Indecomposable solutions of the Yang-Baxter equation with permutation group of sizes $pq$ and $p^2q$

S. Ramírez

IMAS–CONICET and Depto. de Matemática, FCEN, Universidad de Buenos Aires, Buenos Aires, Argentina

ABSTRACT
In this paper we study the problem of the classification of indecomposable solutions of the Yang-Baxter equation. Using a scheme proposed by Bachiller, Cedó, and Jespers, and recent advances in the classification of braces we classify all indecomposable solutions with some particular permutation groups. We do this for all groups of size $pq$, all abelian groups of size $p^2q$ and all dihedral groups of size $p^2q$.

1. Introduction
The study of solutions of the Yang-Baxter equation originates from the works in physics of Yang [26] and Baxter [6]. In 1990 Drinfeld [16] proposed the study of the class of set-theoretical solutions of Yang-Baxter equation (see Definition 2.1).

The foundational works on the algebraic study of these solutions came later in Etingof, Schedler and Soloviev [17] and Gateva-Ivanova and Van den Bergh [19]. In the years following, a great number of connections to other areas of algebra have been found, e.g. Hopf-Galois structures [25], radical rings [22] and Garside groups [13, 14].

One of the main problems is that of the classification and construction of solutions. Although there have been recent improvements in the explicit construction of all solutions of small sizes [3], this approach does not look feasible in general. There are for example almost five million involutive (see Definition 2.2) solutions of size 10, the largest size computed. There seems to be a computational limit for direct calculations.

One might try considering a class of simpler solutions from which one could construct all the rest, and try to classify these simpler ones. One such approach is to consider solutions that cannot be written as a disjoint union of two other solutions. These are called indecomposable solutions and were defined originally in [17]. Classifying indecomposable solutions seems to be a more approachable objective, for comparison there are only 36 indecomposable solutions of size 10. This class of solutions has been intensively studied with many recent results [7–11, 18, 20, 21, 23, 24]. In this paper we give a classification of all indecomposable solutions whose permutation group (see Definition 2.2) has size $pq$, or is abelian or dihedral and of size $p^2q$, where $p$ and $q$ are distinct primes.

2. Preliminaries
In this section we collect the basic definitions and results we will need about solutions and braces, and go over the scheme proposed by Bachiller, Cedó and Jespers [5] that we will use for the classification.
2.1. Solutions and braces

We will restrict ourselves to non-degenerate solutions to the Yang-Baxter equation,

Definition 2.1. A non-degenerate set-theoretic solution to the Yang-Baxter equation is a pair \((X, r)\), with \(X\) a non-empty set and \(r : X \times X \to X \times X\) a bijection that satisfies

\[
(r \times 1)(1 \times r)(r \times 1) = (1 \times r)(r \times 1)(1 \times r),
\]

and such that all the maps \(\sigma_x, \tau_y\) defined by \(r(x, y) = (\sigma_x(y), \tau_y(x))\) are bijective.

Besides this we will also restrict ourselves to involutive solutions.

Definition 2.2. A solution to the set-theoretical Yang-Baxter equation \((X, r)\) is said to be involutive if \(r^2 = \text{id}\).

In this case the group generated by the maps \(\sigma_x\) is called the permutation group of the solution.

In what follows solution will always mean non-degenerate involutive solution of the Yang-Baxter equation. These restrictions guarantee that the permutation group will be well-behaved and nicely reflect properties of the solution. With these restrictions the indecomposables solutions described in the introduction can be alternatively defined in the following way:

Definition 2.3. A solution \((X, r)\) is said to be indecomposable if its permutation group acts transitively on \(X\).

The permutation group of a (involutive) solution has the additional structure of a brace.

Definition 2.4. A brace is a triple \((B, +, \circ)\), where \((B, +)\) is an abelian group, the additive structure of the brace, and \((B, \circ)\) is a group, the multiplicative structure, satisfying

\[
a \circ (b + c) = a \circ b - a + a \circ c.
\]

A brace is said to be trivial if the additive and multiplicative structures are the same.

This structure was originally described in [22], with this definition first appearing in [12], and is a fundamental tool in the classification process. The brace structure on the permutation group of a solution has the composition of permutations as its multiplicative structure. We will not find it necessary to know how to describe the additive structure.

In a brace, \((B, +, \circ)\), the multiplicative group has a natural action (by group automorphisms) on the additive group. This action is usually noted by \(\lambda_\_ : (B, \circ) \to \text{Aut}(B, +)\), and is given by

\[
\lambda_a(b) = -a + a \circ b.
\]

2.2. Classification scheme

We now go over the scheme developed by Bachiller, Cedó and Jespers in [5] for classifying all solutions that have a given brace as permutation group. A related scheme in terms of coverings of solutions was developed by Rump in [23].

Let \(B\) be a brace, to give a solution with brace \(B\) one must first choose a set of elements of \(B\) such that their orbits under the \(\lambda\) action additively generate \(B\). Then for each of these elements one must choose a subgroup of its stabilizer, in such a way that the intersection of all of their normal cores is trivial. The underlying set of the solution is given by the disjoint union of the quotients of \(B\) by the chosen subgroups, while the structure of a solution is obtained from the action of \(B\) on these sets (for the details see [5]). By [5, Theorem 3.1] all solutions can be constructed in this way.
On the other hand in [5, Theorem 4.1] they characterize when two of these solutions are isomorphic. For this to happen there must be a brace automorphism that maps the orbits of the elements chosen for the first one to the orbits of the elements chosen for the second one. Moreover, the image of a chosen subgroup by the automorphism must be conjugate to the corresponding subgroup.

Since we are going to focus on indecomposable solutions this scheme simplifies considerably. Moreover, since indecomposable solutions are precisely those in which the permutation group acts transitively, in the construction we must choose a single element. So rather than consider all possible ways in which a union of orbits may generate the group, we only need to understand which orbits generate the group. The following observation will be particularly useful for this:

**Remark 2.5.** Since the multiplicative group acts by automorphisms of the additive group, all the elements of an orbit must have the same additive order. In particular, if the orbit generates the additive group, which is abelian, this order must be divisible by all the primes dividing the size of the group.

A second important consequence of choosing a single element is that the intersection we need to consider contains a single subgroup. We are then restricted to choosing core-free subgroups of the stabilizer of an element. This further simplifies when considering abelian groups, as in this case the only core-free subgroup is the trivial one. Moreover, it turns out that even in the case of the dihedral groups this is the only subgroup we need to consider.

We can then restate the results of [5] for this simplified situation as follows:

**Theorem 2.6 (Bachiller-Cedó-Jespers).** Let \( B \) be a brace, \( x \in B \) such that the set \( \{ \lambda_b(x) : b \in B \} \) generate the additive group of brace, and \( K < B \) a core-free subgroup of the multiplicative group such that \( \lambda_k(x) = x, \forall k \in K \). Then there is a natural solution structure on \( B/K \). This solution is indecomposable and its permutation group is isomorphic to \( B \) as a brace. Moreover any indecomposable solution with \( B \) as its permutation brace has this form.

In order to classify all solutions with a given permutation group, we must then understand all possible braces with that multiplicative structure. For this we refer to recent work classifying braces, and more general skew-braces, of fixed sizes [1, 2, 4, 15]. We refer mainly to the results of Acri and Bonatto in [1, 2], where they give explicit formulas for braces of order \( pq \) and \( p^2q \).

The process of classification is then the following. Using the explicit description of the braces with fixed multiplicative group we first characterize all generating orbits of the \( \lambda \) action. In the case of abelian groups this gives us all solutions, for the dihedral groups we also need to find the core-free subgroups of the stabilizers to find all solutions. Next we need to find how the brace automorphisms act on the orbits. For this we again use the explicit description to compute the group of automorphisms explicitly. With the explicit description of the orbits and automorphisms we can then see which orbits generate isomorphic solutions.

### 3. Braces of size \( pq \)

We first focus on solutions with permutation group of size \( pq \). For the descriptions of the braces we refer to [1], where all (skew) braces of size \( pq \) are classified. According to the classification there are at most two braces of these sizes. There is always a trivial brace with cyclic multiplicative group. When \( p \equiv 1 \pmod{q} \) there is an additional brace whose multiplicative group is a semidirect product.

First, we classify all indecomposable solutions with a trivial brace as permutation brace,

**Proposition 3.1.** Let \( B \) be a trivial brace. If the underlying group of \( B \) is cyclic then there is a unique indecomposable solution with permutation brace \( B \). If the underlying group is not cyclic then there is no indecomposable solution.
Proof. By [5] we first need to find all orbits under the $\lambda$ action that generate the additive group. Since the brace is trivial all orbits are singletons, and the problem reduces to finding generators. In particular only cyclic groups will produce indecomposable solutions. We can then assume the group is cyclic.

Since the group is cyclic the only possible core-free subgroup is the trivial group, so every generator of the group produces a single solution. However, since the group is cyclic there is a group automorphism mapping every generator to any other one. Moreover, since the brace is trivial any morphism of the additive group is a brace morphism. Finally, this gives an isomorphism between any pair of solutions we obtain since the subgroup used to construct such solutions is trivial.

Now, assume $p \equiv 1 \pmod{q}$ and consider the non-trivial brace of size $pq$. Following [1], we identify the additive structure of the brace $B$ with the group $\mathbb{Z}_p \times \mathbb{Z}_q$. The multiplicative structure is then given by

$$
\left(\begin{array}{c} a \\ b \\
\end{array}\right) \circ \left(\begin{array}{c} c \\ d \\
\end{array}\right) = \left(\begin{array}{c} a + g^b c \\ b + d \end{array}\right)
$$

where $g$ is any element of $\mathbb{Z}_p$ of order $q$.

By Remark 2.5, any generating orbit must contain a generator, i.e. an element of the form $(a, b)$ with both $a$ and $b$ generators of the corresponding group. The stabilizer of any such orbit is then $\mathbb{Z}_p \times \{0\}$, giving $\frac{(p-1)(q-1)}{q}$ distinct orbits. We note that this subgroup has no non-trivial core-free subgroups.

To understand when two of these orbits generate the same solution we need to compute the automorphisms group of the brace.

**Proposition 3.2.** Let $p$ and $q$ be primes with $p \equiv 1 \pmod{q}$. Then the group of automorphisms of the non-trivial brace of size $pq$ is isomorphic to $\mathbb{Z}_p^\times \rtimes \mathbb{Z}_q^\times$.

**Proof.** The automorphisms of the additive group are given by $\mathbb{Z}_p^\times \rtimes \mathbb{Z}_q^\times$, acting by coordinatewise multiplication. An element $(\alpha, \beta)$ in this group is a brace automorphism if it satisfies

$$
\left(\begin{array}{c} \alpha(a + g^b c) \\ \beta(b + d) \end{array}\right) = \left(\begin{array}{c} \alpha(a + g^{\beta b} c) \\ \beta(b + d) \end{array}\right), \quad \forall a, c \in \mathbb{Z}_p, b, d \in \mathbb{Z}_q.
$$

Hence, $(\alpha, \beta)$ is a brace morphism if and only if $\beta = 1$, and the result follows. 

From this it follows that two orbits will generate the same solution if and only if their second coordinates coincide. This means that there are exactly $q - 1$ indecomposable solutions with this brace as permutation brace.

We conclude this section with the following result classifying all Indecomposable solutions with permutation group of size $pq$.

**Theorem 3.3.** Let $G$ be a group of order $pq$. Then:

1. If $G$ is cyclic there is a unique indecomposable solution with permutation group $G$.

2. If $G$ is a semidirect product $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ then there are exactly $q - 1$ indecomposable solutions with permutation group $G$.

In any of these cases all solutions have size $pq$.

As a corollary of this result, we obtain that if $p$ is an odd prime number then there is a single indecomposable solution with permutation group the dihedral group $D_{2p}$.
4. Cyclic braces of size $p^2q$

Now we focus on braces of size $p^2q$, and start by considering those with cyclic multiplicative group. We refer to [2] for the enumeration and explicit descriptions of such braces.

4.1. Case $p = 2$

In [2] the analysis is split into the cases $q \equiv 1 \pmod{4}$ and $q \equiv 3 \pmod{4}$. However, the braces with abelian permutation group can be described uniformly for both cases so we make no such distinction here.

There are two possible braces with cyclic permutation group. The first is the trivial brace. By Theorem 3.1 there is a unique indecomposable solution for such a brace. The other case (see Proposition 7.4 in [2]) is the brace with additive structure given by the group $\mathbb{Z}_2^2 \times \mathbb{Z}_q$, and multiplicative structure given by

$$
\begin{pmatrix}
a \\
b \\
c
\end{pmatrix}
\circ
\begin{pmatrix}
da \\
e \\
f
\end{pmatrix}
= 
\begin{pmatrix}
a + d + be \\
b + e \\
c + f
\end{pmatrix}.
$$

(4.1)

By Remark 2.5 the elements of any generating orbit must have order $2q$. So we must consider the orbits of elements of the form $(\alpha, \beta, \gamma)$ with $\gamma$ a generator of $\mathbb{Z}_q$ and $\alpha$ and $\beta$ not both 0. Since acting via $\lambda$ on one of these elements can only change its first coordinate we must have $\beta = 1$. We then have exactly $q - 1$ generating orbits of the form $O_\gamma = \{(\ast, 1, \gamma)\}$, with $\gamma$ a generator of $\mathbb{Z}_q$.

The following result characterizes the group of brace automorphisms of these braces:

**Proposition 4.1.** Given $q$ a prime number, the group of brace automorphisms of the unique non-trivial brace with multiplicative group isomorphic to $\mathbb{Z}_{4q}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_q^\times$.

**Proof.** The group automorphisms of the additive group are isomorphic to $\text{GL}_2(2) \times \mathbb{Z}_q^\times$, with the first component acting by multiplication on the first two coordinates, and the second component on the third one. Let $(A, u)$ be an element of this group, with $A = \begin{pmatrix} x & y \\ z & 2 \end{pmatrix}$. We use (4.1) to check additive morphisms are also multiplicative morphisms. Focusing on the second coordinate we get

$$
w(a + d) + z(b + e) = w(a + d + be) + z(b + e),
$$

if this holds for any $a, b, d, e \in \mathbb{Z}_2$ then $w$ must be zero. This immediately implies $x = 1 = z$ since the matrix is invertible. The condition on the first coordinate is now automatically satisfied and from the third coordinate we do not get any further restriction, so for $(A, u)$ to be a brace automorphism $A$ must be unitriangular. Since the group of $2 \times 2$ unitriangular matrices is isomorphic to $\mathbb{Z}_2$ we get the desired result. 

Given two generating orbits $O_\gamma$ and $O_{\gamma'}$ we can take $A$ the identity matrix and $u = \gamma^{-1} \gamma'$ to get by the previous result a brace automorphism mapping the first orbit to the second one. In particular all the orbits generate the same solution, i.e. there is a unique indecomposable solution with a non-trivial brace in this case.

4.2. Case $p$ odd

In [2] the case of $p$ odd is described by several results depending on the relation between the primes $p$ and $q$, with different braces obtained in each case. However, the different cases differ only for braces with non-abelian multiplicative group. The braces with abelian multiplicative group can be described uniformly for all primes $p$ and $q$.

In this case we again have only two possible braces, the trivial one and the unique non-trivial one. However, in this case the non-trivial brace also has cyclic additive group. This is the brace with additive
group $\mathbb{Z}_{p^2} \times \mathbb{Z}_q$ and multiplicative structure given by

$$
\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a + c + pac \\ b + d \end{pmatrix}.
$$

(4.2)

By Remark 2.5 any generating orbit is the orbit of a generator of the additive group. Given $(\alpha, \beta)$ a generator of $\mathbb{Z}_{p^2} \times \mathbb{Z}_q$ its orbit under the $\lambda$ action consists of all elements of the form $(\hat{\alpha}, \beta)$ with $\hat{\alpha} \equiv \alpha \pmod{p}$.

Again, to see which orbits generate the same solution, we characterize the group of brace automorphisms of this brace.

**Proposition 4.2.** The group of brace automorphisms of the unique non-trivial brace of order $p^2 q$ with cyclic multiplicative group is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_q$.

**Proof.** The group of automorphisms of the additive group is $\mathbb{Z}_{p^2} \times \mathbb{Z}_q$, acting by coordinatewise multiplication. From (4.2) we can see that for an element $(\alpha, \beta)$ to also be a morphism of the multiplicative group it must satisfy $\alpha^2 \equiv \alpha \pmod{p^2}$. \hfill \Box

From this result we then conclude that two generators of the additive group $(\alpha, \beta)$ and $(\alpha', \beta')$ give the same solution if $\alpha \equiv \alpha' \pmod{p}$. In particular, there are $p - 1$ indecomposable solutions for this brace.

We can summarize what we just proved in the following theorem.

**Theorem 4.3.** Let $p$ and $q$ be distinct prime numbers. There are $p$ distinct indecomposable solutions with permutation group isomorphic to $\mathbb{Z}_{p^2 q}$.

## 5. Non-Cyclic abelian braces of size $p^2 q$

We now focus on the only non-cyclic abelian group of order $p^2 q$. First we note that by Proposition 3.1 the trivial brace will not give us a solution in this case.

### 5.1. Case $p = 2$

In this case, there is a unique non-trivial brace, and it has a cyclic additive group is cyclic. This brace is the one obtained by taking $(i, j) = (0, 1)$ in proposition 7.1 of [2], we note there is a typo in the statement of the theorem and when giving the multiplicative groups the cases $(0, 1)$ and $(1, 0)$ are swapped. This brace has additive group $\mathbb{Z}_q \times \mathbb{Z}_4$ and multiplicative structure given by

$$
\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a + c \\ b + (-1)^b d \end{pmatrix}.
$$

(5.1)

The generating orbits are then of the form $O_\alpha = \{(\alpha, 1), (\alpha, 3)\}$, with $\alpha$ a generator of $\mathbb{Z}_q$.

We can characterize the group of brace automorphisms with the following result:

**Proposition 5.1.** Given $q$ an odd prime, the unique non-trivial brace with multiplicative group $\mathbb{Z}_q \times \mathbb{Z}_2^2$ has group of automorphisms isomorphic to $\mathbb{Z}_{4q}$.

**Proof.** The group of automorphisms of the additive group is $\mathbb{Z}_{4q} \cong \mathbb{Z}_q \times \mathbb{Z}_4 \times \mathbb{Z}_q$, which acts by coordinatewise multiplication. By substituting in (5.1) we see that all of these are also multiplicative automorphisms. \hfill \Box
It follows from this result that all orbits generate the same solution. There is then a unique indecomposable solution with permutation group \( \mathbb{Z}_q \times \mathbb{Z}_2^2 \) for any odd prime \( q \).

### 5.2. Case \( p \) odd

As stated in Section 4.2 in [2] this case is described in several cases. However, the braces with an abelian multiplicative structure can be described uniformly for all primes \( p \) and \( q \). As in the previous case, there is a single non-trivial brace. However, in this case, the additive and multiplicative groups are both isomorphic to \( \mathbb{Z}_p^2 \times \mathbb{Z}_q \) (see Theorem 3.6 of [2]). For such a brace the multiplicative structure is given by

\[
\begin{pmatrix}
a \\
b \\
c
\end{pmatrix}
\circ
\begin{pmatrix}
d \\
e \\
f
\end{pmatrix} =
\begin{pmatrix}
(a + d + be) \\
b + e \\
c + f
\end{pmatrix}.
\]

Notice that this is the same formula that defines the non-trivial brace of Section 4.1. However when \( p \) is an odd prime the resulting multiplicative group is not cyclic. The orbit of an element \((\alpha, 0, \beta)\) only contains elements of the same form, and in particular cannot generate the additive group. The rest of the orbits are of the form \( O_{\alpha, \beta} = \{(*, \alpha, \beta)\} \), with \( \alpha \neq 0 \). Such an orbit generates the abelian group if and only if also \( \beta \) is non-zero. The following proposition characterizes the brace automorphisms:

**Proposition 5.2.** Given \( p \) an odd prime and \( q \) a prime number, the group of brace automorphisms of the unique non-trivial brace with multiplicative group isomorphic to \( \mathbb{Z}_p^2 \times \mathbb{Z}_q \) is isomorphic to \( G \times \mathbb{Z}_q \), with

\[
G = \left\{ \begin{pmatrix} z^2 & y \\ 0 & z \end{pmatrix} : z \in \mathbb{Z}_p^\times, y \in \mathbb{Z}_p \right\} \subset \text{GL}_2(p).
\]

**Proof.** We proceed as in Proposition 4.1. The group automorphisms of the additive group are isomorphic to \( \text{GL}_2(p) \times \mathbb{Z}_q^\times \), with the first component acting by multiplication on the first two coordinates, and the second component on the third one. Let \((A, u)\) be an element of this group, with \( A = \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix} \). We use (5.2) to check which additive morphism \((A, u)\) is also a multiplicative morphisms. Focusing on the second coordinate we get

\[
w(a + d) + z(b + e) = w(a + d + be) + z(b + e),
\]

and as before this implies that \( w \) must be zero. However, in this case, the condition on the first coordinate is not automatically satisfied. Using \( w = 0 \) we get

\[
x(a + d) + y(b + e) + z^2 be = x(a + d) + y(b + e) + xbe,
\]

that will hold for any \( a, b, d, e \in \mathbb{Z}_p \) if and only if \( x = z^2 \). The third coordinate will not give further restrictions, so \((A, u)\) is a brace automorphism if \( A \in G \) and \( u \in \mathbb{Z}_q^\times \).

Given two generating orbits \( O_{\alpha, \beta} \) and \( O_{\alpha', \beta'} \), we can take \( u = \beta^{-1} \beta' \) and \( A = \begin{pmatrix} (\alpha^{-1} \alpha')z^2 & 0 \\ 0 & \alpha^{-1} \alpha' \end{pmatrix} \) to get an automorphism that maps the first orbit to the second one. It follows that all the orbits generate the same solution.

With this and the previous case we have proved the following theorem:

**Theorem 5.3.** Given \( p \) and \( q \) prime numbers, there is a unique indecomposable solution with permutation group \( \mathbb{Z}_2^p \times \mathbb{Z}_q \).

### 6. Dihedral braces of size \( p^2 q \)

In this last section, we focus on solutions with a dihedral permutation group. We rely on the results in [2] to describe all solutions with permutation group isomorphic to \( D_{2p^2} \) or \( D_{4p} \) for \( p \) an odd prime. We
first note that in any dihedral group every rotation generates a normal subgroup, and any two distinct
reflections generate some rotation. In particular, in any dihedral group the only core-free subgroups are
those generated by a single reflection, and so we have the following result:

**Theorem 6.1.** If $X$ is an indecomposable solution with permutation group $D_{2n}$, then $|X| = 2n$ or $|X| = n$. 

### 6.1. Case $2p^2$

For this case, we will analyze the slightly more general situation of a semidirect product $\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_q$ when $p \equiv 1 \pmod{q}$. Taking $q = 2$ we get the desired dihedral group. These semidirect products are given by choosing $g$ an element of order $q$ in $\mathbb{Z}_{p^2}$, and letting a generator of $\mathbb{Z}_q$ act by multiplication by $g$.

There is a unique brace with this group as its multiplicative group, and, in this case, its additive group is isomorphic to the cyclic group. Its multiplicative structure is given by

$$
\left( \begin{array}{c}
a \\
b
\end{array} \right) \circ \left( \begin{array}{c}
c \\
d
\end{array} \right) = \left( \begin{array}{c}
a + g^b c \\
b + d
\end{array} \right).
$$

We note that this formula coincides with (3.1), and with the same arguments as in Section 3 we get the following result

**Proposition 6.2.** Let $p$ and $q$ be primes with $p \equiv 1 \pmod{q}$. Then the group of automorphisms of the non-trivial brace of size $p^2 q$ is isomorphic to $\mathbb{Z}_{p^2}$.

As before the generating orbits are the ones generated by elements $(\alpha, \beta)$ with $\alpha$ and $\beta$ generators, and two elements give the same solution precisely when they have the same second coordinate.

**Theorem 6.3.** Given $p$ and $q$ primes such that $p \equiv 1 \pmod{q}$, there are exactly $q - 1$ indecomposable solutions with permutation group $\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_q$, and all such solutions have size $p^2 q$.

In particular, we get the following as a consequence.

**Corollary 6.4.** Given $p$ an odd prime, there is a unique indecomposable solution with permutation group the dihedral group $D_{2p^2}$. This solution has size $2p^2$.

### 6.2. Case $4p$

In this case, we have several brace structures to study. There are two braces with a cyclic additive group and one with a non-cyclic additive group. The first cyclic one has multiplicative structure given by

$$
\left( \begin{array}{c}
a \\
b
\end{array} \right) \circ \left( \begin{array}{c}
c \\
d
\end{array} \right) = \left( \begin{array}{c}
a + (-1)^b c \\
b + (-1)^b d
\end{array} \right).
$$

The orbit of a generator $(\alpha, \beta)$ consists of itself and the element $(-\alpha, -\beta)$, and its stabilizer is $\{(*, 0), (*, 2)\}$, which is precisely the group of all rotations, and so has no non-trivial core-free subgroups. The following result gives the group of brace automorphisms.

**Proposition 6.5.** Given $p$ an odd prime, the group of brace automorphisms of the brace with cyclic additive group and multiplicative group given by (6.1) is isomorphic to $\mathbb{Z}_{4p}$.

**Proof.** An automorphism of the additive group is given by multiplication by a pair of elements $(x, y)$, and it is easy to verify that all of them are brace automorphisms.

In particular this means that all the orbits give rise to the same solution.
The second brace with cyclic additive group is given by the formula

\[
\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a + (-1)^{b(c-1)/2}c \\ b + (-1)^b d \end{pmatrix}.
\] (6.2)

In this case the orbit of a generator has four elements, and its stabilizer is given by the subgroup \{(*, 0)\}. This group consists entirely of rotations and so has no non-trivial core-free subgroups. We characterize the group of brace automorphisms with the following result:

**Proposition 6.6.** Given \( p \) an odd prime, the group of brace automorphisms of the brace with cyclic additive group and multiplicative group given by (6.2) is isomorphic to \( \mathbb{Z}_p^* \).

**Proof.** An automorphism of the additive group is given by multiplication by a pair of elements \((x, y)\). Testing with an additive automorphism on (6.2), shows that the pair \((x, y)\) is a brace automorphism if \( y = 1 \), which gives us the desired result. \(\square\)

With this we can see that all the orbits generate the same solution.

Finally, we analyze the non-cyclic brace. This brace has \( \mathbb{Z}_2^2 \times \mathbb{Z}_p \) as additive group and multiplicative structure given by

\[
\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} d \\ e \end{pmatrix} = \begin{pmatrix} a + d \\ b + e \\ c + (-1)^d f \end{pmatrix}.
\] (6.3)

The lambda action on an element does not modify the first two coordinates. Concretely this means the orbit of an element \((\alpha, \beta, \gamma)\) is \(\{(\alpha, \beta, \pm \gamma)\}\), and in particular it cannot generate the additive group. So this brace cannot be the permutation group of an indecomposable solution.

In conclusion we get the following result:

**Theorem 6.7.** Given \( p \) an odd prime, there are two indecomposable solutions with permutation group isomorphic to \( D_{4p} \). Moreover all of these solutions have size \( 4p \).

As we noted in **Proposition 6.1**, an indecomposable solution with permutation group \( D_{2n} \) can only have size \( n \) or \( 2n \). From the results obtained here we conjecture the first case never happens:

**Conjecture 6.8.** If \( X \) is an indecomposable solution with permutation group \( D_{2n} \) then \( |X| = 2n \).

Acknowledgments

The author would like to thank Leandro Vendramin for his comments on an earlier draft of this work as well as his general advice.

References

[1] Acri, E., Bonatto, M. (2020). Skew braces of size \( pq \). *Commun. Algebra* 48(5):1872–1881.
[2] Acri, E., Bonatto, M. (2022). Skew braces of size \( p^2q \): Abelian type. *Algebra Colloq.* 29(02):297–320.
[3] Akgün, Ö., Mereb, M., and Vendramin, L. (2022). Enumeration of set-theoretic solutions to the Yang–Baxter equation. *Math. Comput.* 91(335):1469–1481.
[4] Alabdali, A. A., Byott, N. P. (2021). Skew braces of squarefree order. *J. Algebra Appl.* 20(07):2150128.
[5] Bachiller, D., Cedó, F., Jespers, E. (2016). Solutions of the Yang–Baxter equation associated with a left brace. *J. Algebra* 463:80–102.
[6] Baxter, R. J. (1972). Partition function of the eight-vertex lattice model. *Ann. Phys.* 70(1):193–228.
[7] Camp-Mora, S., Sastriques, R. (2021). A criterion for decomposability in QYBE. *Int. Math. Res. Not.* 2023(5):3808–3813.
[8] Castelli, M., Catino, F., Pinto, G. (2019). Indecomposable involutive set-theoretic solutions of the Yang-Baxter equation. *J. Pure Appl. Algebra* 223(10):4477–4493.

[9] Castelli, M., Catino, F., Stefanelli, P. (2021). Indecomposable involutive set-theoretic solutions of the Yang-Baxter equation and orthogonal dynamical extensions of cycle sets. *Mediterr. J. Math.* 18(6):Paper No. 246, 27, 2021.

[10] Castelli, M., Mazzotta, M., Stefanelli, P. (2022). Simplicity of indecomposable set-theoretic solutions of the Yang-Baxter equation. *Forum Math.* 34(2):531–546.

[11] Castelli, M., Pinto, G., Rump, W. (2020). On the indecomposable involutive set-theoretic solutions of the Yang-Baxter equation of prime-power size. *Commun. Algebra* 48(5):1941–1955.

[12] Cedó, F., Jespers, E., Okniński, J. (2014). Braces and the Yang-Baxter equation. *Commun. Math. Phys.* 327(1): 101–116.

[13] Chouraqui, F. (2010). Garside groups and Yang–Baxter equation. *Commun. Algebra* 38(12):4441–4460.

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

[15] Dietzel, C. (2021). Braces of order $p^2q$. *J. Algebra Appl.* 20(08):2150140.

[16] Drinfel’d, V. G. (1992). On some unsolved problems in quantum group theory. In: Kulish, P. P., eds. Quantum Groups (Leningrad, 1990), volume 1510 of Lecture Notes in Mathematics, Berlin: Springer, pp. 1–8.

[17] Etingof, P., Schedler, T., and Soloviev, A. (1999). Set-theoretical solutions to the quantum Yang-Baxter equation. *Duke Math. J.* 100(2):169–209.

[18] Etingof, P., Soloviev, A., Guralnick, R. (2001). Indecomposable set-theoretical solutions to the quantum Yang-Baxter equation on a set with a prime number of elements. *J. Algebra* 242(2):709–719.

[19] Gateva-Ivanova, T., Van den Bergh, M. (1998). Semigroups of I-type. *J. Algebra* 206(1):97–112.

[20] Jedlička, P., Pilitowska, A., Zamojska-Dzienio, A. (2021). Indecomposable involutive solutions of the Yang-Baxter equation of multipermutational level 2 with abelian permutation group. *Forum Math.* 33(5):1083–1096.

[21] Ramirez, S., Vendramin, L. (2021). Decomposition theorems for involutive solutions to the Yang–Baxter equation. *Int. Math. Res. Not.* 2022(22):18078–18091.

[22] Rump, W. (2007). Braces, radical rings, and the quantum Yang–Baxter equation. *J. Algebra* 307(1):153–170.

[23] Rump, W. (2020). Classification of indecomposable involutive set-theoretic solutions to the Yang-Baxter equation. *Forum Math.* 32(4):891–903.

[24] Rump, W. (2020). One-generator braces and indecomposable set-theoretic solutions to the Yang-Baxter equation. *Proc. Edinb. Math. Soc.* (2) 63(3):676–696.

[25] Smoktunowicz, A., Vendramin, L. (2018). On skew braces (with an appendix by N. Byott and L. Vendramin). *J. Comb. Algebra* 2(1):47–86.

[26] Yang, C.-N. (1967). Some exact results for the many-body problem in one dimension with repulsive delta-function interaction. *Phys. Rev. Lett.* 19(23):1312.