

INDECOMPOSABLE INVOLUTIVE SOLUTIONS OF THE YANG-BAXTER EQUATION OF MULTIPERMUTATION LEVEL 2 WITH NON-ABELIAN PERMUTATION GROUP

PŘEMYSL JEDLIČKA AND AGATA PILITOWSKA

ABSTRACT. We give a complete characterization of all indecomposable involutive solutions of the Yang-Baxter equation of multipermutation level 2. In the first step we present a construction of some family of such solutions and in the second step we prove that every indecomposable involutive solution of the Yang-Baxter equation with multipermutation level 2 is a homomorphic image of a solution previously constructed. Analyzing this epimorphism, we are able to obtain all such solutions up to isomorphism and enumerate these of small sizes.

1. INTRODUCTION

The Yang-Baxter equation is a fundamental equation occurring in mathematical physics. It appears, for example, in integrable models in statistical mechanics, quantum field theory or Hopf algebras (see e.g. [20, 22]). Searching for its solutions has been absorbing researchers for many years.

Let us recall that, for a vector space V , a *solution of the Yang-Baxter equation* is a linear mapping $r : V \otimes V \rightarrow V \otimes V$ such that

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

Description of all possible solutions seems to be extremely difficult and therefore there were some simplifications introduced by Drinfeld in [9]. Let X be a basis of the space V and let $\sigma : X^2 \rightarrow X$ and $\tau : X^2 \rightarrow X$ be two mappings. We say that (X, σ, τ) is a *set-theoretic solution of the Yang-Baxter equation* if the mapping

$$x \otimes y \mapsto \sigma(x, y) \otimes \tau(x, y)$$

extends to a solution of the Yang-Baxter equation. It means that $r : X^2 \rightarrow X^2$, where $r = (\sigma, \tau)$, is a bijection and satisfies the *braid relation*:

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

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

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

Various algebraic structures are naturally associated with solutions (X, σ, τ) . Among others, there is a group of bijections defined on the set X . The *permutation group* $\mathcal{G}(X) = \langle \sigma_x : x \in X \rangle$ of a solution is the subgroup of the symmetric group $S(X)$ generated by mappings σ_x , with $x \in X$. The

Date: June 13, 2022.

2010 Mathematics Subject Classification. Primary: 16T25. Secondary: 20B35, 16T30.

Key words and phrases. Yang-Baxter equation, set-theoretic solution, multipermutation solution, indecomposable solution, permutation group.

group $\mathcal{G}(X)$ is also called *the Yang-Baxter group* (IYB group) associated to the solution (X, σ, τ) . A solution (X, σ, τ) is *indecomposable* if the permutation group $\mathcal{G}(X)$ acts transitively on X .

A solution with regular permutation group is called *unconnected* (see [25]). By definition, unconnected solutions are indecomposable.

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

$$x \sim y \iff \tau(-, x) = \tau(-, y).$$

They showed that the quotient set X/\sim can be again endowed with a structure of a solution and they call such a solution the *retraction* of the solution (X, σ, τ) and denote it by $\text{Ret}(X)$. A solution (X, σ, τ) is said to be a *permutation solution* (or *multipermutation solution of level 1*) if $|\text{Ret}(X)| = 1$. A non-permutation solution (X, σ, τ) is said to be a *multipermutation solution of level 2* (or briefly, *2-permutational solution*), if $|\text{Ret}(X)/\sim| = 1$.

Even describing all set-theoretic solutions still remains a very difficult task. For this reason it looks fruitful to prospect less complex solutions and, in some sense, treat them as “bricks” to build new ones. An approach to study solutions is to classify them according to their permutation groups. Special attention is now paid when such groups are transitive. Clearly, knowledge of indecomposable solutions could allow one to build all the decomposable ones. For example, Rump showed in [23] that every finite square free solution admits a nontrivial decomposition.

Cedó and Okniński characterized in [8] so called *simple* solutions (solutions with only trivial congruences). In particular, they proved that each finite simple solution (not of a prime order) is indecomposable. Moreover, by the results from [4], every finite indecomposable solution is a dynamical extension of a simple solution.

Unfortunately, it is not easy to find, in general, all the indecomposable solutions. The investigation of indecomposable solutions was initiated by Etingof et. al. in [10]. They showed there that such solutions of prime cardinality are permutation solutions with cyclic permutation group. In [19] the authors of this paper together with Zamojska-Dzienio gave a complete system of three invariants for finite non-isomorphic indecomposable solutions with cyclic permutation groups (cocyclic solutions). Smoktunowicz and Smoktunowicz presented in [26] a construction of all finite indecomposable solutions based on one-generated left braces. Also Rump in [25] gave another method of constructing indecomposable solutions from left braces. Additionally, the results of Bachiller, Cedó and Jespers [2] allow one to construct all solutions with a given permutation group. But all the above constructions require being able to construct all (finite) left braces. Moreover, by results of Smoktunowicz and Smoktunowicz, we know that one-generated left braces, and in consequence, indecomposable solutions of non-prime cardinality are quite frequent.

In the light of what we know it is reasonable to focus on a smaller class of indecomposable solutions, for instance multipermutation solutions of level 2 with non-abelian permutation group. Note that study multipermutation solutions of low levels attracts, among others, researchers interested in the quantum spaces (see e.g. [14]).

By results of Gateva-Ivanova, multipermutation solutions of level 2 can be characterized in an easy way.

Theorem 1.2. [13, Proposition 4.7] *Let (X, σ, τ) be a solution and $|X| \geq 2$. Then (X, σ, τ) is a multipermutation solution of level 2 if and only if the following condition holds for every $x, y, z \in X$:*

$$(1.2) \quad \sigma_{\sigma_y(x)} = \sigma_{\sigma_z(x)}.$$

All finite indecomposable solutions of the Yang-Baxter equation of multipermutation level at most 2 with abelian permutation groups were constructed in [18]. Probably the first example of an indecomposable solution of multipermutation level 2 with non-abelian permutation group was presented by Etingof et. al. in [10]. In [10, Subsection 3.3.] they constructed all indecomposable

solutions of multipermutation level 2 of order 6. Later on a new family of such solutions of order $2n$, for arbitrary $n \in \mathbb{N}$ and with the permutation group isomorphic to $\mathbb{Z}_n \rtimes \mathbb{Z}_2$, was presented in [18, Example 2.6]. Just recently, Castelli characterized in [5] all the unconnected solutions having odd size, a Z -group permutation group and having multipermutation level at most 2. He classified all such solutions with odd square-free order, up to isomorphism [5, Theorem 5.2].

In our paper, we study general indecomposable solutions of multipermutation level 2. In [17] the authors, together with Zamojska-Dzienio, presented a way how to obtain arbitrary solutions of multipermutation level 2. Now we apply this method to describe indecomposable ones. We show that an important rôle is played by one normal abelian subgroup of the permutation group, called the *displacement group*. We also find a way how to obtain (in theory) all indecomposable solutions of multipermutation level 2 of arbitrary size n and we show that there are at least $2^{n/2} - 1$ such solutions when n is a power of 2. This result has not been expected since the numbers of indecomposable solutions is known by [1] only up to the size of 11 and we have not have enough evidence about the growth of the numbers for powers of primes.

The paper is organized as follows. Since the most standard way how to construct solutions is using braces, in Section 2 we recall that every unconnected solution can be constructed from a left brace on the basis of results of Rump and we present some examples of this construction. In Section 3 we recall a connection between solutions of multipermutation level 2 and so-called *2-reductive* solutions and, based on this relationship, we describe the structure of the displacement group. Section 4 contains a construction of a special class of indecomposable solutions of multipermutation level 2 (Theorem 4.1). We study properties of the construction. In particular we show that the permutation group of each such solution is a semidirect product of its displacement group and a cyclic group and the automorphism group of the solution is transitive. Finally, in Section 5 we characterize all congruence relations of solutions constructed in Section 4, we show that every indecomposable solution of multipermutation level 2 is an image of one particular solution and also give a characterization of all the solutions that can be obtained by the construction described in Theorem 4.1. This allows us to calculate all such solutions up to the size of 17, which is done in Section 6. Additionally, we prove that the automorphism group of any indecomposable solution of multipermutation level 2 is regular.

2. UNCONNECTED 2-PERMUTATIONAL SOLUTIONS

In this section we recall some facts about braces and unconnected solutions. Rump in [24, Definition 2] introduced the notion of a brace and showed the correspondence between such structures and solutions. Here we use an equivalent definition formulated by Cedó, Jespers and Okniński.

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

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

The inverse element to a in the group (B, \circ) shall be denoted by a^- .

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

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

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

A brace is called *cyclic* if the additive group $(A, +)$ is cyclic, *bicyclic* if both groups are cyclic and it is *trivial* if $\text{Soc}(B) = B$.

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

One of methods to construct braces from given ones is by their semidirect product. Let $(B_1, +_1, \circ_1)$ and $(B_2, +_2, \circ_2)$ be two left braces and let $\alpha: (B_2, \circ_2) \rightarrow \text{Aut}(B_1, +_1, \circ_1)$ be a homomorphism of groups. The brace $B_1 \rtimes_{\alpha} B_2 = (B_1 \times B_2, +, \circ)$ with $(B_1 \times B_2, +) = (B_1, +_1) \times (B_2, +_2)$ and for $(x_1, x_2), (y_1, y_2) \in B_1 \times B_2$

$$(x_1, x_2) \circ (y_1, y_2) = (x_1 \circ_1 \alpha(x_2)(y_1), x_2 \circ_2 y_2)$$

is called the *semidirect product of the left braces* with respect to α . In particular,

$$\lambda_{(x_1, x_2)}((y_1, y_2)) = (x_1 \circ_1 \alpha(x_2)(y_1) - x_1, x_2 \circ_2 y_2 - x_2).$$

A subset X of a left brace $(B, +, \circ)$ is called a *cycle base* if X is a union of orbits of the action λ and generates the additive group $(B, +)$. A cycle base is *transitive* if it is a single orbit. Note that a transitive cycle base always exists in a cycle brace.

In [25, Theorem 4.2] Rump showed that with a left brace $(B, +, \circ)$ with a transitive cycle base X one can associate a unconnected solution (B, σ, τ) :

$$(2.2) \quad \sigma_x(y) := (\lambda_x(g))^{-} \circ y$$

for $x, y \in B$ and $g \in X$, such that the permutation group $\mathcal{G}(B)$ is isomorphic to the group (B, \circ) . On the other hand, each unconnected solution can be constructed in this way.

We now present an example of braces which later on will be good illustration of construction described in Section 4. As usual, we will denote by \mathbb{Z}_n the group $(\mathbb{Z}_n, +_n) = \mathbb{Z}/(n)$.

Example 2.2. Let $n \in \mathbb{N}$, $(G, +, 0)$ be an abelian group and $\alpha \in \text{Aut}(G)$ be of an order dividing n . Further, let $(B, +, \circ) = (G \times \mathbb{Z}_n, +, \circ)$ be the α -semidirect product of two trivial braces: $(G, +, +)$ and $(\mathbb{Z}_n, +_n, +_n)$. In this case, for $(a, i), (b, j) \in G \times \mathbb{Z}_n$ we have

$$(a, i) \circ (b, j) = (a + \alpha^i(b), i +_n j), \quad (a, i)^{-} = (-\alpha^{-i}(a), -i), \quad \text{and} \quad \lambda_{(a, i)}((b, j)) = (\alpha^i(b), j).$$

Assume now that an element $(g, h) \in G \times \mathbb{Z}_n$ lies in a transitive cycle base of $(B, +, \circ)$ (if such transitive cycle base exists). By Rump's result, $(G \times \mathbb{Z}_n, \sigma, \tau)$ with

$$\sigma_{(a, i)}((b, j)) = (\lambda_{(a, i)}((g, h)))^{-} \circ (b, j) = (-\alpha^{i-h}(g), -h) \circ (b, j) = (\alpha^{-h}(b) - \alpha^{i-h}(g), j - h),$$

for $(a, i), (b, j) \in G \times \mathbb{Z}_n$, is a unconnected solution with the permutation group $\mathcal{G}(G \times \mathbb{Z}_n)$ isomorphic to the semidirect product $G \rtimes \mathbb{Z}_n$ of groups $(G, +, 0)$ and \mathbb{Z}_n .

Moreover,

$$\sigma_{(a, i)}^{-1}((b, j)) = (\alpha^h(b) + \alpha^i(g), j + h).$$

It is worth noticing that the solution satisfies (1.2); for $(a, i), (a', i'), (b, j), (c, k) \in G \times \mathbb{Z}_n$ we have:

$$\sigma_{\sigma_{(a, i)}^{-1}((b, j))}^{-1}((c, k)) = \sigma_{(\alpha^h(b) + \alpha^i(g), j + h)}^{-1}((c, k)) = (\alpha^h(c) + \alpha^{j+h}(g), k + h) = \sigma_{\sigma_{(a', i')}^{-1}((b, j))}^{-1}((c, k)).$$

Hence, the solution is 2-permutational.

Example 2.3. Let $(G, +, 0) = \mathbb{Z}_2 \times \mathbb{Z}_2$ and let $\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \text{Aut} \mathbb{Z}_2 \times \mathbb{Z}_2$ be an automorphisms of order 3. Let $n = 3$ and $(g, h) = ((1, 0), 1)$. Clearly, the set $\{(\alpha^i((1, 0)), 1) \mid i \in \mathbb{Z}_3\} = \{((1, 0), 1), ((0, 1), 1), ((1, 1), 1)\}$ generates the group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. Hence, by Example 2.2, $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3, \sigma, \tau)$, with

$$\sigma_{((a_1, a_2), i)}(((b_1, b_2), j)) = (\alpha^{-1}((b_1, b_2)) - \alpha^{i-1}((1, 0)), j - 1) = ((b_1 + b_2, b_1) - \alpha^{i-1}((1, 0)), j - 1),$$

is a unconnected 2-permutational solution with the permutation group $\mathcal{G}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3)$ isomorphic to $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_3$.

Straightforward calculations show that all permutations σ_x are composed of cycles of length 3. We have also the abelian subgroup $(\{\text{id}, \sigma_1\sigma_0^{-1}, \sigma_2\sigma_0^{-1}, \sigma_1\sigma_0^{-1}\sigma_2\sigma_0^{-1}\}, \circ)$ of $\mathcal{G}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3)$ with $\mathbf{0} = ((0,0),0)$, $\mathbf{1} = ((0,0),1)$ and $\mathbf{2} = ((0,0),2)$, which is isomorphic to the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\langle \sigma_0 \rangle \cong \mathbb{Z}_3$.

Example 2.4. According to Rump's classification of cyclic left braces [?], for a left cyclic brace $(B, +, \circ)$ with $|B| = p^m$, for some prime p and $m \in \mathbb{N}$, the adjoint group (B, \circ) admits a cyclic subgroup of index less or equal to 2. Hence, if $p \neq 2$, the group (B, \circ) is cyclic, and consequently $(B, +, \circ)$ is bicyclic.

In [18, Corollary 4.8.] we, together with Zamojska-Dzienio, have already described all finite indecomposable solutions of the multipermutation level at most 2 with abelian (cyclic) permutation group. Since an abelian group acting transitively is regular, all of them are unconnected.

For a non-abelian cyclic left brace $(B, +, \circ)$, with $|B| = 2^m$, either $\text{Soc}(B)$ is of index 2 in $(B, +, \circ)$ or $B/\text{Soc}(B)$ is not bicyclic. In the latter case, the unconnected solution associated with $(B, +, \circ)$ is not a multipermutation solution of level at most 2. So, by [?, Proposition 12], to construct all unconnected solutions of the multipermutation level at most 2, of size 2^m with $m > 2$, and originated from a cyclic left brace, we have to consider only two types of such left braces of size 2^m .

Case 1. Let $(\mathbb{Z}_{2^m}, +, \circ)$ be a cyclic left brace with the adjoint group being a dihedral group. Then, for $a, b \in \mathbb{Z}_{2^m}$,

$$a \circ b = a + (-1)^a b = \begin{cases} a + b, & \text{if } a \text{ is even,} \\ a - b, & \text{if } a \text{ is odd.} \end{cases}$$

Let $g = 1$. Hence $\lambda_a(1) = a \circ 1 - a = (-1)^a = (\lambda_a(1))^-$. Thus $(\mathbb{Z}_{2^m}, \sigma, \tau)$, with

$$\sigma_a(b) = (\lambda_a(1))^- \circ b = (-1)^a + (-1)^{(-1)^a} b = \begin{cases} 1 - b, & \text{if } a \text{ is even,} \\ -1 - b = (2^m - 1)(1 + b), & \text{if } a \text{ is odd} \end{cases}$$

is a unconnected solution with the permutation group $\mathcal{G}(\mathbb{Z}_{2^m})$ isomorphic to the dihedral group D_{2^m} . Since the parity of both $1 - b$ and $-1 - b$ is the same for arbitrary $b \in \mathbb{Z}_{2^m}$, $(\mathbb{Z}_{2^m}, \sigma, \tau)$ is a multipermutation solution of level 2.

Case 2. Let $(\mathbb{Z}_{2^m}, +, \circ)$ be a cyclic left brace with the adjoint group being a generalized quaternion group. Then, for $a, b \in B$,

$$a \circ b = a + (2^{m-1} - 1)^a b = \begin{cases} a + b, & \text{if } a \text{ is even,} \\ a + (2^{m-1} - 1)b, & \text{if } a \text{ is odd.} \end{cases}$$

For $g = 1$,

$$\lambda_a(1) = a + (2^{m-1} - 1)^a - a = \begin{cases} 1, & \text{if } a \text{ is even,} \\ 2^{m-1} - 1, & \text{if } a \text{ is odd.} \end{cases}$$

The unconnected solution $(\mathbb{Z}_{2^m}, \sigma, \tau)$ is defined in the following way:

$$\sigma_a(b) = (\lambda_a(1))^- \circ b = \begin{cases} (1 - 2^{m-1})(1 - b), & \text{if } a \text{ is even,} \\ -1 + (2^{m-1} - 1)b, & \text{if } a \text{ is odd.} \end{cases}$$

As in the previous case, it is 2-permutational and its permutation group is isomorphic to the generalized quaternion group Q_{2^m} .

In Section 4 we will show that solutions described in Examples 2.2 - 2.4 are samples of a more general construction.

3. MULTIPERMUTATION SOLUTIONS OF LEVEL 2

In [17] the authors, together with Zamojska-Dzienio, presented a method of constructing all the solutions of multipermutation level 2. These solutions fall into two classes: 2-reductive ones and not 2-reductive ones. The former ones can be effectively constructed using a set of abelian groups and a family of constants. The non-2-reductive solutions can be also easily constructed, using a 2-reductive solution and a permutation. Let us shortly remind these constructions.

The less complicated class is formed by so called 2-reductive solutions. Recall that a solution (X, σ, τ) is called *2-reductive*, if it satisfies, for all $x, y \in X$,

$$(3.1) \quad \sigma_{\sigma_y(x)} = \sigma_x.$$

By [17, Lemma 2.7], Condition (3.1) is equivalent to the following one:

$$(3.2) \quad \sigma_{\sigma_y^{-1}(x)} = \sigma_x.$$

By [17, Theorem 7.7] each 2-reductive solution is a multipermutation solution of level 2 and note also ([15, Proposition 8.2], [13, Proposition 4.7]) that a square free solution is of level at most 2 if and only if it is 2-reductive.

The permutations of the 2-reductive solutions will be in this article, for some reason explained below, denoted by L_x and \mathbf{R}_x . These solutions can be completely characterized as follows:

Theorem 3.1. [17, Theorem 7.8] *Each 2-reductive solution (X, L, \mathbf{R}) is a disjoint union, over a set I , of abelian groups $(A_j, +) = \langle \{c_{i,j} \mid i \in I\} \rangle$, for every $j \in I$, with*

$$(3.3) \quad L_x(y) = y + c_{i,j} \in A_j \quad \text{and} \quad \mathbf{R}_y(x) = x - c_{j,i} \in A_i,$$

where $x \in A_i$ and $y \in A_j$.

According to [17, Lemma 3.3], for each 2-reductive solution the group $\langle L_x \mid x \in X \rangle$ is always abelian. Furthermore, by [17, Theorem 6.12] each multipermutation solution of level 2 originates from some 2-reductive one. The procedure is the following.

Theorem 3.2. [17, Algorithm 7.13] *Let (X, L, \mathbf{R}) be a 2-reductive solution. Assume that there exists $a \in X$ with $L_a = \text{id}$ and let π be a permutation of the set X satisfying, for $x, y \in X$, the condition:*

$$(3.4) \quad L_{\pi(y)} \pi L_x = L_{\pi(x)} \pi L_y.$$

Then (X, σ, τ) with $\sigma_x = L_x \pi$ and $\tau_y = \pi^{-1} \mathbf{R}_{\pi(y)}$ is a multipermutation solution of level 2.

On the other hand, each multipermutation solution of level 2 defines a 2-reductive one.

Theorem 3.3. [17, Theorem 7.12] *Let (X, σ, τ) be a multipermutation solution of level 2 and $e \in X$. Then (X, L, \mathbf{R}) , where $L_x = \sigma_x \sigma_e^{-1}$ and $\mathbf{R}_y = \sigma_e \tau_{\sigma_e^{-1}(y)}$, for $x, y \in X$, is a 2-reductive solution.*

We call the solution (X, L, \mathbf{R}) from Theorem 3.3 the σ_e^{-1} -isotope of (X, σ, τ) . From now on, we shall assume that one such 2-reductive solution is always associated to our solution of multipermutation level 2. Moreover, since $L_e = \text{id}$, by [17, Theorem 6.12], the solution (X, L, \mathbf{R}) satisfies Condition (3.4) for $\pi = \sigma_e$, that means $\sigma_x = L_x \pi = L_x \sigma_e$, for each $x \in X$.

Displacement group. Note that, for every $x, y \in X$,

$$(3.5) \quad L_x L_y^{-1} = L_x \pi \pi^{-1} L_y^{-1} = \sigma_x \sigma_y^{-1} \quad \text{and} \quad L_x L_e^{-1} = L_x.$$

This implies that, for a multipermutation solution of level 2, the group

$$\langle \sigma_x \sigma_y^{-1} \mid x, y \in X \rangle = \langle L_x L_y^{-1} \mid x, y \in X \rangle = \langle L_x \mid x \in X \rangle$$

is an abelian subgroup of $\mathcal{G}(X)$.

Such groups appear, for example, in the theory of racks and quandles under names: *displacement groups* [16] or *transvection groups* [21]. They play important rôle in the theory since some properties of racks or quandles may be described by properties of these groups. In Yang-Baxter equation solutions theory these groups have gained very little attention so far. A probable reason is that, given a left brace $(B, +, \circ)$, we have $\lambda_0 = \text{id}$ and therefore $\mathcal{G}(B) = \langle \sigma_x \sigma_y^{-1} \mid x, y \in B \rangle$, for the associated solution (B, σ, τ) . Nevertheless, it turns out that these groups are crucial when studying indecomposable multipermutation solutions of level 2 (see e.g. Proposition 5.12). Let us then denote the group by $\text{Dis}(X)$ and call it *the displacement group of the solution* (X, σ, τ) .

For the rest of the section we fix the following notation: let us have a solution (X, σ, τ) which is a multipermutation solution of level 2 and fix an element $\tilde{0} \in X$. The choice of the element $\tilde{0}$ might be of some relevance for decomposable solutions but does not matter at all for indecomposable solutions because, as we shall see in Proposition 5.18, the automorphism group of such solutions is transitive. Let us denote $\pi = \sigma_{\tilde{0}}$ and let (X, L, \mathbf{R}) be the π^{-1} -isotope defined in Theorem 3.3. We also, for each $i \in \mathbb{Z}$, denote $\tilde{i} = \pi^i(\tilde{0})$. The set $\{\tilde{i} \mid i \in \mathbb{Z}\}$ is a subset of X only but it turns out that it may be an important subset of X . We also denote $D_x = L_x L_{\pi^{-1}(x)}^{-1}$, for each $x \in X$.

Lemma 3.4. *Let (X, σ, τ) be a multipermutation solution of level 2. For each $x \in X$ and $i \in \mathbb{Z}$, we have*

$$(3.6) \quad \pi L_x = L_{\tilde{1}}^{-1} L_{\pi(x)} \pi$$

$$(3.7) \quad L_x \pi = \pi L_{\pi^{-1}(x)} L_{\tilde{-1}}^{-1}$$

$$(3.8) \quad \pi^i L_x \pi^{-i} = L_{\tilde{i}}^{-1} L_{\pi^i(x)}$$

$$(3.9) \quad \pi D_x = D_{\pi(x)} \pi$$

$$(3.10) \quad \sigma_{\tilde{i}} = \sigma_{\tilde{1}}^i \sigma_{\tilde{0}}^{1-i}$$

$$(3.11) \quad \sigma_{\alpha(x)} = \sigma_x, \text{ for all } \alpha \in \text{Dis}(X).$$

Proof. Using Equation (3.4) with $y = \tilde{0}$ we get

$$L_{\pi(x)} \pi L_{\tilde{0}} = L_{\tilde{1}} \pi L_x$$

and since $L_{\tilde{0}} = \text{id}$, we obtain (3.6). Using Equation (3.4) with $x = \tilde{-1}$ and $y = \pi^{-1}(x)$ we get

$$L_{\tilde{0}} \pi L_{\pi^{-1}(x)} = L_x \pi L_{\tilde{-1}}$$

and thus we obtain (3.7). In particular, by (3.6) and (3.7) we have

$$\pi L_x^{-1} = L_{\pi(x)}^{-1} L_{\tilde{1}} \pi.$$

The equation (3.8) is trivial for $i = 0$, then, by induction and commutativity of the group $\text{Dis}(X)$,

$$\pi \pi^i L_x \pi^{-i} \pi^{-1} = \pi L_{\tilde{i}}^{-1} L_{\pi^i(x)} \pi^{-1} \stackrel{(3.6)}{=} L_{\tilde{i+1}}^{-1} L_{\tilde{1}} \pi L_{\pi^i(x)} \pi^{-1} \stackrel{(3.6)}{=} L_{\tilde{i+1}}^{-1} L_{\tilde{1}} L_{\tilde{1}}^{-1} L_{\pi^{i+1}(x)} = L_{\tilde{i+1}}^{-1} L_{\pi^{i+1}(x)},$$

$$\pi^{-1} \pi^i L_x \pi^{-i} \pi = \pi^{-1} L_{\tilde{i}}^{-1} L_{\pi^i(x)} \pi \stackrel{(3.7)}{=} L_{\tilde{-1}} L_{\tilde{i-1}}^{-1} \pi^{-1} L_{\pi^i(x)} \pi \stackrel{(3.7)}{=} L_{\tilde{-1}} L_{\tilde{i-1}}^{-1} L_{\pi^{i-1}(x)} L_{\tilde{-1}}^{-1} = L_{\tilde{i-1}}^{-1} L_{\pi^{i-1}(x)}.$$

Further by commutativity of the group $\text{Dis}(X)$,

$$\begin{aligned} \pi D_x &= \pi L_x L_{\pi^{-1}(x)}^{-1} \stackrel{(3.6)}{=} L_{\pi(x)} L_{\tilde{1}}^{-1} \pi L_{\pi^{-1}(x)}^{-1} = L_{\pi(x)} L_{\tilde{1}}^{-1} (L_{\pi^{-1}(x)} \pi^{-1})^{-1} \stackrel{(3.6)}{=} \\ &L_{\pi(x)} L_{\tilde{1}}^{-1} (\pi^{-1} L_x L_{\tilde{1}}^{-1})^{-1} = L_{\pi(x)} L_{\tilde{1}}^{-1} L_{\tilde{1}} L_x^{-1} \pi = D_{\pi(x)} \pi. \end{aligned}$$

Then, by an induction on i ,

$$\sigma_{\tilde{i+1}} = L_{\tilde{i+1}} \pi \stackrel{(3.6)}{=} L_{\tilde{1}} \pi L_{\tilde{i}} = \sigma_{\tilde{1}} \sigma_{\tilde{i}} \pi^{-1} = \sigma_{\tilde{1}} \sigma_{\tilde{1}}^i \sigma_{\tilde{0}}^{1-i} \sigma_{\tilde{0}}^{-1} = \sigma_{\tilde{1}}^{i+1} \sigma_{\tilde{0}}^{-i},$$

and

$$\sigma_{\widetilde{i-1}} = L_{\widetilde{i-1}}\pi \stackrel{(3.6)}{=} \pi^{-1}L_{\widetilde{1}}^{-1}L_{\widetilde{i}}\pi^2 = \sigma_{\widetilde{1}}^{-1}\sigma_{\widetilde{i}}\sigma_{\widetilde{0}} = \sigma_{\widetilde{1}}^{-1}\sigma_{\widetilde{1}}^i\sigma_{\widetilde{0}}^{1-i}\sigma_{\widetilde{0}} = \sigma_{\widetilde{1}}^{i-1}\sigma_{\widetilde{0}}^{2-i}.$$

Finally, for $\alpha = \prod L_j^{\varepsilon_j}$, where $\varepsilon_j \in \{-1, 1\}$, we obtain $\sigma_{\alpha(x)} = L_{\prod L_j^{\varepsilon_j}(x)}\pi \stackrel{(3.1)+(3.2)}{=} L_x\pi = \sigma_x$. \square

Proposition 3.5. *Let (X, σ, τ) be a multipermutation solution of level 2. Then $\text{Dis}(X)$ is a normal abelian subgroup of $\mathcal{G}(X)$ and, for each $e \in X$,*

$$\mathcal{G}(X) = \langle \text{Dis}(X) \cup \{\sigma_e\} \rangle.$$

Moreover,

$$\text{Dis}(X) = \langle \sigma_x \sigma_e^{-1} \mid x \in X \rangle = \langle L_x \mid x \in X \rangle = \left\{ \prod \sigma_{x_i}^{\varepsilon_i} \mid \sum \varepsilon_i = 0 \right\}.$$

Proof. For $x \in X$, we have

$$\sigma_x = \sigma_x \sigma_e^{-1} \sigma_e \in \langle \text{Dis}(X) \cup \{\sigma_e\} \rangle.$$

Hence $\mathcal{G}(X) = \langle \text{Dis}(X) \cup \{\sigma_e\} \rangle$ and $\text{Dis}(X)$ is a normal subgroup by Equation (3.8).

Now $\sigma_x \sigma_y^{-1} = \sigma_x \sigma_e^{-1} (\sigma_y \sigma_e^{-1})^{-1}$ and therefore $\text{Dis}(X)$ is generated by the set $\{\sigma_x \sigma_e^{-1} \mid x \in X\}$. Setting $e = \widetilde{0}$ we obtain $\{\sigma_x \sigma_e^{-1} \mid x \in X\} = \{L_x \mid x \in X\}$.

Let $A = \{\prod \sigma_{x_i}^{\varepsilon_i} \mid \sum \varepsilon_i = 0\}$. By (3.5), generators of $\text{Dis}(X)$ belong to A , so we have $\text{Dis}(X) \subseteq A$. To prove the converse inclusion, consider $\alpha \in A$ written in the following form:

$$\alpha = \sigma_{x_1}^{\varepsilon_1} \sigma_{x_2}^{\varepsilon_2} \dots \sigma_{x_{n-1}}^{\varepsilon_{n-1}} \sigma_{x_n}^{\varepsilon_n}$$

with $\sum \varepsilon_i = 0$ and n being an even natural number.

We will prove by induction on n that $\alpha \in \text{Dis}(X)$. Clearly, if $n = 0$ then $\alpha = \text{id}$, hence suppose $n \geq 2$.

If $\varepsilon_1 = \varepsilon_n$ then there is $1 < m < n$ such that $\sum_{i < m} \varepsilon_i = 0$ and $\sum_{i \geq m} \varepsilon_i = 0$. Let $\beta = \sigma_{x_1}^{\varepsilon_1} \dots \sigma_{x_{m-1}}^{\varepsilon_{m-1}}$ and $\gamma = \sigma_{x_m}^{\varepsilon_m} \dots \sigma_{x_n}^{\varepsilon_n}$. By the induction hypothesis, $\beta, \gamma \in \text{Dis}(X)$, and in consequence $\alpha = \beta\gamma \in \text{Dis}(X)$.

If $\varepsilon_1 = -\varepsilon_n$ then $\alpha = \sigma_{x_1}^{\varepsilon_1} \beta \sigma_{x_n}^{-\varepsilon_1}$, where $\beta = \sigma_{x_2}^{\varepsilon_2} \dots \sigma_{x_{n-1}}^{\varepsilon_{n-1}}$. Since $\sum_{2 \leq i \leq n-1} \varepsilon_i = 0$, once again by the induction hypothesis, $\beta \in \text{Dis}(X)$. Moreover, $\alpha = \sigma_{x_1}^{\varepsilon_1} \beta \sigma_{x_n}^{-\varepsilon_1} = \sigma_{x_1}^{\varepsilon_1} \beta \sigma_{x_1}^{-\varepsilon_1} \sigma_{x_1}^{\varepsilon_1} \sigma_{x_n}^{-\varepsilon_1}$ and both $\sigma_{x_1}^{\varepsilon_1} \beta \sigma_{x_1}^{-\varepsilon_1}$ and $\sigma_{x_1}^{\varepsilon_1} \sigma_{x_n}^{-\varepsilon_1}$ lie in $\text{Dis}(X)$ since $\text{Dis}(X)$ is a normal subgroup. \square

Proposition 3.5 implies that, for $x, y \in X$,

$$[\sigma_x, \sigma_y] = \sigma_x^{-1} \sigma_y^{-1} \sigma_x \sigma_y \in \text{Dis}(X).$$

Therefore the commutator subgroup $\mathcal{G}(X)' = [\mathcal{G}(X), \mathcal{G}(X)]$ is a subgroup of $\text{Dis}(X)$. In the case of connected racks, we have $\mathcal{G}(X)' = \text{Dis}(X)$. This is not true in the case of solutions, as we shall see on the following example. Moreover, the example also shows that, $\text{Dis}(X)$ and $\langle \sigma_e \rangle$ may have a nontrivial intersection.

Example 3.6. [18, Example 3.2] Let $X = \mathbb{Z}_{p^2}$, for some prime p , and let $\sigma_i(j) = j + pi + 1$ and $\tau_j(i) = i - 1 - p(j + 1)$, for all $i, j \in X$. Then (X, σ, τ) is an indecomposable solution of multipermutation level 2 and $\mathcal{G}(X) \cong \mathbb{Z}_{p^2}$. It is easy to see that $\text{Dis}(X) = \{j \mapsto j + pk \mid k \in \mathbb{Z}\}$ and therefore $\sigma_i^p \in \text{Dis}(X)$, for all $i \in X$.

Remark 3.7. Let $n \in \mathbb{N}$, $(G, +, 0)$ be an abelian group and $\alpha \in \text{Aut}(G)$ be of an order dividing n . Let $(B, +, \circ)$ be a left non-trivial brace with a transitive cycle base X . Let $g \in X$ and (B, σ, τ) be a uniconnected solution with $\sigma_x(b) := (\lambda_x(g))^{-\circ} \circ b$ and $\sigma_x^{-1}(b) = \lambda_x(g) \circ b$, for $x, b \in B$. Note that by [5, Lemma 3.2], in cyclic braces, g is a generator of the additive group $(B, +)$.

It is well known (see e.g. [24, Proposition 7]) that for a non-zero left brace $(B, +, \circ)$, the solution associated to the factor left brace $B/\text{Soc}(B)$ is equal to the retraction of the solution associated to

$(B, +, \circ)$. Further, by results of Castelli [5, Theorem 3.5], the multipermutation level of the solution associated with a brace $(B, +, \circ)$ coincides with the multipermutation level of the unconnected solution associated with $(B, +, \circ)$. Moreover, by [6, Proposition 6] the multipermutation level of the solution associated with $(B, +, \circ)$ is equal to 2 if and only if $\tilde{B} = B/\text{Soc}(B) \neq \{0\}$ and $\tilde{B}/\text{Soc}(\tilde{B}) = \{0\}$. This gives that for each $x, y \in B$ there exists $s \in \text{Soc}(B)$ such that $x \circ y = x + y + s$ and in consequence for each $x \in X$ there exists $s_x \in \text{Soc}(B)$ such that $\sigma_x \sigma_0^{-1}(b) = s_x \circ b$. Since for $s_1, s_2 \in \text{Soc}(B)$, $s_1 \circ s_2 = s_1 + s_2$, each $\gamma \in \text{Dis}(B) = \langle \sigma_x \sigma_0^{-1} \mid x \in B \rangle$ may be understood as the left translation (with respect to the operation $+$) by some $s \in \text{Soc}(B)$. Thus, $\text{Dis}(B)$ is isomorphic to a subgroup of $(\text{Soc}(B), +)$. If the left brace $(B, +, \circ)$ is cyclic, the group $\text{Dis}(B)$ is cyclic too.

Now let $\gamma \in \text{Dis}(B) \cap \langle \sigma_0 \rangle$. Then there is $s \in \text{Soc}(B)$ such that $\gamma(b) = s \circ b$. On the other hand, there exist $m \in \mathbb{N}$ and $s' \in \text{Soc}(B)$ with $\gamma(b) = \sigma_0^m(b) = (-m \cdot g + s') \circ b$. This implies that $m \cdot g \in \text{Soc}(B)$ and $\sigma_0^m(b) = s \circ b$, for some $s \in \text{Soc}(B)$. This gives that the groups $\text{Dis}(X)$ and $\langle \sigma_0 \rangle$ may have a nontrivial intersection.

Since by assumption $\text{Soc}(B) \neq B$ and if the group $(B, +)$ is cyclic generated by g then $g \notin \text{Soc}(B)$. Hence, for example, groups $\text{Dis}(B)$ and $\langle \sigma_0 \rangle$ have a trivial intersection if $\langle \sigma_0 \rangle \cong \mathbb{Z}_2$.

Example 3.8. Let $(B, +, \circ) = (G \times \mathbb{Z}_n, +, \circ)$ be the α -semidirect product of trivial braces constructed in Example 2.2. Let X be a transitive cycle base of $(B, +, \circ)$, $(g, h) \in X$ and let $(G \times \mathbb{Z}_n, \sigma, \tau)$ with

$$\sigma_{(a,i)}((b, j)) = (\alpha^{-h}(b) - \alpha^{i-h}(g), j - h),$$

for $(a, i), (b, j) \in G \times \mathbb{Z}_n$ be the unconnected solution described in Example 2.2.

Thus we have $\sigma_{(0,0)}((b, j)) = (\alpha^{-h}(b) - \alpha^{-h}(g), j - h)$, and

$$\sigma_{(0,0)}^k((b, j)) = (\alpha^{-kh}(b) - \sum_{r=1}^k \alpha^{-rh}(g), j - kh).$$

Further, for $(a, i) \in G \times \mathbb{Z}_n$,

$$\sigma_{(a,i)} \sigma_{(0,0)}^{-1}((b, j)) = \sigma_{(a,i)}((\alpha^h(b) + g, j + h)) = (b + \alpha^{-h}(g) - \alpha^{i-h}(g), j) = (b, j) + (\alpha^{-h}(g) - \alpha^{i-h}(g), 0).$$

Since X is a transitive cycle base of $(B, +, \circ)$ and $(g, h) \in X$, the set $\{\alpha^{i-h}(g) \mid i \in \mathbb{Z}_n\}$ generates the group $(G, +, 0)$ and $\text{Dis}(G \times \mathbb{Z}_n) \cong (G, +, 0)$. Moreover, h is a generator of the group \mathbb{Z}_n . It is possible to prove that $\sum_{i=1}^n \alpha^i(b) = 0$, thus the order of $\sigma_{(0,0)}$ is equal to n and it is easy to see that $\text{Dis}(G \times \mathbb{Z}_n) \cap \langle \sigma_{(0,0)} \rangle = \{\text{id}\}$.

Example 3.9. Let $(\mathbb{Z}_{2^m}, \sigma, \tau)$ be a unconnected solution described in Example 2.4 with the permutation group isomorphic to the dihedral group D_{2^m} . In this case $\sigma_0(b) = 1 - b = \sigma_0^{-1}(b)$, and

$$\sigma_a \sigma_0^{-1}(b) = \begin{cases} b, & \text{if } a \text{ is even,} \\ (2^m - 1)(1 - b) = b - 2, & \text{if } a \text{ is odd.} \end{cases}$$

Hence, $\text{Dis}(\mathbb{Z}_{2^m}) \cong (\text{Soc}(\mathbb{Z}_{2^m}), +) = (2\mathbb{Z}_{2^m}, +) \cong \mathbb{Z}_{2^{m-1}}$. Moreover $\langle \sigma_0 \rangle \cong \mathbb{Z}_2$ and $\text{Dis}(\mathbb{Z}_{2^m}) \cap \langle \sigma_0 \rangle = \{\text{id}\}$. Consequently, $\mathcal{G}(\mathbb{Z}_{2^m}) = \text{Dis}(\mathbb{Z}_{2^m}) \rtimes \langle \sigma_0 \rangle \cong \mathbb{Z}_{2^{m-1}} \rtimes \mathbb{Z}_2$.

Similarly, for a unconnected solution $(\mathbb{Z}_{2^m}, +, \circ)$ with the permutation group isomorphic to the generalized quaternion group Q_{2^m} , we have $\text{Dis}(\mathbb{Z}_{2^m}) \cong (\text{Soc}(\mathbb{Z}_{2^m}), +) = (2\mathbb{Z}_{2^m}, +)$.

But in this case, $\sigma_0(b) = (1 - 2^{m-1})(1 - b)$, and

$$\sigma_a \sigma_0^{-1}(b) = \begin{cases} b, & \text{if } a \text{ is even,} \\ (2^{m-1} - 2) + b, & \text{if } a \text{ is odd} \end{cases}$$

which gives $\langle \sigma_0 \rangle \cong \mathbb{Z}_4$ and $\text{Dis}(\mathbb{Z}_{2^m}) \cap \langle \sigma_0 \rangle = \{\text{id}, \sigma_0^2\}$.

Note also that $\sigma_1^2 = \sigma_0^2$, which implies $\sigma_1 \sigma_0^{-2} = \sigma_1^{-1}$ and

$$\mathcal{G}(\mathbb{Z}_{2^m}) = \langle \alpha := \sigma_1 \sigma_0^{-1}, \beta := \sigma_0 \mid \alpha^{2^{m-1}} = \text{id}, \beta^2 = \alpha^{2^{m-2}}, \beta \alpha \beta^{-1} = \alpha^{-1} \rangle \cong Q_{2^m}.$$

By [18, Proposition 4.1] the abelian permutation group $\mathcal{G}(X)$ of an indecomposable multipermutation solution (X, σ, τ) of level 2 is generated by at most two elements and all the permutations σ_x , for $x \in X$, have the same order. Surprisingly, the same is also true for any indecomposable multipermutation solution of level 2.

Proposition 3.10. *Let (X, σ, τ) be an indecomposable solution of multipermutation level at most 2. Then*

- (1) *the permutation group $\mathcal{G}(X)$ is generated by at most two elements,*
- (2) *for all $x \in X$, σ_x have the same order,*
- (3) $\text{Dis}(X) = \langle L_{\tilde{i}} \mid i \in \mathbb{Z} \rangle = \langle D_{\tilde{i}} \mid i \in \mathbb{Z} \rangle.$

Proof. Let $x \in X$. The permutation group $\mathcal{G}(X)$ is transitive and therefore there exist $k \in \mathbb{N}$ and $y_1, \dots, y_k \in X$, such that

$$x = \sigma_{y_1}^{\varepsilon_1} \sigma_{y_2}^{\varepsilon_2} \cdots \sigma_{y_k}^{\varepsilon_k}(\tilde{0}) = (L_{y_1} \pi)^{\varepsilon_1} (L_{y_2} \pi)^{\varepsilon_2} \cdots (L_{y_k} \pi)^{\varepsilon_k}(\tilde{0}), \text{ with } \varepsilon_i \in \{-1, 1\}.$$

Since the displacement group is a normal subgroup of $\mathcal{G}(X)$ there is $\alpha \in \text{Dis}(X)$, such that

$$(L_{y_1} \pi)^{\varepsilon_1} (L_{y_2} \pi)^{\varepsilon_2} \cdots (L_{y_k} \pi)^{\varepsilon_k}(\tilde{0}) = \alpha \pi^k(\tilde{0}).$$

Then, by (3.11)

$$\sigma_x = L_x \pi = L_{\alpha \pi^k(\tilde{0})} \pi = L_{\pi^k(\tilde{0})} \pi = \sigma_{\tilde{k}} \stackrel{(3.10)}{=} \sigma_{\tilde{1}}^k \sigma_{\tilde{0}}^{1-k}$$

and therefore the permutation group $\mathcal{G}(X)$ is generated by $\sigma_{\tilde{0}}$ and $\sigma_{\tilde{1}}$, proving (1).

By an easy inductive argument on j , we have, for all integers $i \leq j+1$,

$$(3.12) \quad \prod_{k=i}^j D_{\tilde{k}} = L_{\tilde{j}} L_{\tilde{i-1}}^{-1}.$$

In particular, for $i = 1$ and $j \geq 0$ we obtain

$$(3.13) \quad L_{\tilde{j}} = \prod_{k=1}^j D_{\tilde{k}}.$$

Moreover, for $i \leq 0$ and $j = 0$ we have

$$(3.14) \quad L_{\tilde{i}} = \prod_{k=1+i}^0 D_{\tilde{k}}^{-1}.$$

We have already seen that, for each $x \in X$, there exists $k \in \mathbb{Z}$ such that $\sigma_x = \sigma_{\tilde{k}}$ and therefore $L_x = L_{\tilde{k}}$. Hence $\text{Dis}(X) = \langle L_x \mid x \in X \rangle = \langle L_{\tilde{k}} \mid k \in \mathbb{Z} \rangle = \langle D_{\tilde{k}} \mid k \in \mathbb{Z} \rangle$, proving (3).

Finally, let $\pi^r = \text{id}$, for some $r \in \mathbb{N}$. By (3.8) we have for $i, k \in \mathbb{Z}$

$$\pi L_{\tilde{k}}^{-1} L_{\tilde{i+k}} = L_{\tilde{k+1}}^{-1} L_{\tilde{i+k+1}} \pi.$$

Hence we obtain

$$(\sigma_{\tilde{i}})^r = (L_{\tilde{i}} \pi)^r \stackrel{(3.8)}{=} \prod_{k=0}^{r-1} (L_{\tilde{k}}^{-1} L_{\tilde{i+k}}) \pi^r = \prod_{k=0}^{r-1} L_{\tilde{k}}^{-1} \prod_{k=0}^{r-1} L_{\tilde{i+k}} = \text{id}$$

since $\tilde{m} = \widetilde{m+r}$, for all $m \in \mathbb{Z}$, and therefore $\{\tilde{0}, \dots, \widetilde{r-1}\} = \{\tilde{i}, \dots, \widetilde{i+r-1}\}$. Hence the order of $\sigma_{\tilde{i}}$ divides the order of $\sigma_{\tilde{0}}$. But $\tilde{0}$ was chosen randomly and thus we obtain (2). \square

Let us recall that a mapping $\Phi: X \rightarrow X'$ is a *homomorphism* of two solutions (X, σ, τ) and (X', σ', τ') if, for each $x \in X$,

$$\Phi\sigma_x = \sigma'_{\Phi(x)}\Phi.$$

We shall then denote by $\Phi_{\mathcal{G}}$ the homomorphism from the group $\mathcal{G}(X)$ to the group $\mathcal{G}(X')$ defined by $\sigma_x \mapsto \sigma'_{\Phi(x)}$. And by Φ_D we mean the restriction of $\Phi_{\mathcal{G}}$ to the homomorphism $\text{Dis}(X) \rightarrow \text{Dis}(X')$. Note that, for $\chi \in \mathcal{G}(X)$ and $x \in X$,

$$\Phi(\chi(x)) = \Phi_{\mathcal{G}}(\chi)\Phi(x).$$

Corollary 3.11. *Let (X, σ, τ) and (Y, ρ, ν) be two indecomposable solutions of multipermutation level 2. Let $\Phi_1: X \rightarrow Y$ and $\Phi_2: X \rightarrow Y$ be two homomorphisms of the solutions. If there exists $e \in X$ such that $\Phi_1(e) = \Phi_2(e)$ then $\Phi_1 = \Phi_2$.*

Proof. According to Proposition 3.10, the permutation group is generated by σ_e and $\sigma_{\sigma_e(e)}$. Let now $d \in X$. Since (X, σ, τ) is indecomposable, there exist numbers k and $\varepsilon_1, \dots, \varepsilon_k$ such that

$$d = \sigma_e^{\varepsilon_1} \sigma_{\sigma_e(e)}^{\varepsilon_2} \sigma_e^{\varepsilon_3} \sigma_{\sigma_e(e)}^{\varepsilon_4} \cdots \sigma_e^{\varepsilon_k}(e).$$

Now

$$\begin{aligned} \Phi_1(d) &= \Phi_1(\sigma_e^{\varepsilon_1} \sigma_{\sigma_e(e)}^{\varepsilon_2} \sigma_e^{\varepsilon_3} \sigma_{\sigma_e(e)}^{\varepsilon_4} \cdots \sigma_e^{\varepsilon_k}(e)) = \rho_{\Phi_1(e)}^{\varepsilon_1} \rho_{\rho_{\Phi_1(e)}(\Phi_1(e))}^{\varepsilon_2} \cdots \rho_{\Phi_1(e)}^{\varepsilon_k}(\Phi_1(e)) = \\ &\quad \rho_{\Phi_2(e)}^{\varepsilon_1} \rho_{\rho_{\Phi_2(e)}(\Phi_2(e))}^{\varepsilon_2} \cdots \rho_{\Phi_2(e)}^{\varepsilon_k}(\Phi_2(e)) = \Phi_2(\sigma_e^{\varepsilon_1} \sigma_{\sigma_e(e)}^{\varepsilon_2} \sigma_e^{\varepsilon_3} \sigma_{\sigma_e(e)}^{\varepsilon_4} \cdots \sigma_e^{\varepsilon_k}(e)) = \Phi_2(d). \quad \square \end{aligned}$$

4. A CONSTRUCTION OF INDECOMPOSABLE SOLUTIONS OF MULTIPERMUTATION LEVEL 2 WITH NON-ABELIAN PERMUTATION GROUP

In [18, Example 2.6] we, together with Zamojska-Dzienio, provided an example of an indecomposable solution of multipermutation level 2 of even order with non-abelian permutation group. In this section we extend the idea applied there and we construct a wider class of solutions of multipermutation level 2 with non-abelian permutation group.

Let us denote the group $(\mathbb{Z}, +, 0)$ by \mathbb{Z}_{∞} which will be helpful for our further considerations. Additionally, in the case $n = \infty$ we assume that $a \equiv b \pmod{n}$ if and only if $a = b$.

Theorem 4.1. *Let $n \in \mathbb{N} \cup \{\infty\}$ and $(G, +, 0)$ be an abelian group. Further, let $\mathbf{c} = (c_i)_{i \in \mathbb{Z}_n} \in G^n$ be a sequence such that $c_0 = 0$ and the group $(G, +, 0)$ is generated by the set $\{c_i \mid i \in \mathbb{Z}_n\}$. Then $(G \times \mathbb{Z}_n, \sigma, \tau)$ with*

$$\sigma_{(a,i)}((b,j)) = (b + c_{i-j-1} - c_{-j-1}, j+1)$$

and

$$\tau_{(a,i)}((b,j)) = (b - c_{i-j+1} + c_{-j}, j-1)$$

is an indecomposable solution of multipermutation level 2. Moreover, for any $(e, k) \in G \times \mathbb{Z}_n$,

$$\mathcal{G}(G \times \mathbb{Z}_n) = \text{Dis}(G \times \mathbb{Z}_n) \rtimes \langle \sigma_{(e,k)} \rangle.$$

Proof. Let us first define a matrix of constants $c_{i,j} = c_{i-j} - c_{-j}$, for $i, j \in \mathbb{Z}_n$. Note that, for each $j \in \mathbb{Z}_n$, $c_{j,0} = c_j$, $c_{0,j} = 0$ and $(G, +, 0) = \langle c_{i,j} \mid i \in \mathbb{Z}_n \rangle$. With this matrix we define, by Theorem 3.1, a 2-reductive solution $(G \times \mathbb{Z}_n, L, \mathbf{R})$ with

$$L_{(a,i)}((b,j)) = (b + c_{i,j}, j) \quad \text{and} \quad \mathbf{R}_{(a,i)}((b,j)) = (b - c_{i,j}, j),$$

for $(a,i), (b,j) \in G \times \mathbb{Z}_n$. Note that $L_{(a,i)} = L_{(0,i)}$, for every $a \in G$ and $i \in \mathbb{Z}_n$, and that $L_{(0,0)} = \text{id}$.

Now, let $\pi: G \times \mathbb{Z}_n \rightarrow G \times \mathbb{Z}_n$ be $\pi((a,i)) = (a, i+1)$. Clearly, this is a permutation on the set $G \times \mathbb{Z}_n$ with the inverse mapping $\pi^{-1}: G \times \mathbb{Z}_n \rightarrow G \times \mathbb{Z}_n$ given by $\pi^{-1}((a,i)) = (a, i-1)$.

To complete the construction of a solution of multipermutation level 2 we need to check Condition (3.4). Let us compute, for $(a, i), (b, j), (e, k) \in G \times \mathbb{Z}_n$,

$$\begin{aligned}
L_{\pi((a,i))} \pi L_{(b,j)}((e, k)) &= L_{(a,i+1)} \pi((e + c_{j,k}, k)) = L_{(a,i+1)}((e + c_{j,k}, k + 1)) \\
&= (e + c_{j,k} + c_{i+1,k+1}, k + 1) \\
&= (e + c_{j-k} - c_{-k} + c_{i-k} - c_{-k-1}, k + 1), \\
L_{\pi((b,j))} \pi L_{(a,i)}((e, k)) &= L_{(b,j+1)} \pi((e + c_{i,k}, k)) = L_{(b,j+1)}((e + c_{i,k}, k + 1)) \\
&= (e + c_{i,k} + c_{j+1,k+1}, k + 1) \\
&= (e + c_{i-k} - c_{-k} + c_{j-k} - c_{-k-1}, k + 1).
\end{aligned}$$

Then, by Theorem 3.2, the solution $(G \times \mathbb{Z}_n, \sigma, \tau)$ with

$$\sigma_{(a,i)}((b, j)) = L_{(a,i)} \pi((b, j)) = L_{(a,i)}((b, j + 1)) = (b + c_{i,j+1}, j + 1),$$

for $(a, i), (b, j) \in G \times \mathbb{Z}_n$, is a 2-permutational solution.

Recall, the solution is indecomposable, if the permutation group $\mathcal{G}(X)$ is transitive. Let us have $a \in G$ arbitrary. We first prove that $(a + c_i, 0)$ is in the same orbit as $(a, 0)$, for any $i \in \mathbb{Z}_n$:

$$\sigma_{(0,i)} \sigma_{(0,0)}^{-1}((a, 0)) \stackrel{(3.5)}{=} L_{(0,i)}((a, 0)) = (a + c_i, 0).$$

By an induction argument then $(a, 0)$ lies in the same orbit as $(0, 0)$, for any $a \in G$. Now, for any $b \in G$ and $j \in \mathbb{Z}_n$,

$$\sigma_{(0,0)}^j((b, 0)) = \pi^j((b, 0)) = (b, j)$$

and therefore the permutation group $\mathcal{G}(X)$ is transitive on $G \times \mathbb{Z}_n$.

Let $(a, i), (b, j) \in G \times \mathbb{Z}_n$. By the construction of permutations $L_{(a,i)}$ and $\sigma_{(b,j)}$, the intersection $\text{Dis}(G \times \mathbb{Z}_n) \cap \langle \sigma_{(b,j)} \rangle$ is trivial. Hence, Proposition 3.5 finishes the proof. \square

We will denote the solution described above by $\mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$, for $n \in \mathbb{N} \cup \{\infty\}$, a group $(G, +, 0)$ and $\mathbf{c} \in G^n$ specified in Theorem 4.1.

Let us note that $\mathcal{S}(\mathbb{Z}_1 \times \mathbb{Z}_n, \mathbf{0})$ is a permutation solution. On the other hand, $n = 1$ forces $|G| = 1$ and $\mathcal{S}(\mathbb{Z}_1 \times \mathbb{Z}_1, 0)$ is a trivial one element solution. Hence, from now on, we can assume $n > 1$.

Proposition 4.2. *Let $(X, \sigma, \tau) = \mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$ and let $\Psi: \text{Dis}(X) \rightarrow G$ be defined by $\prod L_{(0,i)}^{p_i} \mapsto \sum p_i \cdot c_i$. Then the mapping Ψ is a well-defined epimorphism and $\text{Ker } \Psi = \text{Dis}(X)_{(0,0)}$. In particular, $(G, +, 0) \cong \text{Dis}(X)/\text{Dis}(X)_{(0,0)}$.*

Proof. Recall, the abelian group $\text{Dis}(X)$ is generated by the set $\{L_{(0,i)} \mid i \in \mathbb{Z}_n\}$ and the group $(G, +, 0)$ is generated by the set $\{c_i \mid i \in \mathbb{Z}_n\}$. Since $L_{(0,i)}((a, 0)) = (a + c_i, 0)$, for all $a \in G$ and $i \in \mathbb{N}$, the mapping Ψ can be viewed as the action of $\text{Dis}(X)$ on $G \times \{0\}$ and therefore it is a homomorphism from $\text{Dis}(X)$ onto G . Clearly $\text{Ker } \Psi = \text{Dis}(X)_{(0,0)}$ and hence $(G, +, 0) \cong \text{Dis}(X)/\text{Dis}(X)_{(0,0)}$. \square

The following example presents in details the construction described in Theorem 4.1.

Example 4.3. Let $n = 4$, $(G, +, 0) = \mathbb{Z}_4 \times \mathbb{Z}_2$. and let choose $\mathbf{c} = (c_0, c_1, c_2, c_3) \in (\mathbb{Z}_4 \times \mathbb{Z}_2)^4$ as: $c_0 = (0, 0)$, $c_1 = (1, 0)$, $c_2 = (1, 0)$ and $c_3 = (2, 1)$. Clearly, $\mathbb{Z}_4 \times \mathbb{Z}_2 = \langle c_i : i \in \mathbb{Z}_4 \rangle$ and the 16 constants $c_{i,j}$ are:

$c_{i,j}$	0	1	2	3
1	(1, 0)	(2, 1)	(1, 1)	(0, 0)
2	(1, 0)	(3, 1)	(3, 0)	(1, 1)
3	(2, 1)	(3, 1)	(0, 0)	(3, 0)

Then $(\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_4, L, \mathbf{R})$ with

$$L_{(a_1, a_2, i)}((b_1, b_2, j)) = ((b_1, b_2) + c_{i,j}, j)$$

is a 2-reductive solution with an abelian permutation group generated by $\{L_{(0,0,i)} \mid i \in \{1, 2, 3\}\}$.

It is easy to see that the group is isomorphic to the subgroup of the group G^4 which is generated by the vectors $\vec{c}_i = (c_{i,0}, c_{i,1}, c_{i,2}, c_{i,3})$, for $i \in \{1, 2, 3\}$. Moreover, we see, for each $i \in \{1, 2, 3\}$, that $c_{i,i}$ is not a linear combination of the other two coefficients in the same column. Hence the permutation group has no less than three generators. Furthermore, we have $2\vec{c}_1 + 2\vec{c}_2 + 2\vec{c}_3 = \mathbf{0}$ and therefore the group is not a free \mathbb{Z}_4 -module. A GAP ([12]) calculation showed us that the order of the group is 2^5 .

Let us continue: the permutation $\pi: \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \rightarrow \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_4$ is given by

$$\pi((a_1, a_2, i)) = (a_1, a_2, i + 1).$$

Finally, $(\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_4, \sigma, \tau)$ with

$$\sigma_{(a_1, a_2, i)}((b_1, b_2, j)) = L_{(a_1, a_2, i)}\pi((b_1, b_2, j)) = ((b_1, b_2) + c_{i, j+1}, j + 1)$$

is an indecomposable solution $\mathcal{S}(\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbf{c})$ of multipermutation level 2 of size 2^5 .

Once again by GAP calculation, the group $\mathcal{G}(\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_4)$ is of order 2^7 and is isomorphic to the group $(\mathbb{Z}_4^2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_4$. Since the order of $\mathcal{G}(\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_4)$ is greater than the size of $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_4$, the solution $\mathcal{S}(\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbf{c})$ is not unconnected.

In the sequel, let us have $(X, \sigma, \tau) = \mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$, for some $n \in \mathbb{N} \cup \{\infty\}$, a group $(G, +, 0)$ and $\mathbf{c} \in G^m$.

Proposition 4.4. *The permutation group $\mathcal{G}(X)$ is abelian if and only if $c_{i \bmod n} = i \cdot c_1$, for all $i \in \mathbb{Z}$.*

Proof. Taking in (3.6), $\tilde{0} = (0, 0)$, we directly obtain

$$(4.1) \quad \pi L_{(a,i)} \pi^{-1} = L_{\pi((0,0))}^{-1} L_{\pi((a,i))} = L_{(0,1)}^{-1} L_{(a,i+1)}$$

for $a \in G$ and $i \in \mathbb{Z}_n$.

Recall that the abelian group $\text{Dis}(X)$ is generated by the set $\{L_{(0,i)} \mid i \in \mathbb{Z}_n\}$. Then by (4.1), the group $\mathcal{G}(X)$ is abelian if and only if for every $(b, j) \in G \times \mathbb{Z}_n$ and all $i \in \mathbb{Z}_n$

$$L_{(0,i)}((b, j)) = L_{(0,i+1)} L_{(0,1)}^{-1}((b, j)).$$

This is equivalent to, for all $i, j \in \mathbb{Z}_n$,

$$c_{i+1,j} = c_{i,j} + c_{1,j}.$$

This condition is equivalent to $c_{i+1-j} = c_{i-j} + c_{1-j} - c_{-j}$, for all $i, j \in \mathbb{Z}_n$. In particular, for $j = 0$, we obtain $c_{i+1} = c_i + c_1$, which, by an easy induction, implies $c_{i \bmod n} = i \cdot c_1$, for $i \in \mathbb{Z}$. On the other hand, $c_{i \bmod n} = i \cdot c_1$ implies $c_{i+1-j} + c_{-j} = c_{i-j} + c_{1-j}$ for $i, j \in \mathbb{Z}_n$. \square

Note that by Proposition 4.4, for a solution $\mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$ with abelian permutation group, the group $(G, +, 0)$ is cyclic. In a finite case, such solution with $\mathbf{c} = (c_i)_{i \in \mathbb{Z}_n} = (i)_{i \in \mathbb{Z}_n}$ overlaps with the solution $\mathcal{C}(m, n, 0)$ described in [18, Theorem 3.1].

Proposition 4.5. *For $x \in X$, the permutation $\sigma_x \in \mathcal{G}(X)$ is composed of cycles of length n .*

Proof. Let $(a, i), (b, j) \in G \times \mathbb{Z}_n$. By a straightforward induction we get for any $k \in \mathbb{N}$

$$(4.2) \quad \sigma_{(a,i)}^k((b, j)) = (b + \sum_{\ell=1}^k (c_{i-j-\ell} - c_{-j-\ell}), j + k)$$

and therefore $\sigma_{(a,i)}^k((b, j)) \neq (b, j)$ if k is not a multiple of n . Now

$$\sum_{\ell=1}^n (c_{i-j-\ell} - c_{-j-\ell}) = \sum_{\ell \in \mathbb{Z}_n} c_\ell - \sum_{\ell \in \mathbb{Z}_n} c_\ell = 0$$

and therefore $\sigma_{(a,i)}^n((b,j)) = (b,j)$. □

Proposition 4.6. *The automorphism group of the solution $\mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$ is regular.*

Proof. Let $g \in G$ and $k \in \mathbb{Z}_n$. For each $i \in \mathbb{Z}_n$ and $a \in G$, let

$$\Phi((a,i)) = \sigma_{(g,k)}^i((a+g,k)) = (a + \sum_{\ell=1}^i (c_{-\ell} - c_{-k-\ell}) + g, k+i).$$

This mapping is clearly a bijection and we shall now prove that it is a homomorphism of the solution.

$$\begin{aligned} \Phi(\sigma_{(a,i)}((b,j))) &= \Phi((b + c_{i-j-1} - c_{-j-1}, j+1)) = \\ &= (b + c_{i-j-1} - c_{-j-1} + \sum_{\ell=1}^{j+1} (c_{-\ell} - c_{-k-\ell}) + g, k+j+1) = \\ &= (b + \sum_{\ell=1}^j (c_{-\ell} - c_{-k-\ell}) + c_{i-j-1} - c_{-j-1} + c_{-j-1} - c_{-k-j-1} + g, k+j+1) \\ &= (b + \sum_{\ell=1}^j (c_{-\ell} - c_{-k-\ell}) + c_{i-j-1} - c_{-k-j-1} + g, k+j+1) = \\ &= \sigma_{(\text{anything}, k+i)}(b + \sum_{\ell=1}^j (c_{-\ell} - c_{-k-\ell}) + g, k+j) = \sigma_{\Phi((a,i))} \Phi((b,j)). \end{aligned}$$

Clearly $\Phi((0,0)) = (g,k)$ and hence $\text{Aut}(X)$ is transitive and, according to Corollary 3.11, it is regular. □

It is a question, which choice of parameters in the construction yields the same solution (up to isomorphism). We show that the obvious choice is the only possibility.

Theorem 4.7. *Two solutions $(X, \sigma, \tau) = \mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$ and $(X', \sigma', \tau') = \mathcal{S}(G' \times \mathbb{Z}_{n'}, \mathbf{c}')$ are isomorphic if and only if*

- (1) $n' = n$
- (2) *there exists a group isomorphism $g : G \rightarrow G'$ such that, for each $i \in \mathbb{Z}_n$*

$$c'_i = g(c_i).$$

Proof. “ \Rightarrow ” Let $\Phi : G \times \mathbb{Z}_n \rightarrow G' \times \mathbb{Z}_{n'}$ be an isomorphism of the solutions. According to Proposition 4.5, we have $n = n'$. According to Proposition 4.6, we may suppose $\Phi((0,0)) = (0,0)$. Since $\sigma_{(0,0)}((0,i)) = (0,i+1)$, we have $\Phi((0,i)) = (0,i)$, for each $i \in \mathbb{Z}_n$.

By Proposition 4.2, groups $\text{Dis}(X)/\text{Dis}(X)_{(0,0)}$ and $(G, +, 0)$ and $\text{Dis}(X')/\text{Dis}(X')_{(0,0)}$ and $(G', +, 0)$ are isomorphic through the isomorphism $\Psi : \text{Dis}(X)/\text{Dis}(X)_{(0,0)} \rightarrow G$ such that $L_{(0,i)}\text{Dis}(X)_{(0,0)} \mapsto c_i$ and the isomorphism $\Psi' : \text{Dis}(X')/\text{Dis}(X')_{(0,0)} \rightarrow G'$ such that $L'_{(0,i)}\text{Dis}(X')_{(0,0)} \mapsto c'_i$. Let $g = \Psi'\Phi_D\Psi^{-1}$ and $\alpha \in \text{Dis}(X)$. Hence $\Phi_D(\alpha)(\Phi((0,0))) = \Phi(\alpha((0,0)))$. Since $\Phi((0,0)) = (0,0)$ this implies that $\alpha \in \text{Dis}(X)_{(0,0)}$ if and only if $\Phi_D(\alpha) \in \text{Dis}(X')_{(0,0)}$. Then

$$g(c_i) = \Psi'\Phi_D(L_{(0,i)}\text{Dis}(X)_{(0,0)}) = \Psi'(L'_{(0,i)}\text{Dis}(X')_{(0,0)}) = c'_i.$$

“ \Leftarrow ” It is evident by straightforward calculations. □

Example 4.8. By Theorem 4.7, solutions $\mathcal{S}(\mathbb{Z}_m \times \mathbb{Z}_2, \mathbf{c} = (0,1))$ and $\mathcal{S}(\mathbb{Z}_m \times \mathbb{Z}_2, \mathbf{c} = (0,g))$, where $g \in \mathbb{Z}_m^*$, are isomorphic. Hence there is exactly one non-isomorphic solution of the form $\mathcal{S}(\mathbb{Z}_m \times \mathbb{Z}_2, \mathbf{c})$. On the other hand, for any prime number p , there are $p+1$ non-isomorphic

solutions of the form $\mathcal{S}(\mathbb{Z}_p \times \mathbb{Z}_3, \mathbf{c})$: $\mathcal{S}(\mathbb{Z}_p \times \mathbb{Z}_3, \mathbf{c} = (0, 0, 1))$ and $\mathcal{S}(\mathbb{Z}_p \times \mathbb{Z}_3, \mathbf{c} = (0, 1, g))$, for any $g \in \mathbb{Z}_p$.

We know that the displacement subgroup $\text{Dis}(G \times \mathbb{Z}_n)$ of a solution $\mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$ is abelian but, by Proposition 4.2, in general it is larger than the group $(G, +, 0)$. We shall show an example where this does not happen.

Proposition 4.9. *Let $r, k \in \mathbb{N}$ and let $(G, +, 0)$ be a free \mathbb{Z}_k -module of rank r . Let e_1, \dots, e_r be a free basis of $(G, +, 0)$. We set $n = 2r$, $c_0 = 0$, $c_i = \sum_{k=1}^i e_k$ and $c_{i+r} = \sum_{k=i+1}^r e_k$, for $i \in \{1, \dots, r\}$. Then the solution $(X, \sigma, \tau) = \mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$ is unconnected, $(G, +, 0) \cong \text{Dis}(X)$ and $\mathcal{G}(X) \cong G \rtimes_{\alpha} \mathbb{Z}_n$, where $\alpha(1)(e_i) = e_{i+1}$, for $i < r$, and $\alpha(1)(e_r) = -e_1$.*

Proof. The group generated by $\{L_{(0,i)} \mid i \in \mathbb{Z}_n\}$ is clearly a \mathbb{Z}_k -module. Actually, this module is generated by $\{L_{(0,1)}, \dots, L_{(0,r)}\}$ since $L_{(0,0)}$ is the identity permutation and $L_{(0,r+i)} = L_{(0,i)}^{-1} L_{(0,r)}$ for each $0 < i < r$.

By Proposition 4.2, $(G, +, 0) \cong \text{Dis}(X)/\text{Dis}(X)_{(0,0)}$ and the stabilizer $\text{Dis}(X)_{(0,0)}$ is the kernel of the group epimorphism $\Psi: \text{Dis}(X) \rightarrow G$ defined by $L_{(0,i)} \mapsto c_i$. Then, since for each $\gamma \in \text{Dis}(X)$ there is $a \in G$ such that $\gamma((0,0)) = (a, 0)$ and e_1, \dots, e_r is a free basis of $(G, +, 0)$, the kernel of Ψ is trivial and $(G, +, 0) \cong \text{Dis}(X)$.

Clearly, for $(b, j) \in G \times \mathbb{Z}_n$, $\pi((b, j)) = \sigma_{(0,0)}((b, j)) = (b, j+1)$, hence the order of π is equal to n and by Theorem 4.1, $\mathcal{G}(X) \cong G \rtimes \mathbb{Z}_n$. Moreover, $\Psi(D_{(0,i)}) = \Psi(L_{(0,i)} L_{(0,i-1)}^{-1}) = c_i - c_{i-1} = e_i$, for $0 < i \leq r$, and $\Psi(D_{(0,i)}) = -e_{i-r}$, for $r < i \leq 2r$. The rest follows from Equation (3.9). \square

Corollary 4.10. *Each finite abelian group embeds into the permutation group of an indecomposable unconnected solution of multipermutation level 2.*

Proof. Let $(G, +, 0)$ be a finite abelian group of an exponent k with r generators. Then $(G, +, 0)$ embeds into the free \mathbb{Z}_k -module of rank r . According to the Proposition 4.9, this module embeds into the permutation group of a unconnected solution. \square

5. HOMOMORPHIC IMAGES

In this section we focus on homomorphic images of the solutions constructed in the previous section. It turns out that there exists one universal indecomposable multipermutation solution of level 2, meaning that every indecomposable multipermutation solution of level 2 is a homomorphic image of the universal one. Since each image of an indecomposable multipermutation solution of level 2 is an indecomposable multipermutation solution of level at most 2, we may then conclude that indecomposable multipermutation solutions of level at most 2 form the class of all the images of one universal solution. This solution is constructed using the free abelian group of rank ω .

Recall from Section 3 that, for (X, σ, τ) a solution, we choose $\tilde{0} \in X$. Let $\pi = \sigma_{\tilde{0}}$ and let $\tilde{i} = \pi^i(\tilde{0})$, for each $i \in \mathbb{N}$. Let $L_{\tilde{i}} = \sigma_{\tilde{i}} \pi^{-1}$ and $D_{\tilde{i}} = L_{\tilde{i}} L_{\tilde{i}-1}^{-1}$.

Proposition 5.1. *Let $\bigoplus_{\mathbb{Z}} \mathbb{Z}$ be the free abelian group of rank ω and let $\{e_i \mid i \in \mathbb{Z}\}$ be a free basis of $\bigoplus_{\mathbb{Z}} \mathbb{Z}$. Each indecomposable multipermutation solution of level at most 2 is a homomorphic image of the solution $\mathcal{S}((\bigoplus_{\mathbb{Z}} \mathbb{Z}) \times \mathbb{Z}, \mathbf{c})$, where*

$$c_i = \begin{cases} \sum_{k=1}^i e_k & \text{for } i > 0, \\ 0 & \text{for } i = 0, \\ \sum_{k=1}^{-i} -e_{1-k} & \text{for } i < 0. \end{cases}$$

Proof. Let (X, σ, τ) be an indecomposable multipermutation solution of level at most 2. It is easy to see that $c_i - c_j = \sum_{k=j+1}^i e_k$, for any $i \geq j$. Let us define $\Phi: (\bigoplus_{\mathbb{Z}} \mathbb{Z}) \times \mathbb{Z} \rightarrow X$ by

$$\Phi((\sum r_k \cdot e_k, j)) = \prod D_{k+j}^{r_k}(\tilde{j}).$$

Now, for $i \geq 0$,

$$\begin{aligned} \Phi(\sigma(\sum r_k \cdot e_k, i)((\sum s_k \cdot e_k, j))) &= \Phi((\sum s_k \cdot e_k + c_{i-j-1} - c_{-j-1}, j+1)) = \\ \Phi((\sum s_k \cdot e_k + \sum_{\ell=-j}^{i-j-1} e_\ell, j+1)) &= \prod D_{k+j+1}^{s_k} \prod_{\ell=-j}^{i-j-1} D_{\ell+j+1}(\tilde{j+1}) = \\ \prod D_{k+j+1}^{s_k} \prod_{\ell=1}^i D_{\ell}(\tilde{j+1}) &\stackrel{(3.13)}{=} L_{\tilde{i}} \prod D_{k+j+1}^{s_k}(\tilde{j+1}), \\ \sigma_{\Phi((\sum r_k \cdot e_k, i))}(\Phi((\sum s_k \cdot e_k, j))) &= \sigma_{\prod D_{k+i}^{r_k}(\tilde{i})} \prod D_{k+j}^{s_k}(\tilde{j}) \stackrel{(3.11)}{=} \sigma_{\tilde{i}} \prod D_{k+j}^{s_k}(\tilde{j}) = \\ L_{\tilde{i}} \pi \prod D_{k+j}^{s_k}(\tilde{j}) &\stackrel{(3.9)}{=} L_{\tilde{i}} \prod D_{k+j+1}^{s_k} \pi(\tilde{j}) = L_{\tilde{i}} \prod D_{k+j+1}^{s_k}(\tilde{j+1}). \end{aligned}$$

For $i < 0$ we use $c_{i-j-1} - c_{-j-1} = -\sum_{k=i-j}^{-j-1} e_k = \sum_{k=i+1}^0 -e_k$ and then instead of (3.13) we apply (3.14). Hence Φ is a homomorphism which is clearly onto. \square

The researchers tend to focus on finite solutions and therefore it is useful to know that a finite solution is an image of a finite construction.

Proposition 5.2. *Let (X, σ, τ) be an indecomposable multipermutation solution of level at most 2. Then it is a homomorphic image of the solution $(Y, \rho, \nu) = \mathcal{S}(\text{Dis}(X) \times \mathbb{Z}_n, \mathbf{c})$, where $n = o(\pi)$ and $c_i = L_{\tilde{i}}$.*

Proof. We prove that the mapping $\Phi: Y \rightarrow X$ given by $(\gamma, j) \mapsto \pi^j \gamma(\tilde{0})$ is a homomorphism of solutions: (Y, ρ, ν) and (X, σ, τ) . Indeed, for $(\beta, i), (\gamma, j) \in \text{Dis}(X) \times \mathbb{Z}_n$

$$\begin{aligned} \Phi(\rho_{(\beta, i)}((\gamma, j))) &= \Phi((\gamma L_{i-j-1} L_{-j-1}^{-1}, j+1)) = \pi^{j+1} L_{i-j-1} L_{-j-1}^{-1} \gamma(\tilde{0}) \stackrel{(3.8)}{=} \\ L_{\tilde{i}} \pi^{j+1} L_{\pi^{-j-1}(\tilde{i})}^{-1} L_{i-j-1} \gamma(\tilde{0}) &= L_{\tilde{i}} \pi^j \pi^j \gamma(\tilde{0}) = \sigma_{\tilde{i}} \pi^j \gamma(\tilde{0}) \stackrel{(3.11)}{=} \sigma_{\pi^i \beta(\tilde{0})} \pi^j \gamma(\tilde{0}) = \sigma_{\Phi((\beta, i))}(\Phi((\gamma, j))). \end{aligned}$$

The homomorphism Φ is onto since the permutation group $\mathcal{G}(X)$ is transitive. \square

We can see in the proof that we can replace the group $\text{Dis}(X)$ by the group $\text{Dis}(X)/\text{Dis}(X)_{\tilde{0}}$ and it works as well. This gives us a characterization of all the solutions that can be obtained by the construction described in Theorem 4.1.

Corollary 5.3. *An indecomposable multipermutation solution (X, σ, τ) of level at most 2 is isomorphic to the solution of the form $\mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$, for some $n \in \mathbb{N}$, a group $(G, +, 0)$ and a sequence $\mathbf{c} \in G^n$, if and only if $\text{Dis}(X) \cap \langle \pi \rangle = \{\text{id}\}$ and $\mathcal{G}(X)_{\tilde{0}} \subseteq \text{Dis}(X)$.*

Proof. “ \Leftarrow ” By Proposition 5.2 it is sufficient to show that for solutions (X, σ, τ) with $\text{Dis}(X) \cap \langle \pi \rangle = \{\text{id}\}$ and $\mathcal{G}(X)_{\tilde{0}} \subseteq \text{Dis}(X)$, the mapping $\Phi: X \rightarrow \text{Dis}(X)/\text{Dis}(X)_{\tilde{0}}$ given by $(\gamma, j) \mapsto \pi^j \gamma(\tilde{0})/\text{Dis}(X)_{\tilde{0}}$ is an injection. Let $(\gamma, j), (\gamma', j') \in \text{Dis}(X) \times \mathbb{Z}_n$. Then

$$\pi^j \gamma(\tilde{0}) = \pi^{j'} \gamma'(\tilde{0}) \Leftrightarrow (\gamma')^{-1} \pi^{j-j'} \gamma(\tilde{0}) = \tilde{0} \Leftrightarrow (\gamma')^{-1} \pi^{j-j'} \gamma \in \mathcal{G}(X)_{\tilde{0}}.$$

The assumption $\mathcal{G}(X)_{\tilde{0}} \subseteq \text{Dis}(X)$ forces $\pi^{j-j'}$ to belong to $\text{Dis}(X)$. Further, by $\text{Dis}(X) \cap \langle \pi \rangle = \{\text{id}\}$, we obtain $\pi^{j-j'} = \text{id}$. Hence, $(\gamma')^{-1} \gamma \in \text{Dis}(X)_{\tilde{0}}$, which proves that $\gamma \equiv \gamma' \pmod{\text{Dis}(X)_{\tilde{0}}}$.

“ \Rightarrow ” It follows from the construction of the solution $\mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$. \square

In particular, whenever (X, σ, τ) is unconnected and $\text{Dis}(X) \cap \langle \pi \rangle$ is trivial, the mapping Φ from the proof of Proposition 5.2 is an isomorphism. One such example comes from Example 3.8.

Remark 5.4. Let us consider the solution $(G \times \mathbb{Z}_n, \sigma, \tau)$ from Example 3.8. In this case $\text{Dis}(G \times \mathbb{Z}_n) \cong (G, +, 0)$,

$$\pi((b, j)) = \sigma_{(0,0)}((b, j)) = (\alpha^{-h}(b) - \alpha^{-h}(g), j - h),$$

and for $i \in \mathbb{Z}_n$

$$\begin{aligned} L_i((b, j)) &= L_{\pi^i((0,0))}((b, j)) = \sigma_{\pi^i((0,0))} \sigma_{(0,0)}^{-1}((b, j)) = \sigma_{(-\sum_{r=1}^i \alpha^{-rh}(g), -ih)} \sigma_{(0,0)}^{-1}((b, j)) = \\ &= (b + \alpha^{-h}(g) - \alpha^{-ih-h}(g), j). \end{aligned}$$

Therefore, we obtain that $(G \times \mathbb{Z}_n, \sigma, \tau)$ is isomorphic to the solution $\mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$, for $\mathbf{c} = (c_i)_{i \in \mathbb{Z}_n} = (\alpha^{-h}(g) - \alpha^{-(i+1)h}(g))_{i \in \mathbb{Z}_n} \in G^n$. Clearly, by Theorem 4.7 this solution is isomorphic to the solution $\mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$, for $\mathbf{c} = (-\alpha^{-(i+1)h}(g))_{i \in \mathbb{Z}_n} \in G^n$.

Example 5.5. By Remark 5.4 the solution $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3, \sigma, \tau)$, with

$$\sigma_{((a_1, a_2), i)}(((b_1, b_2), j)) = (\alpha^2((b_1, b_2)) + \alpha^{i-1}((1, 0)), j - 1) = ((b_1 + b_2, b_1) + \alpha^{i-1}((1, 0)), j - 1),$$

and $\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, described in Example 2.3, is isomorphic to the solution:

$$\mathcal{S}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3, \mathbf{c} = ((0, 0), (1, 0), (0, 1))).$$

In this case $c_{0,j} = (0, 0)$, $c_{1,j} = (1, 0)$ and $c_{2,j} = (0, 1)$ and

$$\sigma_{((a_1, a_2), i)}(((b_1, b_2), j)) = ((b_1, b_2) + c_{i,j+1}, j + 1).$$

Congruences. In the sequel we focus on homomorphic images of the solutions. It is well known that homomorphisms of solutions and equivalence relations preserving the structure of solutions are closely related: let (X, σ, τ) be a solution. An equivalence relation $\asymp \subseteq X \times X$ such that for $x_1, x_2, y_1, y_2 \in X$

$$(5.1) \quad x_1 \asymp x_2 \text{ and } y_1 \asymp y_2 \quad \Rightarrow \quad \sigma_{x_1}^\varepsilon(y_1) \asymp \sigma_{x_2}^\varepsilon(y_2),$$

where $\varepsilon \in \{-1, 1\}$, is called a *congruence* of the solution (X, σ, τ) .

If $\Phi: X \rightarrow X'$ is a homomorphism from a solution (X, σ, τ) to a solution (X', σ', τ') then the *kernel* of Φ , defined by

$$x_1 \ker \Phi x_2 \quad \Leftrightarrow \quad \Phi(x_1) = \Phi(x_2)$$

is a congruence of (X, σ, τ) . On the other hand, for a congruence \asymp of the solution (X, σ, τ) , let $\chi: X \rightarrow X/\asymp$ defined by $(a, i) \mapsto (a, i)/\asymp$ be the *natural projection* from the solution to the quotient one. Clearly, χ is onto and $\ker \chi = \asymp$.

Moreover, for any epimorphism $\Phi: X \rightarrow X'$, the solution (X', σ', τ') is isomorphic to the quotient solution $(X, \sigma, \tau)/\ker \Phi$. Hence, a solution is a homomorphic image of a solution (X, σ, τ) if and only if it is isomorphic to a quotient of (X, σ, τ) by some congruence. Thus the problem of finding all homomorphic images of (X, σ, τ) reduces to the problem of finding all congruences of (X, σ, τ) .

Lemma 5.6. Let $(X, \sigma, \tau) = \mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$ and \asymp be a congruence of the solution (X, σ, τ) . Then

(1) there exists H , a subgroup of $(G, +, 0)$ such that, for all $a, b \in G$ and each $i \in \mathbb{Z}_n$,

$$(a, i) \asymp (b, i) \quad \text{if and only if} \quad a - b \in H;$$

(2) there exists $m \in \mathbb{N} \cup \{\infty\}$ such that

- m is a divisor of n , if n is finite,
- if $(a, i) \asymp (b, j)$, for some $a, b \in G$ and $i, j \in \mathbb{Z}_n$, then $i - j \equiv 0 \pmod{m}$,

- if m is finite then $c_i - c_{i+m} \in H$, for all $i \in \mathbb{Z}_n$.

Proof. Recall that, for $(a, i), (b, j) \in G \times \mathbb{Z}_n$, $L_{(a,i)}((b, j)) = (b + c_{i-j} - c_{-j}, j)$, $\pi((b, j)) = (b, j + 1)$ and $\sigma_{(a,i)}((b, j)) = (b + c_{i-j-1} - c_{-j-1}, j + 1)$.

(1) By definition, the group $(G, +, 0)$ is generated by the set $\{c_i : i \in \mathbb{Z}_n\}$. It simply means that, for each $g \in G$ and $i \in \mathbb{Z}_n$, there exists a permutation $\alpha \in \text{Dis}(G \times \mathbb{Z}_n)$ such that, for every $a \in G$,

$$(5.2) \quad (a + g, i) = \alpha((a, i)).$$

Hence, for each $a, b \in G$, $i \in \mathbb{Z}_n$ and $g \in G$,

$$(a, i) \asymp (b, i) \Rightarrow \alpha((a, i)) \asymp \alpha((b, i)) \Rightarrow (a + g, i) \asymp (b + g, i).$$

Analogously, using π^k we prove, for $a, b \in G$ and $i, j, k \in \mathbb{Z}_n$,

$$(5.3) \quad (a, i) \asymp (b, j) \Rightarrow (a, i + k) \asymp (b, j + k).$$

Let $(a, i), (b, i), (a', i), (b', i) \in G \times \mathbb{Z}_n$ be such that $(a, i) \asymp (b, i)$ and $(a', i) \asymp (b', i)$. Hence

$$(a + a', i) \asymp (b + a', i) \asymp (b + b', i).$$

Therefore, for each $i \in \mathbb{Z}_n$, $H_i = \{a \in G \mid (a, i) \asymp (0, i)\}$ is a subgroup of $(G, +, 0)$ and

$$\begin{aligned} a, a' \in H_i &\Leftrightarrow (a, i) \asymp (a', i) \Leftrightarrow (0, i) \asymp (a - a', i) \\ &\Leftrightarrow (0, 0) \asymp (a - a', 0) \Leftrightarrow a - a' \in H_0. \end{aligned}$$

In particular, for each $i \in \mathbb{Z}_n$, $H_i = H_0$.

(2) If $(a, i) \asymp (a', i')$ always implies $i = i'$ then we can take $m = n$ and the proof is finished. Suppose hence, for the rest of the proof, that there exist $(a, i), (a', i') \in G \times \mathbb{Z}_n$ such that $(a, i) \asymp (a', i')$ and $i \neq i'$.

Let m be the smallest positive integer such that there exists $d \in G$ with $(0, 0) \asymp (d, m)$. Let $\gamma \in \text{Dis}(X)$ be such that $\gamma((0, m)) = (d, m)$. Then $(0, 0) \asymp \gamma\pi^m((0, 0))$ and, by induction, $(0, 0) \asymp (\gamma\pi^m)^k((0, 0))$, for any $k \in \mathbb{Z}$. If n is finite then we can set $k = \lceil \frac{n}{m} \rceil$ and we see that there exists some $b \in G$ such that $(0, 0) \asymp (b, km) = (b, km - n)$. Since $0 \leq km - n < m$ and m is minimal, necessarily m divides n .

Let again $(a, i) \asymp (a', i')$ for some $a, a' \in G$ and $i, i' \in \mathbb{Z}_n$. Let $\beta \in \text{Dis}(X)$ be such that $\beta((0, 0)) = (a, 0)$. Then by (5.3),

$$(a, i) \asymp (a', i') \Leftrightarrow (a, 0) \asymp (a', i' - i) \Leftrightarrow (0, 0) \asymp \beta^{-1}((a', i' - i)).$$

Hence $i' \equiv i \pmod{m}$.

Finally, for each $i \in \mathbb{Z}_n$,

$$\begin{aligned} (5.4) \quad (0, 0) \asymp (d, m) &\Leftrightarrow (0, i) \asymp (d, m + i) \Rightarrow L_{(0,i)}((0, 0)) \asymp L_{(d, m+i)}((0, 0)) \\ &\Leftrightarrow (c_i, 0) \asymp (c_{m+i}, 0) \Leftrightarrow c_i - c_{m+i} \in H_0. \quad \square \end{aligned}$$

Lemma 5.7. Let (X, σ, τ) , \asymp , H and m be as in Lemma 5.6. Let m be finite and let $\Phi : X \rightarrow X/\asymp$ be the natural projection. Then $[\pi^m, \text{Dis}(X)] \subseteq \text{Ker } \Phi_D$.

Proof. For all $b \in G$ and $i, j \in \mathbb{Z}_n$ we have

$$\begin{aligned} \pi^{-m} L_{(0,i)}^{-1} \pi^m L_{(0,i)}((b, j)) &= \pi^{-m} L_{(0,i)}^{-1} \pi^m((b + c_{i-j} - c_{-j}, j)) = \\ \pi^{-m} L_{(0,i)}^{-1}((b + c_{i-j} - c_{-j}, j + m)) &= \pi^{-m}((b + c_{i-j} - c_{-j} - (c_{i-j-m} - c_{-j-m}), j + m)) = \\ &= (b + c_{i-j} - c_{i-j-m} + c_{-j-m} - c_{-j}, j) = (b + h, j) \end{aligned}$$

for some $h \in H$, according to Lemma 5.6 (2). Hence, by Lemma 5.6 (1),

$$(b, j) \asymp (b + h, j) = [\pi^m, L_{(0,i)}]((b, j)).$$

This gives $\Phi((b, j)) = \Phi_{\mathcal{G}}([\pi^m, L_{(0,i)}])\Phi((b, j))$ and therefore $[\pi^m, L_{(0,i)}] \in \text{Ker}(\Phi_{\mathcal{G}})$. Since $\text{Dis}(X)$ is a normal subgroup of $\mathcal{G}(X)$, we obtain $[\pi^m, L_{(0,i)}] \in \text{Dis}(X)$. Because $\text{Dis}(X) = \langle L_{(0,i)} \mid i \in \mathbb{Z}_n \rangle$, this completes the proof. \square

Proposition 5.8. *An equivalence relation \asymp is a congruence of the solution $(X, \sigma, \tau) = \mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$ if and only if there exist a subgroup H of $(G, +, 0)$, $m \in \mathbb{N} \cup \{\infty\}$ and $r \in G$ such that:*

- i) m divides n , if n is finite;
- ii) if m is finite then $c_i - c_{i+m} \in H$, for each $i \in \mathbb{Z}_n$;
- iii) if n and m are finite then $\frac{n}{m} \cdot r \in H$;
- iv) for all $a, a' \in G$ and $i, i' \in \mathbb{Z}_n$

$$(5.5) \quad (a, i) \asymp (a', i') \Leftrightarrow i - i' \equiv 0 \pmod{m} \text{ and } \begin{cases} a' - a \equiv \frac{i-i'}{m} \cdot r \pmod{H} & \text{if } m < \infty \\ a' - a \in H & \text{if } m = \infty. \end{cases}$$

Proof. Let \asymp be a congruence of the solution (X, σ, τ) . The items (i) and (ii) were proved in Lemma 5.6. If $n = m$ then (iii) and (iv) also follow from Lemma 5.6. Suppose hence $m < n$.

Recall that, if n is finite, m is the smallest positive integer such that there exists $d \in G$ with $(0, 0) \asymp (d, m)$. Let now $\gamma \in \text{Dis}(X)$ be such that $(0, 0) \asymp \pi^m \gamma(0, 0)$ and denote by r the element from G such that $\gamma((0, 0)) = (r, 0)$. Let $\iota = [\gamma, \pi^m]$. By Lemma 5.7, $\iota((0, 0)) \asymp (0, 0)$. By Lemma 5.6, there exists $h \in H$ such that $\iota((0, 0)) = (h, 0)$.

Then

$$(\pi^m \gamma)^{n/m}((0, 0)) = \pi^n \gamma^{n/m} \iota^{\binom{n/m}{2}}((0, 0)) = \left(\frac{n}{m} \cdot r + \binom{n/m}{2} \cdot h, 0\right).$$

Since $\pi^m \gamma((0, 0)) \asymp (0, 0)$, then by Lemma 5.6 we obtain $r \cdot \frac{n}{m} \in H$.

Further, we will show that for $a, b \in G$ and $k \in \mathbb{Z}_n$ with $m \mid k$, if $(a, 0) \asymp (b, k)$ then $(0, 0) \asymp (b - a, k)$. Let $\chi \in \text{Dis}(X)$ be such that $\chi((a, 0)) = (0, 0)$. Assume $\chi = L_{(0,i_1)}^{p_1} \dots L_{(0,i_s)}^{p_s}$ for some numbers $i_1, \dots, i_s \in \mathbb{Z}_n$ and $p_1, \dots, p_s \in \mathbb{Z}$. This implies

$$\chi((a, 0)) = L_{(0,i_1)}^{p_1} \dots L_{(0,i_s)}^{p_s}((a, 0)) = \left(a + \sum_{\ell=1}^s p_{\ell} \cdot c_{i_{\ell}}, 0\right) = (0, 0)$$

and therefore $\sum p_{\ell} \cdot c_{i_{\ell}} = -a$. Hence,

$$\chi((b, k)) = L_{(0,i_1)}^{p_1} \dots L_{(0,i_s)}^{p_s}((b, k)) = \left(b + \sum_{\ell=1}^s p_{\ell} \cdot c_{i_{\ell}, k}, k\right) = \left(b + \sum_{\ell=1}^s p_{\ell} \cdot (c_{i_{\ell}-k} - c_{-k}), k\right).$$

Since $m \mid k$ then, by Lemma 5.6, $c_{i_{\ell}} - c_{i_{\ell}-k} \in H$ and $c_{-k} \in H$. So, there is $\bar{h} \in H$ such that

$$\chi((b, k)) = \left(b + \sum_{\ell=1}^s p_{\ell} \cdot c_{i_{\ell}} + \bar{h}, k\right) = (b - a + \bar{h}, k) \asymp (b - a, k).$$

Now, let $a, a' \in G$ and $i \neq i' \in \mathbb{Z}_n$ be such that $(a, i) \asymp (a', i')$. Then, $m \mid (i' - i)$ by Lemma 5.6 and, by (5.3), $(a, 0) \asymp (a', i' - i)$. Hence, $(0, 0) \asymp (a' - a, i' - i)$. Now

$$(0, 0) \asymp (\pi^m \gamma)^{\frac{i'-i}{m}}((0, 0)) = \pi^{i'-i} \gamma^{\frac{i'-i}{m}} \iota^{\binom{i'-i}{2}/m}((0, 0)) = \left(\frac{i'-i}{m} \cdot r + \binom{i'-i}{2}/m \cdot h, i' - i\right).$$

Hence, once again by Lemma 5.6

$$a' - a - \frac{i'-i}{m} \cdot r + \binom{i'-i}{2}/m \cdot h \in H$$

which is equivalent to

$$a' - a + \frac{i'-i}{m} \cdot r \equiv 0 \pmod{H}.$$

Conversely, we will show that an equivalence relation \asymp defined by (5.5) is a congruence of the solution (X, σ, τ) . Suppose $m < \infty$.

Let $(a, i) \asymp (a', i')$ and $(b, j) \asymp (b', j')$. By definition, $(j' + 1) \equiv (j + 1) \pmod{m}$ and $b - b' + \frac{j'-j}{m} \cdot r \equiv 0 \pmod{H}$. Further, by Lemma 5.6,

$$\begin{aligned} b - b' + \frac{j'-j}{m} \cdot r &= b + c_{i-j-1} - c_{-j-1} - b' - c_{i-j-1} + c_{-j-1} + \frac{j'-j}{m} \cdot r \equiv \\ &= b + c_{i-j-1} - c_{-j-1} - b' - c_{i'-j'-1} + c_{-j'-1} + \frac{j'-j}{m} \cdot r = \\ &= b + c_{i-j-1} - c_{-j-1} - b' + c_{i'-j'-1} - c_{-j'-1} + \frac{(j'+1)-(j+1)}{m} \cdot r \equiv 0 \pmod{H}. \end{aligned}$$

Since

$$\begin{aligned} \sigma_{(a,i)}((b, j)) &= (b + c_{i-j-1} - c_{-j-1}, j + 1), \quad \text{and} \\ \sigma_{(a',i')}((b', j')) &= (b' + c_{i'-j'-1} - c_{-j'-1}, j' + 1), \end{aligned}$$

this finishes the proof for $m < \infty$. But the case $m = \infty$ is similar. \square

Let $\theta(m, H, r)$ denote the congruence relation of a solution $\mathcal{S}(G \times \mathbb{Z}_m, \mathbf{c})$ specified by the triple m, H and r from Proposition 5.8. By (5.5), $\theta(m, G, r) = \theta(m, G, s)$, whenever $r \equiv s \pmod{H}$. In Theorem 5.19 we will show that this is the only possibility how to obtain isomorphic solutions.

Example 5.9. Let us consider the 12-element solution $\mathcal{S}(\mathbb{Z}_2 \times \mathbb{Z}_6, \mathbf{c} = (0, 1, 1, 0, 1, 1))$. Since, $c_i = c_{i+3}$, for each $i \in \mathbb{Z}_6$, by Proposition 5.8 there are seven different congruences of the solution: $\theta(6, \{0\}, 0)$, $\theta(3, \{0\}, 0)$, $\theta(3, \{0\}, 1)$, $\theta(6, \mathbb{Z}_2, 0)$, $\theta(3, \mathbb{Z}_2, 0)$, $\theta(2, \mathbb{Z}_2, 0)$ and $\theta(1, \mathbb{Z}_2, 0)$

The congruence $\theta = \theta(3, \{0\}, 1)$ induces the quotient solution (Y, σ, τ) , where $Y = \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}\}$ is defined by:

$$\begin{aligned} \mathbf{0} &= (0, 0)/\theta = (1, 3)/\theta & \mathbf{1} &= (1, 0)/\theta = (0, 3)/\theta & \mathbf{2} &= (0, 1)/\theta = (1, 4)/\theta, \\ \mathbf{3} &= (1, 1)/\theta = (0, 4)/\theta & \mathbf{4} &= (0, 2)/\theta = (1, 5)/\theta & \mathbf{5} &= (1, 2)/\theta = (0, 5)/\theta. \end{aligned}$$

It is then possible to compute the permutations:

$$\sigma_0 = \sigma_1 = (\mathbf{024135}); \quad \sigma_2 = \sigma_3 = (\mathbf{035124}); \quad \sigma_4 = \sigma_5 = (\mathbf{025134}).$$

Hence $\mathcal{G}(Y)$ is a non-abelian group of order 24, $\text{Dis}(Y) = \{\text{id}, (\mathbf{23})(\mathbf{45}), (\mathbf{01})(\mathbf{45}), (\mathbf{23})(\mathbf{01})\}$ and $\text{Dis}(Y) \cap \langle \sigma_0 \rangle = \{\text{id}\}$ with $|\text{Dis}(Y)_0| = 2$. But the solution (Y, σ, τ) is not isomorphic to a solution $\mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$ for any $(G, +, 0)$, n and \mathbf{c} . Indeed, by Proposition 4.2, such a group $(G, +, 0)$ would be a two-element group and, by Proposition 4.5, n would be equal to 6 and we would obtain a 12-element solution.

Example 5.10. By Proposition 5.2, the solution $(\mathbb{Z}_{2^m}, \sigma, \tau)$ from Example 2.4 Case 1 is isomorphic to the solution $\mathcal{S}(2\mathbb{Z}_{2^m} \times \mathbb{Z}_2, \mathbf{c} = (0, -2))$. The isomorphism $\Phi: 2\mathbb{Z}_{2^m} \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_{2^m}$ is given by $(s, 0) \mapsto s$ and $(s, 1) \mapsto s + 1$, and clearly $\ker \Phi = \theta(2, \{0\}, 0)$.

On the other hand, the solution $(\mathbb{Z}_{2^m}, \sigma, \tau)$ from Case 2 is the homomorphic image of the solution $\mathcal{S}(2\mathbb{Z}_{2^m} \times \mathbb{Z}_4, \mathbf{c} = (0, 2^{m-1} - 2, 0, 2^{m-1} - 2))$. The homomorphism $\Phi: 2\mathbb{Z}_{2^m} \times \mathbb{Z}_4 \rightarrow \mathbb{Z}_{2^m}$ is given by $(s, 0) \mapsto s$, $(s, 1) \mapsto s + 1 + 2^{m-1}$, $(s, 2) \mapsto s + 2^{m-1}$ and $(s, 3) \mapsto s + 1$. In this case, $\ker \Phi = \theta(2, \{0\}, 2^{m-1})$.

By Proposition 5.8, for each indecomposable solution of multipermutation level 2 there are a solution $(X, \sigma, \tau) = \mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$, a subgroup H of the group $(G, +, 0)$, a number m , an element $r \in G$ and a congruence $\theta = \theta(m, H, r)$ determined by (5.5) such that the solution is isomorphic to the quotient solution of $\mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$ by the relation θ . Hence, each indecomposable solution of multipermutation level 2 is of the form $(X, \sigma, \tau)/\theta = (X/\theta, {}^\theta\sigma, {}^\theta\tau)$.

Let $Y = X/\theta$. Clearly, for each $y \in Y$, there is $(a, i) \in G \times \mathbb{Z}_n$ such that $y = (a, i)/\theta$. In particular, for $y_1 = (a_1, i_1)/\theta$ and $y_2 = (a_2, i_2)/\theta \in Y$, the equality $y_1 = y_2$ implies $i_1 - i_2 \equiv 0 \pmod{m}$ and, for $i \in \mathbb{N}$, the element $\tilde{i} \in Y$ corresponds to the congruence class $\pi^i(\tilde{0})/\theta = (0, i)/\theta$.

In the sequel (until Proposition 5.18) we suppose the following situation: we have (Y, ρ, v) , an indecomposable solution of multipermutation level 2 and we know, according to Propositions 5.1 and 5.2, that there exist a solution $(X, \sigma, \tau) = \mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$ and a congruence $\theta = \theta(m, H, r)$ such that $(Y, \rho, v) \cong (X/\theta, {}^\theta\sigma, {}^\theta\tau)$.

As the first application of the characterization of congruences of a solution $\mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$ we prove the analogy of Proposition 4.5 for all indecomposable solutions.

Proposition 5.11. *Let (Y, ρ, v) be a finite indecomposable solution of multipermutation level 2. Each permutation ρ_y , for $y \in Y$, is composed of cycles of length ℓ .*

Proof. We shall prove that $\ell = km$, where k is the smallest positive integer such that $k \cdot r \in H$.

Let $(a, i), (b, j) \in G \times \mathbb{Z}_n$ and we shall compute the smallest ℓ such that $\sigma_{(a,i)}^\ell((b, j))/\theta = (b, j)/\theta$. By (4.2), we have

$$\sigma_{(a,i)}^\ell((b, j)) = (b + \sum_{j'=1}^{\ell} (c_{i-j-j'} - c_{-j-j'}), j + \ell)$$

and therefore $m \mid \ell$. Moreover, since $c_{i'} - c_{i'+\ell} \in H$, for each i' , this implies that there exists $h \in H$ such that $\sum_{j'=1}^{\ell} c_{i-j-j'} - c_{-j-j'} = h$. Now from $\sigma_{(a,i)}^\ell((b, j))/\theta = (b, j)/\theta$ we obtain

$$b + h - b + \frac{j-j-\ell}{m} \cdot r \in H$$

which is equivalent to $\frac{\ell}{m} \cdot r \in H$. \square

In the sequel we shall show several properties of the image determined by the parameters of the congruence.

Proposition 5.12. *Let (Y, ρ, v) be an indecomposable solution of multipermutation level 2 and $e \in Y$. Then $\text{Dis}(Y)/\text{Dis}(Y)_e \cong G/H$.*

Proof. We can suppose, without loss of generality, that $e = (0, 0)/\theta$. Clearly, each permutation $\delta \in \mathcal{G}(X)$ induces the permutation ${}^\theta\delta \in \mathcal{G}(Y)$. In particular, ${}^\theta L_{(a,i)/\theta}((b, j)/\theta) = L_{(a,i)}((b, j))/\theta$ and, for each $\gamma \in \text{Dis}(X)_{(0,0)}$, ${}^\theta\gamma(e) = {}^\theta\gamma((0, 0)/\theta) = \gamma((0, 0))/\theta = (0, 0)/\theta = e$. Hence, the mapping $\gamma \mapsto {}^\theta\gamma$ is a well defined homomorphism from $\text{Dis}(X)/\text{Dis}(X)_{(0,0)}$ onto $\text{Dis}(Y)/\text{Dis}(Y)_e$.

By Remark 4.2 we know that $\Psi: \text{Dis}(X) \rightarrow G$ defined by $\prod L_{(0,i)}^{p_i} \mapsto \sum p_i \cdot c_i$ is a well-defined epimorphism with $\text{Ker } \Psi = \text{Dis}(X)_{(0,0)}$ and $G \cong \text{Dis}(X)/\text{Dis}(X)_{(0,0)}$. Hence there exists a homomorphism Φ from $(G, +, 0)$ onto $\text{Dis}(Y)/\text{Dis}(Y)_e$. Let us now compute $\text{Ker } \Phi$. An element $\prod {}^\theta L_{(a_k, i_k)/\theta}^{p_k}$ lies in $\text{Dis}(Y)_e$ if and only if $\prod L_{(a_k, i_k)}^{p_k}((0, 0)) = (h, 0)$, for some $h \in H$. Since $\prod L_{(a_k, i_k)}^{p_k}((0, 0)) = (\sum p_k \cdot c_{i_k}, 0)$, this is equivalent to $\sum p_k \cdot c_{i_k} \in H$ and therefore also to $\Psi(\prod L_{(a_k, i_k)}^{p_k}) \in H$. Hence $\text{Ker } \Phi = H$, which finishes the proof. \square

Lemma 5.13. *Let $(G, \cdot, 1)$ be a group that acts on a set X . Then $\langle \bigcup G_x \rangle$ is a normal subgroup of $(G, \cdot, 1)$.*

Proof. Let $g \in G_x$, for some $x \in X$, and let $h \in G$. Then $hgh^{-1}(h(x)) = hg(x) = h(x)$ and therefore $hgh^{-1} \in G_{h(x)}$. \square

Lemma 5.14. *Let (Y, ρ, v) be an indecomposable solution of multipermutation level 2 and let $e \in Y$. Then $\mathcal{G}(Y)_e \text{Dis}(Y) = \langle \bigcup \mathcal{G}(Y)_y \rangle \text{Dis}(Y)$ and it is a normal subgroup of $\mathcal{G}(Y)$.*

Proof. Let $\alpha \in \mathcal{G}(Y)_y$, for some $y \in Y$. Let $\beta \in \mathcal{G}(Y)$ send e to y . Then $\beta^{-1}\alpha\beta \in \mathcal{G}(Y)_e$ and $\alpha = \beta^{-1}\alpha\beta[\beta, \alpha] \in \mathcal{G}(Y)_e \text{Dis}(Y)$. Hence $\bigcup \mathcal{G}(Y)_y \subseteq \mathcal{G}(Y)_e \text{Dis}(Y)$.

Now $\langle \bigcup \mathcal{G}(Y)_y \rangle \text{Dis}(Y)$ is normal since it is a product of two normal subgroups. \square

Proposition 5.15. *Let (Y, ρ, v) be an indecomposable solution of multipermutation level 2 and let $e \in Y$. Then $\mathcal{G}(Y)/(\mathcal{G}(Y)_e \text{Dis}(Y)) \cong \mathbb{Z}_m$.*

Proof. Let $\Phi: X \rightarrow Y$ be the natural projection from (X, σ, τ) onto (Y, ρ, v) . This homomorphism induces the onto group homomorphism $\Phi_{\mathcal{G}}: \mathcal{G}(X) \rightarrow \mathcal{G}(Y)$ with $\Phi_{\mathcal{G}}(\nu)(x/\theta) = \nu(x)/\theta$, for $\nu \in \mathcal{G}(X)$. Further, let Ψ be the natural projection from the group $\mathcal{G}(Y)$ onto $\mathcal{G}(Y)/(\langle \bigcup \mathcal{G}(Y)_y \rangle \text{Dis}(Y))$. This means that $\text{Ker } \Psi = \langle \bigcup \mathcal{G}(Y)_y \rangle \text{Dis}(Y)$ and $\mathcal{G}(Y)/\text{Ker } \Psi \cong \mathcal{G}(X)/\Phi_{\mathcal{G}}^{-1}[\text{Ker } \Psi]$.

Recall that m is the smallest positive integer such that there exists $a \in G$ with $(0, 0)/\theta = (a, m)/\theta$. Clearly, $\Phi_{\mathcal{G}}(\text{Dis}(X)) \subseteq \text{Ker } \Psi$. Now let $\gamma \in \text{Dis}(X)$ be such that $\gamma((0, m)) = (a, m)$. We then know that $\Phi_{\mathcal{G}}(\gamma\pi^m) \in \mathcal{G}(Y)_{\Phi((0, 0))}$. Hence $\Phi_{\mathcal{G}}(\gamma\pi^m) \in \text{Ker } \Psi$ and therefore $\text{Dis}(X)\langle \pi^m \rangle \subseteq \Phi_{\mathcal{G}}^{-1}[\text{Ker } \Psi]$. On the other hand, let $\gamma\pi^k \in \mathcal{G}(X)$ and $\Phi_{\mathcal{G}}(\gamma\pi^k) \in \mathcal{G}_{\Phi((0, 0))}$. Hence $(0, 0)/\theta = \Phi((0, 0)) = \Phi_{\mathcal{G}}(\gamma\pi^k)(\Phi((0, 0))) = \Phi(\gamma\pi^k((0, 0))) = \gamma\pi^k((0, 0))/\theta = \gamma((0, k))/\theta$. So, $(0, 0)/\theta = \gamma((0, k))/\theta$ and $m|k$. Therefore, $\pi^k \in \langle \pi^m \rangle$ which implies $\Phi_{\mathcal{G}}^{-1}[\text{Ker } \Psi] \subseteq \text{Dis}(X)\langle \pi^m \rangle$.

Finally, $\mathcal{G}(Y)/\text{Ker } \Psi \cong \mathcal{G}(X)/\Phi_{\mathcal{G}}^{-1}[\text{Ker } \Psi] = \text{Dis}(X)\langle \pi \rangle / \text{Dis}(X)\langle \pi^m \rangle = \langle \pi \rangle / \langle \pi^m \rangle \cong \mathbb{Z}_m$. \square

Corollary 5.16. *Let (Y, ρ, v) be an indecomposable solution of multipermutation level 2. Then $|Y| = m \cdot [G : H]$.*

Proof. Choose $e \in Y$ and

$$|Y| = [\mathcal{G}(Y) : \mathcal{G}(Y)_e] = [\mathcal{G}(Y) : \mathcal{G}(Y)_e \text{Dis}(Y)] \cdot [\mathcal{G}(Y)_e \text{Dis}(Y) : \mathcal{G}(Y)_e] = [\mathcal{G}(Y) : \mathcal{G}(Y)_e \text{Dis}(Y)] \cdot [\text{Dis}(Y) : \text{Dis}(Y)_e] = m \cdot [G : H]. \quad \square$$

Lemma 5.17. *Let (Y, ρ, v) be an indecomposable solution of multipermutation level 2. For each $x, y \in Y$, $\rho_x^m = \rho_y^m$.*

Proof. By Proposition 5.8, for each $i \in \mathbb{Z}_n$, there exists some $h \in H$, such that, for $(a, i), (b, j) \in G \times \mathbb{Z}_n$,

$$\sigma_{(a, i)}^m((b, j)) = (b + \sum_{\ell=1}^m (c_{i-j-\ell} - c_{-j-\ell}), j + m) = (b + h, j + m).$$

Since $\sigma_{(0, 0)}^m((b, j)) = (b, j + m)$, by (5.5) we have that $\sigma_{(a, i)}^m((b, j))/\theta = \sigma_{(0, 0)}^m((b, j))/\theta$, which means that, for all $y \in Y$, $\rho_y^m = \rho_{(a, i)/\theta}^m = \rho_{(0, 0)/\theta}^m$. \square

Proposition 5.18. *Let (Y, ρ, v) be an indecomposable solution of multipermutation level 2. The automorphism group $\text{Aut}(Y)$ is regular.*

Proof. Let $\gamma \in \text{Dis}(Y)$, $\pi = \rho_{(0, 0)/\theta}$ and $k \in \mathbb{N}$. For each $i \in \mathbb{N}$ and $\alpha \in \text{Dis}(Y)$, let

$$\Phi(\alpha(\tilde{i})) = \rho_k^i \pi^{k-i} \alpha \pi^{i-k} \gamma(\tilde{k}).$$

We want to show that Φ is an automorphism of the solution (Y, ρ, v) but first we have to show that Φ is well defined since each element $\alpha(\tilde{i})$ may admit several representations. Let $\alpha, \alpha' \in \text{Dis}(Y)$ and $i, i' \in \mathbb{N}$. First note that $\pi^{k-i} \alpha \pi^{i-k} \gamma \in \text{Dis}(Y)$. Further, if $i - i' = m\ell$, for some $\ell \in \mathbb{N}$, then by Lemma 5.17 we have

$$\begin{aligned} \alpha(\tilde{i}) = \alpha'(\tilde{i}') &\Leftrightarrow \alpha \pi^{i-k}(\tilde{k}) = \alpha' \pi^{i'-k}(\tilde{k}) \Leftrightarrow \gamma \pi^{k-i} \alpha \pi^{i-k}(\tilde{k}) = \gamma \pi^{-m\ell} \pi^{k-i'} \alpha' \pi^{i'-k}(\tilde{k}) \Leftrightarrow \\ \rho_k^i \pi^{k-i} \alpha \pi^{i-k} \gamma(\tilde{k}) &= \rho_k^i \rho_k^{-m\ell} \pi^{k-i'} \alpha' \pi^{i'-k} \gamma(\tilde{k}) \Leftrightarrow \rho_k^i \pi^{k-i} \alpha \pi^{i-k} \gamma(\tilde{k}) = \rho_k^{i'} \pi^{k-i'} \alpha' \pi^{i'-k} \gamma(\tilde{k}) \Leftrightarrow \\ &\Phi(\alpha(\tilde{i})) = \Phi(\alpha'(\tilde{i}')). \end{aligned}$$

Hence, the mapping Φ is well-defined since $\alpha(\tilde{i}) = \alpha'(\tilde{i}')$ implies $m \mid (i - i')$. Conversely, necessarily $\rho_k^i \pi^{k-i} \alpha \pi^{i-k} \gamma(\tilde{k}) = \rho_k^{i'} \pi^{k-i'} \alpha' \pi^{i'-k} \gamma(\tilde{k})$ implies $m \mid (i - i')$, and therefore Φ is injective.

Moreover, $\Phi(\tilde{0}) = \gamma(\tilde{k})$ and Φ is clearly onto. We shall now prove that it is endomorphism of the solution. Note that $\rho_k^i \gamma \pi^{k-i} \alpha \pi^{-k} = \rho_k^i \pi^{-i} \pi^k \alpha \pi^{-k} \gamma \in \text{Dis}(Y)$. This implies, for $\beta \in \text{Dis}(Y)$,

$$\begin{aligned}
\Phi(\rho_{\alpha(\tilde{i})}(\beta(\tilde{j}))) &\stackrel{(3.11)}{=} \Phi(L_{\tilde{i}} \pi \beta(\tilde{j})) = \Phi(L_{\tilde{i}} \pi \beta \pi^{-1}(\tilde{j}+1)) \\
&= \rho_k^{j+1} \pi^{k-j-1} L_{\tilde{i}} \pi \beta \pi^{-1} \pi^{1+j-k} \gamma(\tilde{k}) \stackrel{(3.8)}{=} \rho_k^{j+1} L_{k-j-1}^{-1} L_{i+k-j-1} \pi^{k-j-1} \pi \beta \pi^{j-k} \gamma(\tilde{k}) \\
&\stackrel{(3.8)}{=} L_{\tilde{k}}^{-1} L_{i+k} \rho_k^{j+1} \pi^{k-j} \beta \pi^{j-k} \gamma(\tilde{k}) = L_{i+k} \pi \rho_k^j \pi^{k-j} \beta \pi^{j-k} \gamma(\tilde{k}) \\
&= \rho_{i+k} \Phi(\beta(\tilde{j})) \stackrel{(3.11)}{=} \rho_{\rho_k^i \pi^{k-i} \alpha \pi^{-k} \gamma(\tilde{k})} \Phi(\beta(\tilde{j})) = \rho_{\Phi(\alpha(\tilde{i}))} \Phi(\beta(\tilde{j}))
\end{aligned}$$

and hence $\text{Aut}(Y)$ is transitive. And, according to Corollary 3.11, $\text{Aut}(Y)$ is semi-regular. \square

Theorem 5.19. *Let $(X, \sigma, \tau) = \mathcal{S}(G \times \mathbb{Z}_n, \mathbf{c})$. Let $\theta_1 = \theta(m_1, H_1, r_1)$ and $\theta_2 = \theta(m_2, H_2, r_2)$. Then the solutions $(X, \sigma, \tau)/\theta_1$ and $(X, \sigma, \tau)/\theta_2$ are isomorphic if and only if $m_1 = m_2$, $H_1 = H_2$ and $r_1 \equiv r_2 \pmod{H_2}$.*

Proof. “ \Rightarrow ” Suppose that there is an isomorphism $\Phi : X/\theta_1 \rightarrow X/\theta_2$. Clearly $m_1 = m_2$, according to Proposition 5.12. According to Proposition 5.18, we can suppose, without loss of generality $\Phi((0, 0)/\theta_1) = (0, 0)/\theta_2$. Since $\sigma_{(0,0)}^i((0, 0)) = (0, i)$, necessarily $\Phi((0, i)/\theta_1) = (0, i)/\theta_2$, for each $i \in \mathbb{Z}$. Now, for each $a \in G$ and $i \in \mathbb{Z}_n$, there exist $j_1, \dots, j_k \in \mathbb{Z}_n$ and $p_1, \dots, p_k \in \mathbb{Z}$ such that

$$(a, i) = \prod L_{(0, j_\ell)}^{p_\ell}((0, i)) = \prod (\sigma_{(0, j_\ell)} \sigma_{(0,0)}^{-1})^{p_\ell}((0, i))$$

and therefore $\Phi((a, i)/\theta_1) = (a, i)/\theta_2$.

Suppose $h \in H_1$. Then by (5.5), $(h, 0)/\theta_2 = \Phi((h, 0)/\theta_1) = \Phi((0, 0)/\theta_1) = (0, 0)/\theta_2$ and therefore $h \in H_2$ and $H_1 \subseteq H_2$. Analogously $H_2 \subseteq H_1$. Now, once again by (5.5)

$$(r_2, m_2)/\theta_2 = (0, 0)/\theta_2 = \Phi((0, 0)/\theta_1) = \Phi((r_1, m_2)/\theta_1) = (r_1, m_2)/\theta_2,$$

which implies $r_1 \equiv r_2 \pmod{H_2}$.

“ \Leftarrow ” If $m_1 = m_2$, $H_1 = H_2$ and $r_1 \equiv r_2 \pmod{H_2}$ then $\theta_1 = \theta_2$. \square

6. ENUMERATION

We have now a theoretic means of constructing all indecomposable solutions of multipermutation level 2 and we shall explicitly do so in some particular cases. Every such solution is a homomorphic image of the solution $\mathcal{S}((\bigoplus_{\mathbb{Z}} \mathbb{Z}) \times \mathbb{Z}, \mathbf{c})$ from Proposition 5.1. To construct all of them we have to find all congruences $\theta(m, H, r)$ of the solution. Then, according to Theorem 5.19, different congruences give non-isomorphic solutions. If m is finite and H is a subgroup of $(G, +, 0) = \bigoplus_{\mathbb{Z}} \mathbb{Z}$ then, by Proposition 5.8 (iii),

$$0 = c_0 \equiv c_m = \sum_{i=1}^m e_i \pmod{H}$$

and also, for each $i \in \mathbb{Z}$, $e_{i+m} = c_{i+m} - c_{i+m-1} \equiv c_i - c_{i-1} = e_i \pmod{H}$. In particular, the group G/H has at most $m-1$ generators.

If we want to construct all finite n -element indecomposable solutions of multipermutation level 2 necessarily, by Corollary 5.16, we have to consider all m which divide n . Moreover we know $[G : H] = \frac{n}{m}$.

If $m = 1$ then G/H has 0 generators and hence $G = H$. Another trivial case is $m = n$; then $G = H$ and $\mathcal{S}((\bigoplus_{\mathbb{Z}} \mathbb{Z}) \times \mathbb{Z}, \mathbf{c})/\theta(m, G, 0)$ is a permutation solution.

If $m = 2$ then G/H has to be cyclic and there is only one choice of such H . Nevertheless, there are $[G : H]$ choices of r (one for each coset of H) and hence there are $[G : H]$ non-isomorphic solutions.

Another easy to calculate case is the case when G/H is essentially a vector space. For this situation, let us recall that, given a vector space V of dimension n over a field \mathbb{F}_q , the number of all subspaces of V of dimension $0 < k \leq n$ is equal to

$$(6.1) \quad \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})} = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}.$$

Proposition 6.1. *Let p be a prime number, $(A, +, 0)$ be an elementary abelian group of order p^k and let $m \in \mathbb{N}$. Then the number $\mathbf{n}(A, m)$ of indecomposable solutions (X, σ, τ) of multipermutation level 2 such that $\text{Dis}(X)/\text{Dis}(X)_e \cong A$ and $[\mathcal{G}(X) : \mathcal{G}(X)_e \text{Dis}(X)] = m$ is*

$$\mathbf{n}(A, m) = \begin{cases} p^k \cdot \frac{(p^{m-1}-1)(p^{m-2}-1) \cdots (p^{k+1}-1)}{(p^{m-k-1}-1)(p^{m-k-2}-1) \cdots (p-1)} & \text{if } m > k+1, \\ p^k & \text{if } m = k+1, \\ 0 & \text{if } m \leq k. \end{cases}$$

Proof. Every indecomposable solution (X, σ, τ) of multipermutation level 2 can be obtained as a quotient of the solution $\mathcal{S}(G, \mathbf{c})$ with $G = (\bigoplus_{\mathbb{Z}} \mathbb{Z}) \times \mathbb{Z}$ via a congruence $\theta(m, H, r)$, for some subgroup H with $G/H \cong A$ and $r \in G$. According to Theorem 5.19, different choices of H and r (mod H) yield non-isomorphic solutions. Let us count the number of such choices of H .

According to Proposition 5.8, $\sum_{i=1}^m e^i \in H$ and also $e_{i+m} - e_i \in H$, for each $i \in \mathbb{Z}$. Let now

$$N = \left\langle \sum_{i=1}^m e^i, e_{i+m} - e_i, p \cdot e_i \mid i \in \mathbb{Z} \right\rangle.$$

Clearly, G/N is an elementary abelian group of order p^{m-1} and $N \leq H$. If we treat G/N as a vector space over \mathbb{F}_p of dimension $m-1$ then H/N is a subspace of dimension $m-1-k$. According to (6.1), for $k < m-1$, there are

$$\frac{(p^{m-1}-1)(p^{m-2}-1) \cdots (p^{k+1}-1)}{(p^{m-k-1}-1)(p^{m-k-2}-1) \cdots (p-1)}$$

such choices of H/N and therefore as many choices of H . If $k = m-1$ there is exactly 1 subspace of dimension 0. If $k > m-1$ then there is no such subspace.

Now, for each choice of H , there are p^k cosets of H and therefore there are p^k choices of r . \square

Remark 6.2. For $k = 1$, the expression for the number $\mathbf{n}(A, m)$ simplifies to $\frac{p^m - p}{p - 1}$.

Remark 6.3. By Proposition 6.1 there are exactly $1 + \frac{p^p - p}{p - 1}$ indecomposable solutions of multipermutation level 2 of order p^2 , for a prime p . Exactly p^{p-1} of them are composed of cycles of length p^2 . For example, there are 13 indecomposable solutions of multipermutation level 2 of order 9 and 9 of them are cycles of length 9.

Let $2 < p < q$ be two different primes. There are $1 + \frac{p^q - p}{p - 1} + \frac{q^p - q}{q - 1}$ indecomposable solutions of multipermutation level 2 of order pq . For example, there are 151 indecomposable solutions of multipermutation level 2 of order 15. Or, another example, there are $2^p + p - 1$ indecomposable solutions of multipermutation level 2 of order $2p > 4$.

Since the work of Etingof, Schedler and Soloviev [10] the researchers ask themselves a question about the proportion of the numbers of the indecomposable solutions with respect to the decomposable ones. And it was conjectured by Vendramin that the limit towards infinity of the ratio

indecomposables/decomposables goes to 0. The result of Blackburn [3] about the numbers of racks can be easily adapted to solutions and therefore we know that there are at least $2^{O(n^2)}$ decomposable solutions for each size n . Now it turns out that there are exponentially many indecomposable solutions as well.

Corollary 6.4. *Let $s \in \mathbb{N}$. Then there are at least $2^{n/2} - 1$ indecomposable solutions of size $n = 2^s$.*

Proof. For $s = 1$ there exists exactly one solution, namely the permutation one. Hence suppose $s > 1$. According to Proposition 6.1 and Remark 6.2, there are $2^{2^{s-1}} - 2$ solutions of size 2^s with $m = 2^{s-1}$. Plus there is one solution with $m = 2^s$. \square

Regardless of the exponential growth, still $2^{O(n)} \ll 2^{O(n^2)}$. Of course, we have a lower bound for the number of indecomposables only but the experience from other types of algebraic structures suggests that the upper bound might be similar.

Conjecture 6.5. *There is a constant $c \in \mathbb{Q}^+$ such that the number of indecomposable solutions of size n is less than 2^{cn} , for each $n \in \mathbb{N}$.*

Proposition 6.1 may be generalized to the case when A is a free \mathbb{Z}_t -module, for some number t . However, the expression would be too complicated and hence we give a special case only, namely with a group $(A, +, 0)$ cyclic of size p^k .

Proposition 6.6. *Let p be a prime number, let $(A, +, 0)$ be a cyclic group of order p^k and let $m > 1$. Then the number $\mathbf{n}(A, m)$ of indecomposable solutions (X, σ, τ) of multipermutation level 2 such that $\text{Dis}(X)/\text{Dis}(X)_e \cong A$ and $[\mathcal{G}(X) : \mathcal{G}(X)_e \text{Dis}(X)] = m$ is*

$$\mathbf{n}(A, m) = p^{km-m-k+2} \cdot \frac{p^{m-1} - 1}{p - 1}.$$

Proof. The proof is the same as for Proposition 6.1, with the exception that N is a free \mathbb{Z}_{p^k} -module of rank $m - 1$ and we count the number of its hyperplanes (free submodules of rank $m - 2$). It is well known that each hyperplane corresponds to a line in the dual free module and hence the number of hyperplanes is equal to the number of lines. Each line is generated by a vector with at least one coordinate invertible. There are $(p^k)^{m-1} - (p^{k-1})^{m-1}$ such vectors. There are $p^k - p^{k-1}$ multiples of the vector that generate the same submodule. Hence there are $\frac{(p^k)^{m-1} - (p^{k-1})^{m-1}}{p^k - p^{k-1}}$ choices of H . For each such H , there are p^k choices of r . \square

Example 6.7. Let us compute the number of all indecomposable solutions of multipermutation level 2 of size 16:

- 8 solutions with $m = 2$ and $G/H \cong \mathbb{Z}_8$,
- 112 solutions with $m = 4$ and $G/H \cong \mathbb{Z}_4$,
- 28 solutions with $m = 4$ and $G/H \cong \mathbb{Z}_2^2$,
- 254 solutions with $m = 8$ and $G/H \cong \mathbb{Z}_2$,
- 1 solution with $m = 16$ and $G/H \cong \mathbb{Z}_1$.

Analogously, just using the ideas from the beginning of the section and Propositions 6.1 and 6.6, we are able to compute the numbers of indecomposable solutions of multipermutation level 2 up to the size of 17. We can also compare our numbers with the results from [1] (the numbers from the first three rows of Table 1).

Well known results of Etingof, Schedler, Soloviev [10] and Etingof, Guralnick, Soloviev [11] say that indecomposable solutions of prime cardinality are affine and have cyclic permutation group. Smoktunowicz and Smoktunowicz investigated in [26] whether an analogous characterization for indecomposable solutions of arbitrary cardinality also exists and they concluded that with high

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
solutions	1	2	5	23	88	595	3456	34530	321931	4895272						
2-permut.	1	2	5	19	70	359	2095	16332								
indecom.	1	1	1	5	1	10	1	100	16	36	1		1			
2-permut. ind.	1	1	1	3	1	10	1	19	13	36	1	136	1	134	151	403
2-per. ind. abel.	1	1	1	3	1	1	1	3	4	1	1	3	1	1	1	7
2-per. ind. cycl.	1	1	1	2	1	1	1	2	3	1	1	2	1	1	1	4

TABLE 1. The number of 2-permutational indecomposable solutions of size n , up to isomorphism.

probability to obtain similar results are not possible. But perhaps not all is lost and some analogies may be achieved.

In [5, Proposition 6.1] Castelli showed that each unconnected solution of square-free odd order is always of multipermutation level at most 2. On the other hand by Example 5.9 there is 2-permutational indecomposable solution of size 6 which is not unconnected. According to Table 1 the following natural question arises:

Question 6.8. *Is it true that each indecomposable solution of square-free order is always of multipermutation level at most 2?*

REFERENCES

- [1] Ö. Agkün, M. Mereb, L. Vendramin, *Enumeration of set-theoretic solutions to the Yang-Baxter equation*, Math. Comp. **91** (2022), 1469–1481.
- [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] S. Blackburn, *Enumerating finite racks, quandles and kei*, Electron. J. Combin. **20** (2013), no. 3, Paper 43, 9 pp.
- [4] M. Castelli, F. Catino, G. Pinto, *Indecomposable involutive set-theoretic solutions of the Yang-Baxter equation*, J. Pure Appl. Algebra **223** (2019), 4477–4493.
- [5] M. Castelli, *The construction of unconnected involutive solutions of the Yang-Baxter equation of multipermutation level 2 with odd size and a Z-group permutation group*, available at <http://arxiv.org/abs/2110.01912>
- [6] F. Cedó, T. Gateva-Ivanova, A. Smoktunowicz, *On the Yang-Baxter equation and left nilpotent left braces*, J. Pure Appl. Algebra **221** (2017), 751–756.
- [7] F. Cedó, E. Jespers, J. Okniński, *Braces and the Yang-Baxter equation*, Comm. Math. Phys. **327** (2014), 101–116. Extended version arXiv:1205.3587.
- [8] F. Cedó, J. Okniński, *Constructing finite simple solutions of the Yang-Baxter equation*, Adv. in Math. **391** (2021), 107968.
- [9] V.G. Drinfeld, *On some unsolved problems in quantum group theory*, In: P.P. Kulish (ed.) Quantum groups, in: Lecture Notes in Math., vol. 1510, Springer-Verlag, Berlin, (1992), pp. 1–8.
- [10] P. Etingof, T. Schedler, A. Soloviev, *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. **100** (1999), 169–209.
- [11] P. Etingof, R. Guralnick, A. Soloviev, *Indecomposable set-theoretical solutions to the quantum Yang-Baxter equation on a set with a prime number of elements*, J. Algebra, **249** (2001), 709–719.
- [12] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.11.1; 2021. Available at <http://www.gap-system.org>
- [13] T. Gateva-Ivanova, *Set-theoretic solutions of the Yang-Baxter equation, braces and symmetric groups*, Adv. in Math. **338** (2018), 649–701.
- [14] T. Gateva-Ivanova, S. Majid, *Quantum spaces associated to multipermutation solutions of level two*, Algebr. Represent. Theory **14** (2011), 341–376.
- [15] T. Gateva-Ivanova, P. Cameron, *Multipermutation solutions of the Yang-Baxter equation*, Comm. Math. Phys. **309** (2012), 583–621.
- [16] A. Hulpke, D. Stanovský, P. Vojtěchovský, *Connected quandles and transitive groups*, J. Pure Appl. Algebra **220** (2016), 735–758.

- [17] P. Jedlička, A. Pilitowska, A. Zamojska-Dzienio, *The construction of multipermutation solutions of the Yang-Baxter equation of level 2*, J. Comb. Theory Ser. A. **176** (2020), 1–35.
- [18] 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. **33**(5) 2021, 1083–1096.
- [19] P. Jedlička, A. Pilitowska, A. Zamojska-Dzienio, *Cocyclic braces and indecomposable cocyclic solutions of the Yang-Baxter equation*, to appear in Proc. Amer. Math. Soc. (2022).
- [20] M. Jimbo, *Introduction to the Yang-Baxter equation*, Int. J. Modern Physics A, **4-15** (1989), 3759–3777.
- [21] D. Joyce, *Classifying invariant of knots, the knot quandle*, J. Pure Applied Algebra, **23** (1982), 37–65.
- [22] C. Kassel, *Quantum groups*, Springer-Verlag, 2012.
- [23] W. Rump, *A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation*, Adv. Math. **193** (2005), 40–55.
- [24] W. Rump, *Braces, radical rings, and the quantum Yang-Baxter equation*, J. Algebra **307** (2007), 153–170.
- [25] W. Rump, *Classification of indecomposable involutive set-theoretic solutions to the Yang-Baxter equation*, Forum Math. **32**(4) (2020), 891–903.
- [26] A. Smoktunowicz, A. Smoktunowicz, *Set-theoretic solutions to the Yang-Baxter equation and new classes of R-matrices*, Linear Algebra Appl. **546** (2018), 86–114.

(P.J.) DEPARTMENT OF MATHEMATICS, FACULTY OF ENGINEERING, CZECH UNIVERSITY OF LIFE SCIENCES, KAMÝČKÁ 129, 16521 PRAHA 6, CZECH REPUBLIC

(A.P.) FACULTY OF MATHEMATICS AND INFORMATION SCIENCE, WARSAW UNIVERSITY OF TECHNOLOGY, KOSZYKOWA 75, 00-662 WARSAW, POLAND

Email address: (P.J.) jedlickap@tf.czu.cz

Email address: (A.P.) agata.pilitowska@pw.edu.pl