size $p_2^{\alpha_2}$. Let $(b_2, b_1), (b'_2, b'_1)$ be elements of $B_2 \times_\alpha B_1$ belonging to some transitive cycle bases and let $X_1$ (resp. $X_2$) be the uniconnected cycle set associated to $(b_2, b_1)$ (resp. $(b'_2, b'_1)$). By Lemma 5.6, we have that $Aut(B_2 \times_\alpha B_1, +, \circ)$
is equal to the set \( \{ (\psi_2, id_{B_1}) \mid \psi_2 \in Aut(B_2, +) \} \), therefore by Lemma 5.7, \( X_1 \) and \( X_2 \) are isomorphic if and only if \( b_1 \) and \( b'_1 \) are in the same orbit with respect to the lambda-maps of \( (B_1, +, \circ) \).

Theorem 5.8 is also useful to count the non-isomorphic uniconnected cycle sets with odd size and a \( Z \)-group permutation group having a fixed left brace \( \bar{A} \times \bar{B} \) as associated left brace.

**Proposition 5.9.** The number of non-isomorphic uniconnected cycle sets with odd size and a \( Z \)-group permutation group having a fixed left brace \( \bar{A} \times \bar{B} \) as associated left brace is exactly \( (\prod_{i=1}^{m} k_i) \cdot (\prod_{j=1}^{n} l_j) \) where \( k_i = \max\{q_i^{\min(\gamma_i-d_i,d_i)}-1(q_i-1), 1\} \) for all \( i \in \{1, ..., v\} \) and \( l_j = p_j^{\min(\beta_j-f_j,f_j)}-1(p_j-1) \) for all \( j \in \{1, ..., m\} \).

**Proof.** By Theorem 5.8, to show the thesis we have to count the number of the groups of \((A_i, +)\) module \( q_i^{\min(\gamma_i-d_i,d_i)} \) for every \( i \in \{1, ..., v\} \) and the number of the generators of \((B_i, +)\) module \( p_j^{\min(\beta_j-f_j,f_j)} \) for every \( j \in \{1, ..., m\} \). The first number is equal to \( \max\{q_i^{\min(\gamma_i-d_i,d_i)}-1(q_i-1), 1\} \) for every \( i \in \{1, ..., v\} \); the second one is \( p_j^{\min(\beta_j-f_j,f_j)}-1(p_j-1) \) for all \( j \in \{1, ..., m\} \), hence the thesis follows. \(\square\)

In this section we showed that all the uniconnected cycle set with odd size and having a \( Z \)-group permutation group can be easily constructed and classified as follows. We skip the proof, since it is a direct consequence of the previous results.

**Theorem 5.10.** Let \( H = C_1 \times_o C_2 \) be a \( Z \)-group having odd size (by [11, Theorem 9.4.3]), \( H \) must be isomorphic to the semidirect product of cyclic groups \( C_1 \) and \( C_2 \). Then, an uniconnected cycle set with permutation group isomorphic to \( H \) can be constructed as follows:

- Given \( \{B_m+1, ..., B_v\} \) the Sylow subgroups of \( C_1 \) and \( \{B_1, ..., B_m\} \) the ones of \( C_2 \), consider the Sylow Basis \( \{B_1, ..., B_v\} \) of \( H \);
- Construct all the cyclic left braces on the \( B_i \) using [18, Theorem 1];
- Construct \( \bar{A} \) and \( \bar{B} \) as in Propositions 4.2 and 4.2;
- Give the left brace \( A := \bar{A} \times \bar{B} \), compute its multipermutation level using Theorem 5.3;
- Given the left brace \( A := \bar{A} \times \bar{B} \), use Eq. 11 of Proposition 2.4 (where \( g \) is simply a generator of the additive group of \( A \) - see Lemma 3.4) to construct all the uniconnected cycle sets \( X \) having \( A \) as associated left brace. By Theorem 3.5, \( X \) has multipermutation level equal to \( mpl(A) \). Finally, cut the isomorphism classes using Theorem 5.8.

We remark that this machinery works because we only have to consider cyclic left braces. Since there exist left braces with a \( Z \)-group as multiplicative group, even size and non-cyclic additive group, we can not remove the "odd size" restriction.

Now, we close the section showing that the cycle sets considered in this section can uniquely be determined by 5 parameters.
Lemma 5.11. A complete set of invariants for a finite Z-group \( G \) is a triple of natural numbers \((m_1, n_1, r_1)\) such that \( \gcd((r_1 - 1)n_1, m_1) = 1 \), \( r_1 \in \{0, ..., m_1 - 1\} \) and \( r_1^{n_1} \equiv 1 \pmod{m_1} \). In this way, \( G \) can be identified with the semidirect product \((\mathbb{Z}/m_1\mathbb{Z}, +) \rtimes_{\alpha_{r_1}} (\mathbb{Z}/n_1\mathbb{Z}, +)\) where \( \alpha \) is given by \( \alpha_{r_1}(1) := r_1 \).

Proof. It follows by [11, Chapter 9].

Lemma 5.12. A complete set of invariants for a cyclic left brace \( A \) having odd size and with a Z-group multiplicative group is a quadruple of natural numbers \((m_1, n_1, r_1, t)\) such that \( \gcd((r_1 - 1)n_1, m_1) = 1 \), \( r_1 \in \{0, ..., m_1 - 1\} \) and \( r_1^{n_1} \equiv 1 \pmod{m_1} \) and \( t \) is such that every prime which divides \( m_1n_1 \) divides \( t \).

Proof. It follows by Lemma 5.11, [18, Theorem 1] and [19, Sections 4-5].

Theorem 5.13. A complete set of invariants for a finite uniconnected cycle set \( X \) having odd size and with a Z-group permutation group is the following:

1) a quadruple of natural numbers \((m_1, n_1, r_1, t)\) as in Lemma 5.12 which determines the structure of the cyclic left brace \( A = \bar{A} \times \bar{B} \) associated to \( X \);

2) a generator of the additive group \((\bar{A}, +) \times (B_1, +) \times ... \times (B_m, +), \) where \( m \) is the natural number as in Convention 4.

Proof. It follows by Lemma 5.12 and Theorem 5.8.

Note that if a finite uniconnected cycle set \( X \) has odd size and cyclic permutation group, by the previous theorem we obtain that it is uniquely determined by the quadruple \((1, |X|, 1, t)\) and a generator of the additive group \((\bar{A}, +), \) hence the set of invariants in this case has 3 elements. This is consistent with [13, Theorem 3.15].

6. The square-free case

In this section, we apply the results obtained before to the uniconnected cycle sets of square-free odd order. To exhibit the result in a comfortable way, in the following we use the same notation of the previous section.

At first, we show that the uniconnected cycle sets of square-free odd order belong to the family of the ones having a Z-group permutation group and that they are all of multipermutation level at most 2.

Proposition 6.1. Let \( X \) be an uniconnected cycle set of square-free odd order. Then, \( \mathcal{G}(X) \) is a Z-group and \( X \) has multipermutation level at most 2. Moreover, it has multipermutation level 1 if and only if the permutation group \( \mathcal{G}(X) \) is abelian.

Proof. By Proposition 2.4 there exist a left brace \( A \) such that \( X \) is isomorphic to an uniconnected associated cycle set \((A, \cdot)\). Since \((A, \circ)\) (which is equal to \( \mathcal{G}(X) \)) has square-free order, by [11, Chapter 9] it is a Z-group and by [19, Corollary 2] \( A \) is a cyclic left brace. By [11, Chapter 9] and [19, Sections 3-4], \( A \) must be isomorphic to a semidirect product of two trivial cyclic left braces \( C_1 \rtimes C_2 \). By Theorem 5.3 \( A \) has multipermutation level at most 2 and by Theorem 5.5 the first part of the thesis follows.

Now, if \( X \) has multipermutation level 1 then \( \mathcal{G}(X) \) is cyclic and hence abelian. Conversely,
if $G(X)$ is abelian it follows that $(A,\circ)$ is abelian and hence $A$ is a trivial cyclic left brace of multipermutation level 1, therefore by Theorem 5.8 $X$ also has multipermutation level 1.

**Corollary 6.2.** Let $A := \bar{A} \times \bar{B}$ be a cyclic left brace of square-free odd order. Moreover, let $g := (g_1, g_2, g_3) \in \bar{A} \times \bar{B}$ be an element of a transitive cycle base of $A$, where $g_1 \in A$, $g_2 \in B_{m+1} \times \ldots \times B_n$ and $g_3 \in B_1 \times \ldots \times B_m$. Then, the binary operation $\bullet_g$ on $A$ given by

$$(a_1, a_2, a_3) \bullet_g (b_1, b_2, b_3) := \lambda_{(a_1, a_2, a_3)}(g_1, g_2, g_3)^{-1} \circ (b_1, b_2, b_3)$$

for all $(a_1, a_2, a_3), (b_1, b_2, b_3) \in A$ makes $A$ into an uniconnected cycle set having multipermutation level 2. Moreover, if $h := (h_1, h_2, h_3)$ is another element of a transitive cycle base of $A$ and $\bullet_h$ the binary operation on $A$ defined as $\bullet_g$, we have that $(A, \bullet_g)$ is isomorphic to $(A, \bullet_h)$ if and only if $h_3 = g_3$.

**Proof.** Since in this case $d_j = \gamma_j$ for all $j \in \{1, \ldots, v\}$, $f_j = \beta_j$ and $f'_j = 0$ for all $j \in \{1, \ldots, m\}$, the result follows by Theorem 5.8.

It is well-known that all the group having square-free order are $Z$-group. Moreover, by a result due by Rump, given a group $H$ of square-free order, there exist a unique left brace $A$ such that $(A, \circ) \cong H$ (see [17, Corollary 2]) and it always is a semidirect product of trivial left braces. Therefore, the previous theorem allow to give a precise classification of all the uniconnected cycle sets of square-free odd order.

**Corollary 6.3.** Let $X$ be an uniconnected cycle set of square-free odd order with multipermutation level 2 and let $A$ be a cyclic left brace such that $X$ is an uniconnected associated cycle set. Moreover, with the same notation of the previous corollary, let $g := (g_1, g_2, g_3)$ be an element of $A$ such that $X \cong (A, \bullet_g)$. Let $Y$ be another uniconnected cycle set such that $G(Y) \cong G(X)$. Then, there exist an element $h := (h_1, h_2, h_3) \in A$ such that $Y \cong (A, \bullet_h)$ and $X \cong Y$ if and only if $h_3 = g_3$.

**Proof.** Since $G(Y) \cong G(X)$, by [18, Corollary 2] it follows that $A$ is the cyclic left brace associated to $Y$ hence by Proposition 2.1 there exist an element $h := (h_1, h_2, h_3) \in A$ such that $Y \cong (A, \bullet_h)$. The rest of the proof follows by Corollary 6.2.

**Corollary 6.4.** Let $X$ be an uniconnected cycle set having square-free order and with permutation group $H$. Then, $X$ has multipermutation level 1 or it has multipermutation level 2 and it is an uniconnected associated cycle set constructed as in Corollary 6.2 starting from the unique left brace $A$ having multiplicative group isomorphic to $H$.

**Proof.** Straightforward.

By Proposition 6.1 for every square-free number $n$ there is only one uniconnected cycle set having order $n$ and with abelian permutation group: it is the one having multipermutation level 1. Now, we give an explicit formula to count the non-isomorphic uniconnected cycle sets of square-free odd order with non-abelian permutation group.

**Corollary 6.5.** Let $H$ be a non-abelian group having square-free odd order and let $(A, +, \circ)$ be the cyclic left brace such that $(A, \circ) \cong H$. Then, the number of non-isomorphic uniconnected cycle sets of square-free order having permutation group isomorphic to $H$ is $\phi(|B_1 \times \ldots \times B_m|)$, where $\phi$ is the Euler function.
Proof. By Lemma 3.2 and Corollary 6.3 it is sufficient to count the possible values $g_3$ of a generator $(g_1, g_2, g_3)$ of the additive group $(A, +)$, and these clearly are $\phi(|B_1 \times \ldots \times B_m|)$. \qed

References

[1] D. Bachiller, Classification of braces of order $p^3$, Journal of Pure and Applied Algebra 219 (8) (2015) 3568–3603. URL https://doi.org/10.1015/forum-2015-0240
[2] D. Bachiller, F. Cedó, E. Jespers, Solutions of the Yang–Baxter equation associated with a left brace, J. Algebra 463 (2016) 80–102.
[3] M. Castelli, F. Catino, G. Pinto, Indecomposable involutive set-theoretic solutions of the Yang-Baxter equation, J. Pure Appl. Algebra 220 (10) (2019) 4477–4493. URL https://doi.org/10.1016/j.jpaa.2019.01.017
[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 (5) (2020) 1941–1955. URL https://doi.org/10.1080/00927872.2019.1710163
[5] F. Cedó, E. Jespers, J. Okniński, Braces and the Yang-Baxter equation, Comm. Math. Phys. 327 (1) (2014) 101–116. URL https://doi.org/10.1007/s00220-014-1935-y
[6] F. Cedó, E. Jespers, J. Okniński, Primitive set-theoretic solutions of the Yang-Baxter equation, arXiv preprint arXiv:2003.01983. URL https://arxiv.org/pdf/2003.01983.pdf
[7] V. G. Drinfel’d, On some unsolved problems in quantum group theory, in: Quantum groups (Leningrad, 1990), vol. 1510 of Lecture Notes in Math., Springer, Berlin, 1992, pp. 1–8. URL https://doi.org/10.1007/BFb0101175
[8] P. Etingof, T. Schedler, A. Soloviev, Set-theoretical solutions to the Quantum Yang-Baxter equation, Duke Math. J. 100 (2) (1999) 169–209. URL http://doi.org/10.1215/S0012-7094-99-10007-x
[9] T. Gateva-Ivanova, S. Majid, Matched pairs approach to set theoretic solutions of the Yang–Baxter equation, J. Algebra 319 (4) (2008) 1462–1529. URL https://doi.org/10.1016/j.jalgebra.2007.10.035
[10] T. Gateva-Ivanova, M. Van den Bergh, Semigroups of I-Type, J. Algebra 206 (1) (1998) 97–112. URL https://doi.org/10.1006/jabr.1997.7399
[11] M. Hall, The theory of groups, Courier Dover Publications, 2018.
[12] P. Jedlička, A. Pilitowska, A. Zamojska-Dzienio, Indecomposable involutive solutions of the Yang-Baxter equation of multipermutational level 2 with abelian permutation group, Forum Math. 2020. URL https://doi.org/10.1515/forum-2021-0130
[13] P. Jedlička, A. Pilitowska, A. Zamojska-Dzienio, Cyclic braces and indecomposable cocyclic solutions of the Yang-Baxter equation, arXiv preprint arXiv:2107.12319. URL https://arxiv.org/pdf/2107.12319.pdf
[14] S. Ramírez, L. Vendramin, Decomposition theorems for involutive solutions to the Yang-Baxter equation, Int. Math. Res. Not. IMRN. URL https://doi.org/10.1093/imrn/rnb232
[15] D. J. Robinson, A Course in the Theory of Groups, vol. 80, Springer Science & Business Media, 2012. URL http://doi.org/10.1007/978-1-4419-8594-1
[16] W. Rump, A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation, Adv. Math. 193 (2005) 40–55. URL https://doi.org/10.1016/j.aim.2004.03.019
[17] W. Rump, Braces, radical rings, and the quantum Yang-Baxter equation, J. Algebra 307 (1) (2007) 153–170. URL https://doi.org/10.1016/j.jalgebra.2006.03.040
[18] W. Rump, Classification of cyclic braces, Journal Pure Appl. Algebra 209 (3) (2007) 671–685. URL https://doi.org/10.1016/j.jpaa.2006.07.001
[19] W. Rump, Classification of cyclic braces. II, Trans. Amer. Math. 372 (1) (2019) 305–328. URL https://doi.org/10.1090/tran/7956
[20] W. Rump, Classification of indecomposable involutive set-theoretic solutions to the Yang-Baxter equation, Forum Math. 32 (4) (2020) 891–903. URL https://doi.org/10.1515/forum-2019-0274

[21] W. Rump, Cocyclic solutions to the Yang-Baxter equation, Proc. Amer. Math. Soc. 149 (2) (2021) 471–479. URL https://doi.org/10.1090/proc/15220

[22] 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. URL https://doi.org/10.1016/j.laa.2018.02.001