INDECOMPOSABILITY AND IRREDUCIBILITY OF MONOMIAL REPRESENTATIONS FOR SET-THEORETICAL SOLUTIONS TO THE YANG–BAXTER EQUATION

CARSTEN DIETZEL, EDOUARD FEINGESICHT, SILVIA PROPERZI

Abstract. This article investigates Dehornoy's monomial representations for structure groups and Coxeter-like groups of a set-theoretic solution to the Yang-Baxter equation. Using the brace structure of these two groups and the language of cycle sets, we relate the irreducibility of monomial representations to the indecomposability of the solutions. Furthermore, in the case of an indecomposable solution, we show how to obtain these representations by induction from explicit one-dimensional representations.

1. Introduction

In 1992, Drinfeld [7] proposed to classify set-theoretical solutions of the Yang–Baxter equation, that is, couples (X, r) where X is a set and $r\colon X^2 \to X^2$ is a bijective map satisfying the Yang–Baxter equation $r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23}$. Here r_{ij} denotes r acting on the i-th and j-th coordinate of X^3. In their seminal paper [8], Etingof, Schedler and Soloviev associated with a solution a structure group $G(X, r)$ and studied many of its properties in the particular case where r is involutive, i.e. $r^2 = \mathrm{id}_{X^2}$, and non-degenerate, meaning that when writing $r(x, y) = (\lambda_x(y), \rho_y(x))$ the maps λ_x and ρ_y are bijective for all $x, y \in X$. In this case, $G(X, r)$ was proven to be a Garside group by Chouraqui [3]. Later, a Garside germ, that is, a finite quotient that can recover the Garside structure, was constructed by Dehornoy [6].

The current approach to study solutions is by adding an extra structure to the structure group, making it a brace, following the work of Rump [11, 12]. In this work, we use brace-theoretic machinery to gain a better understanding of monomial representations associated with set-theoretic solutions.

In Section 3, we relate the indecomposability of a solution with the irreducibility of the monomial representations defined by Dehornoy [6]:

Theorem. *Let (X, r) be an involutive non-degenerate solution of the Yang–Baxter equation of Dehornoy class d. Then the following are equivalent:*

(1) (X, r) is indecomposable.

(2) The monomial representation Θ of the structure group G is irreducible.

If moreover $l > 1$ or $d > 2$, then the previous conditions are also equivalent to

(3) The monomial representation $\overline{\Theta}_l$ of $\overline{G}_l = G/ldG$ is irreducible.

Furthermore, when $d = 2$, we give a sufficient numerical condition for the irreducibility of $\overline{\Theta}_1$.

In Section 4, we then show that the representations constructed from an indecomposable solution are induced from characters of the subgroup $\mathrm{Stab}(x_0)$, for $x_0 \in X$. More precisely Θ is induced by the character $\sum_{x\in X} g_x x \mapsto q^{g_{x_0}}$ and $\overline{\Theta}_l$ by the the character $\sum_{x\in X} g_x x \mapsto \exp\left(g_{x_0} \cdot \frac{2i\pi}{ld}\right)$.

Date: September 30, 2024.

2. Preliminaries

2.1. **Braces.** Rump introduced braces in [12] as a generalization of radical rings in order to study cycle sets. A *brace*, as reformulated in [2], is a triple $(B,+,\circ)$, where $(B,+)$ is an abelian group and $(B,\circ)$ is a group such that

$$a\circ(b+c)=a\circ b-a+a\circ c,$$

for all $a,b,c\in B$, where $-a$ denotes the inverse of a in $(B,+)$. More generally, for $n\in\mathbb{Z}$ and $a\in B$, we will denote by na the n-th power of a in $(B,+)$ and by a^n the n-th power of a in $(C,\circ)$.

If B is a brace, then the *multiplicative group* $(C,\circ)$ acts by automorphisms on the *additive group* $(B,+)$ via the λ-action, defined as

$$\lambda_a(b)=-a+a\circ b.$$

Example 2.1. If $(G,+)$ is an abelian group, then $\mathrm{Triv}(G)=(G,+,+)$ is a brace, called the *trivial brace* on G. It is easily seen that trivial braces are characterized by the property that B° acts trivially on $(B,+)$ by means of the λ-action.

A *subbrace* of a brace B is a subset $A\subseteq B$ that is a subgroup of both $(B,+)$ and $(C,\circ)$. A *left ideal* of B is a subset I of B such that I is a subgroup of $(B,+)$, and $\lambda_a(I)\subseteq I$ for all $a\in B$. If additionally, I is a normal subgroup of $(C,\circ)$, one calls I an *ideal*. For example, the *socle* of B,

$$\mathrm{Soc}(B)=\ker\lambda=\{b\in B\mid a\circ b=a+b\text{ for all }b\in B\},$$

is an ideal of B.

Convention. *Throughout the rest of this article, we will suppress* $\circ$ *for the multiplication in a brace and indicate it by juxtaposition.*

2.2. **Cycle sets.** A *cycle set* is a non-empty set X with a binary operation $(x,y)\mapsto x*y$ such that the left multiplication by x

$$\sigma_x:y\mapsto x*y$$

is a bijection for each $x\in X$ and

$$(x*y)*(x*z)=(y*x)*(y*z)$$

holds for all $x,y,z\in X$. If additionally, the *square map* $\mathrm{Sq}:x\mapsto x*x$ is bijective, we say that the cycle set is *non-degenerate*. Recall that a finite cycle set is always non-degenerate, as proven in [11, Theorem 2].

Convention. *This article considers non-degenerate cycle sets only, so we will refer to* non-degenerate cycle sets *more briefly as* cycle sets.

A cycle set $(X,*)$ is called *indecomposable* if there are no proper partitions $X=X_1\sqcup X_2$ such that the X_i $(i=1,2)$ are closed under the cycle set operation.

It can be shown that any brace $(B,+,\circ)$ becomes a cycle set under the mappings $\sigma_b=\lambda_b^{-1}$ $(b\in B)$. On the other hand, cycle sets give rise to several braces, as well: for any cycle set $(X,*)$, define its *permutation group* as the subgroup

$$\mathcal{G}(X)=\langle\sigma_x\mid x\in X\rangle\leqslant\mathrm{Sym}_X,$$

the latter denoting the symmetric group of permutations on the set X. Recall that, as proven in [8, Proposition 2.12], X is indecomposable if and only if $\mathcal{G}(X)$ acts transitively on X. Moreover, there is a unique way to equip $(\mathcal{G}(X),\circ)$ with an abelian group operation $+$ that satisfies $\lambda_x+\lambda_y=\lambda_x\lambda_{\lambda_x^{-1}(y)}$, such that $(\mathcal{G}(X),+,\circ)$ is a brace.

Convention. Sym_X *acts from the left on* X*, so we mainly use the* λ*-notation to express the action of an element* $g \in \mathcal{G}(X)$ *on an element* $y \in X$ *by* $\lambda_g(y)$*. Furthermore, we have the identification* $\lambda_x = \sigma_x^{-1}$ *and use* σ*-notation whenever it is more comfortable to do so.*

Note also that in this work, the notation λ_g *for an element* $g \in \mathcal{G}(X)$ *or* $g \in G(X)$ *can appear in two contexts: either it is the action of* g *on the set* X *or it is the* λ*-action of* g *by an automorphism of the braces* $\mathcal{G}(X)$ *or* $G(X)$*. As the* λ*-action on these braces is a mere extension of the* λ*-action on* X*, there will be no danger of confusion as it will always be clear which set is acted upon by* λ_g*.*

Example 2.2. For some $n > 0$, let $X = \{x_1, \dots, x_n\}$ and fix the permutation cycle $\sigma = (1\ 2 \dots\ n)$. Then the operation $x_i * x_j = x_{\sigma(j)}$ turns X into a cycle set, called a *cyclic* cycle set. It can be shown that $(X, *)$ is an indecomposable cycle set with permutation group $\mathcal{G}(X) = \langle (1\ 2 \dots n) \rangle \cong \mathbb{Z}_n$, the cyclic group of order n. Furthermore, $\mathcal{G}(X)$ is a trivial brace when equipped with the canonical brace structure described above.

With any cycle set $(X, *)$ we also associate its *structure group*

$$G(X) = \langle X \mid (x * y)x = (y * x)y \rangle$$

that contains X, as the canonical map $X \to G(X)$, $x \mapsto x$ can be shown to be injective.

Moreover, there is a unique way of defining an addition on $G(X)$ that extends

$$x + y = x\sigma_x(y) = x\lambda_x^{-1}(y)$$

for $x, y \in X$ and that provides $G(X)$ with a brace structure (see [1], for instance). Under the cycle set structure of the thus constructed brace $G(X)$, the embedding $X \hookrightarrow G(X)$ identifies X with a sub-cycle set of $G(X)$.

Note also that there is a surjective brace homomorphism $G(X) \to \mathcal{G}(X)$ given by $x \mapsto \lambda_x$ which has kernel $\mathrm{Soc}(G(X))$. This implies also that the map $\lambda : X \to \mathcal{G}(X)$, $x \mapsto \lambda_x$ is a cycle set homomorphism.

An important invariant of a non-degenerate cycle set X that we are going to use throughout the whole paper is the *Dehornoy class*. It is the smallest positive integer d such that $dx \in \mathrm{Soc}(G(X))$ for every $x \in X$.

There is also a different interpretation of the Dehornoy class, given in [10]:

Proposition 2.3. *The Dehornoy class* d *of a finite cycle set* X *is the least common multiple of the additive orders of the generators* $\lambda_x \in \mathcal{G}(X)$ $(x \in X)$*. Equivalently,* d *is the exponent of the group* $(\mathcal{G}(X), +)$*.*

Let $\pi(k)$ denote the set of prime divisors of an integer k. In [9], the following properties are proven

Proposition 2.4. *Let* X *be a cycle set of size* n *and Dehornoy class* d*. Then* d *divides* $|\mathcal{G}(X)|$ *and* $|\mathcal{G}(X)|$ *divides* d^n*, so* $\pi(d) = \pi(|\mathcal{G}(X)|)$*.*

In particular, if X *is indecomposable, then* $\pi(n) \subseteq \pi(d) = \pi(|\mathcal{G}(X)|)$

Let X be a cycle set with Dehornoy class d, then for any integer $l \geqslant 1$, the additive subgroup $ldG(X) = \{(ld)g : g \in G(X)\} \leqslant (G(X), +)$ is a left ideal of $G(X)$ that is contained in $\mathrm{Soc}(G(X))$ and therefore, is an ideal of $G(X)$. This justifies the following definition

Definition 2.5. Let X be a cycle set with Dehornoy class d. Given an integer $l \geqslant 1$, we define the *Coxeter-like group*

$$\overline{G}_l(X) = G(X)/ldG(X).$$

Note that the additive group of $\overline{G}_l(X)$ is isomorphic to $\mathbb{Z}_{ld}^X$. Also observe that, as $ldG(X) \subset \mathrm{Soc}(G(X))$, the canonical morphism $G(X) \to \mathcal{G}(X)$ factorizes through $\overline{G}_l(X)$, i.e $\mathcal{G}(X) = \overline{G}_l(X)/\,\mathrm{Soc}(\overline{G}_l(X))$.

The importance of the Coxeter-like groups lies in the fact that they play the role of a germ of the Garside structure on $G(X)$ (see [6]).

Convention. *From now on, we will often abbreviate $G(X)$ with G when the context is clear. The same convention applies to $\mathcal{G}(X)$, $\overline{G}(X)$ and $\overline{G}_l(X)$.*

2.3. **Induced representations.** Let G be a group, R a commutative ring and V an R-module. It is well-known that a representation $\rho\colon G \to \mathrm{Aut}(V)$ is equivalent to an $R[G]$-module structure on V.

Proposition-Definition 2.6 ([5, §43])**.** *If H is a subgroup of G and V is an $R[H]$-module, the* induced $R[G]$-module *is defined as $\mathrm{Ind}_H^G V = R[G] \otimes_{R[H]} V$.*

By the correspondence between representations and modules, the *induced representation* $\mathrm{Ind}_H^G \rho$ is the representation of G associated with the $R[G]$-module $\mathrm{Ind}_H^G V$, where V is the $R[H]$-module associated with the representation ρ.

It is well-known that induced representations are connected to systems of imprimitivity.

Definition 2.7 ([5, §50.1])**.** Let V be an $R[G]$-module. A family of R-submodules $(U_i)_{i\in I}$ of V is a *system of imprimitivity* if the following three conditions are satisfied:

(1) $V = \bigoplus_{i\in I} U_i$,
(2) G permutes the family, i.e. for all $i \in I$, $g \in G$, there is a $j \in I$ such that $g \cdot U_i = U_j$,
(3) G acts transitively on the family, i.e. for all $i, j \in I$, there is a $g \in G$ such that $g \cdot U_i = U_j$.

Proposition 2.8. *Let V be an $R[G]$-module and $(U_i)_{i\in I}$ a system of imprimitivity thereof. For an $i_0 \in I$, let $G_0 = \{g \in G : g \cdot U_{i_0} = U_{i_0}\}$. Then, by restriction, U_{i_0} is an $R[G_0]$-module and there is a canonical homomorphism of $R[G]$-modules*

$$V \cong \mathrm{Ind}_{G_0}^G U_{i_0}.$$

Proof. [5, §50.2]. □

Remark 2.9. Although [5] treats the concept of (systems of) imprimitivity in terms of modules over group rings over a *field*, Definition 2.7 and Proposition 2.8 are also valid for group rings over a commutative ring.

Moreover, we decided to change the notation for induced modules in the reference in favour of the more suggestive notation Ind_H^G.

2.4. **Monomial representation.** In 2015, Dehornoy [6] developed a calculus of words to study structure groups of cycle sets and their Garside structure. In particular, give n a cycle set X, he deduces the existence of a monomial representation of its structure group $\Theta : G(X) \to M_X(\mathbb{C}(q))$, where $M_X(\mathbb{C}(q))$ is the ring of matrices with entries in $\mathbb{C}(q)$ indexed by $X \times X$. Moreover, he shows that this representation descends to a representation of the Coxeter-like group $\overline{G}$ when specializing q to a d-th root of unity ζ_d, where d is the Dehornoy class of X.

Given a permutation $\sigma \in \mathrm{Sym}_X$, we write $P_\sigma = (P_{ij})_{i,j\in X}$ for its *permutation matrix* whose entries are given by

$$P_{ij} = \begin{cases} 1 & i = \sigma(j) \\ 0 & i \neq \sigma(j). \end{cases}$$

This matrix acts on a basis vector e_i ($i \in X$) as $P_\sigma(e_i) = e_{\sigma(i)}$. In $M_X(\mathbb{C}(q))$ for $x \in X$, denote by D_x the diagonal matrix $\mathrm{diag}(1, \dots, 1, q, 1, \dots, 1)$ with a q on the x-coordinate. Furthermore, define for $x \in X$ the permutation matrix $P_x = P_{\lambda_x}$ and, more generally, $P_g = P_{\lambda_g}$ for $g \in \mathcal{G}(X)$.

Theorem-Definition 2.10 ([6], Proposition 5.13)**.** *The map $X \to M_X(\mathbb{C}(q))$ defined by $x \mapsto D_x P_x$ extends to a faithful representation*

$$\Theta\colon G(X) \to M_X(\mathbb{C}(q)).$$

Let d be the Dehornoy class of X. Then, for any positive integer l, specializing at $q = \zeta_{ld} = e^{\frac{2i\pi}{ld}}$ yields a faithful representation

$$\begin{aligned} \overline{\Theta}_l\colon \overline{G}_l(X) = G(X)/ldG(X) &\to M_X(\mathbb{C}) \\ g \cdot ldG(X) &\mapsto \Theta(g)_{q=\zeta_{ld}}. \end{aligned}$$

Moreover, if $g \in G(X)$ is expressed in the brace structure as $g = \sum_{x \in X} g_x x$ then $\Theta(g)$ can be uniquely written as the product of a diagonal matrix and a permutation matrix as follows:

$$\Theta(g) = \left(\prod_{x \in X} D_x^{g_x} \right) P_{\lambda_g}. \tag{2.1}$$

We will denote $D_g = \prod_{x \in X} D_x^{g_x}$, so that $\Theta(g) = D_g P_g$.

The representations Θ, $\overline{\Theta}_l$ are called the monomial representations *of $G(X)$ resp. $\overline{G}_l(X)$.*

Remark 2.11. In [6], well-definedness and faithfulness of $\overline{\Theta}_l$ have only been proven for $l = 1$. However, an inspection of Eq. (2.1) shows that $\Theta(g)_{q=\zeta_{ld}}$ is the identity matrix if and only if $g \in ldG(X)$, which proves that $\overline{\Theta}_l$ is indeed well-defined and faithful on $\overline{G}_l = G/ldG$.

Convention. *Throughout the rest of the article, we will abbreviate $\overline{G}_1$ with $\overline{G}$, and $\overline{\Theta}_1$ with $\overline{\Theta}$.*

3. Irreducibility

Let X be a cycle set of size n, class d, permutation group $\mathcal{G}$ and structure group G. Recall that $\sigma_x = \lambda_x^{-1}$, and that $|\mathcal{G}|$ divides d^n Proposition 2.4.

As G is a brace and $(G, +)$ is generated by X, we can express any g in G as $g = \sum_{x \in X} g_x x$ with $g_x \in \mathbb{Z}$ ($x \in X$).

Proposition 3.1. *If X is a decomposable cycle set, the representations Θ and $\overline{\Theta}_l$ are reducible.*

Proof. If X is decomposable, say $X = X_1 \sqcup X_2$, then the action of G stabilizes the proper subspaces spanned by X_1 and X_2 in $\mathbb{C}(q)^X$, thus Θ is reducible. The proof for $\overline{\Theta}_l$ is exactly the same. □

In the following, we will prove that $\overline{\Theta}$ (i.e. $\overline{\Theta}_1$) is irreducible for most indecomposable cycle sets X.

Theorem 3.2. *Let X be an indecomposable cycle set of size n and Dehornoy class d. $\overline{\Theta}$ is irreducible if one of the following conditions is satisfied:*

(1) $d > 2$,
(2) $d = 2$ *and* $|\mathcal{G}(X)| < 2^{\frac{n}{2}}$.

We provide some machinery first:

Let p be a prime and $n > 0$. We can always uniquely factorize $n = p^v m$ with $v, m \geqslant 0$ and $p \nmid m$. Therefore, one can define the *p-valuation* $v_p(n)$ as the exponent v in such a factorization.

On the other hand, there is a unique p-adic representation $n = \sum_{i=0}^{\infty} a_i p^i$ with $0 \leqslant a_i < p$ for all $i \geqslant 0$. The *p-adic digit sum* of n is defined as $\mathrm{DS}_p(n) = \sum_{i=0}^{\infty} a_i$.

We will need the following elementary result about the p-valuation of factorials:

Lemma 3.3. *For all $n \geqslant 0$, we have $v_p(n!) = \frac{n - \mathrm{DS}_p(n)}{p-1}$.*

Proof. [4, Lemma 4.2.8.]. □

The following estimate for the p-valuation of $|\mathcal{G}(X)|$ is now immediate:

Lemma 3.4. *Let X be a cycle set of size n. Then, $v_p(|\mathcal{G}(X)|) \leqslant \frac{n-1}{p-1}$ for any prime p.*

Proof. As $\mathcal{G}(X)$ is a subgroup of Sym_X, the order $|\mathcal{G}(X)|$ divides $|\mathrm{Sym}_X| = n!$ and therefore,

$$v_p(|\mathcal{G}(X)|) \leqslant v_p(n!) = \frac{n - \mathrm{DS}_p(n)}{p-1} \leqslant \frac{n-1}{p-1}.$$

□

Denote the set of invertible diagonal $n \times n$-matrices over a field K by $\mathcal{D}_n(K)$. We will use the following general lemma:

Lemma 3.5. *Let $n > 0$, G be a group and let $\rho : G \to \mathcal{D}_n(K)$ be a representation. Let $\rho(g) = \mathrm{diag}(d_{1,g}, \ldots, d_{n,g})$ and suppose that for any $1 \leqslant i < j \leqslant n$, there is a $g \in G$ such that $d_{i,g} \neq d_{j,g}$. Then every G-invariant subspace $0 \neq U \leqslant K^n$ contains some unit vector e_i.*

Proof. Let $0 \neq U \subseteq K^n$ be G-invariant and pick $0 \neq v \in U$ whose *support* $\mathrm{supp}(v) = \{i \in \{1, \ldots, n\} : v_i \neq 0\}$ is as small as possible. If $|\mathrm{supp}(v)| = 1$, then $v = a e_i$ for some $0 \neq a \in K$ and some index i, and the claim is proven. Suppose that $|\mathrm{supp}(v)| > 1$ and choose indices $i < j$ with $i, j \in \mathrm{supp}(v)$. By assumption, there is a $g \in G$ such that $d_{i,g} \neq d_{j,g}$. Consider the vector $w = \rho(g)(v) - d_{j,g} v \in U$. As ρ acts by diagonal matrices, it is immediate that $\mathrm{supp}(w) \subseteq \mathrm{supp}(v)$. For this vector, we observe:

$$\begin{aligned} w_i &= d_{i,g} v_i - d_{j,g} v_i = (d_{i,g} - d_{j,g}) v_i \neq 0; \\ w_j &= d_{j,g} v_j - d_{j,g} v_j = 0. \end{aligned}$$

The first calculation allows us to conclude that $w \neq 0$. The other calculation shows that $j \notin \mathrm{supp}(w)$ which implies $|\mathrm{supp}(w)| \leqslant |\mathrm{supp}(v)| - 1$. But this contradicts the assumption that the support of v is as small as possible among the nonzero vectors in U. □

Lemma 3.6. *Let X be an indecomposable cycle set. Furthermore, let U be an invariant subspace of $\mathbb{C}^X$ under $\overline{\Theta}_l$ (resp. an invariant subspace of $\mathbb{C}(q)^X$ under Θ). If e_x is in U for some $x \in X$, then $U = \mathbb{C}^X$ (resp. $U = \mathbb{C}(q)^X$).*

Proof. We will only consider the representation Θ as the proof is similar for $\overline{\Theta}_l$. By indecomposability, for all e_y, there exists $g \in G$ such that $P_g e_x = e_y$, therefore an application of Eq. (2.1) shows that $\Theta(g) e_x = D_g P_g e_x = D_g e_y \in U$. As D_g is diagonal, $\Theta(g) e_x$ is a scalar multiple of e_y, so $e_y \in U$. It follows that $U = \mathbb{C}(q)^X$. □

Proof of Theorem 3.2. Let p be a prime dividing d and write $d = m p^v$ with $p \nmid m$.

Write $\overline{G}^{(p)}$ for the (additive) p-Sylow subgroup of $\overline{G}$ and consider the p-Sylow subgroup of the socle, $S^{(p)} = \mathrm{Soc}(\overline{G})^{(p)} \subseteq \overline{G}^{(p)}$. Then $\overline{\Theta}$ restricts to a faithful diagonal representation $\overline{\Theta}|_{S^{(p)}} : S^{(p)} \to \mathcal{D}_X(\mathbb{C})$, such that the diagonal matrices in the image have p^v-th roots of unity on the diagonal.

As $(\overline{G}, +) = \mathbb{Z}_d^X$, it follows that $\overline{G}^{(p)} = m\overline{G}$, so we can express each element $g \in \overline{G}^{(p)}$ uniquely as

$$g = \sum_{x \in X} g_x m x \quad (\forall x \in X : \; 0 \leqslant g_x < p^v).$$

Using this notation, we define on X the equivalence relation:

$$x \sim y \Leftrightarrow \forall s \in S^{(p)} : s_x = s_y.$$

If $x \sim y$ and $g \in \overline{G}$, then for all $s \in S^{(p)}$, we also have

$$s_{\lambda_g(x)} = (\lambda_g^{-1}(s))_x = (\lambda_g^{-1}(s))_y = s_{\lambda_g(y)}.$$

Here we use the fact that $S^{(p)}$ is a left ideal in $\overline{G}$: as $\mathrm{Soc}(\overline{G})$ is an ideal in $\overline{G}$ and $S^{(p)}$, its unique p-Sylow subgroup, is characteristic therein, each λ_g $(g \in \overline{G})$ has to restrict to an automorphism of $\mathrm{Soc}(\overline{G})$ that leaves $S^{(p)}$ invariant.

Therefore, the equivalence relation $\sim$ is $\overline{G}$-invariant and the classes in $X/\!\sim$ are blocks for the action of $\overline{G}$ on X. In particular, all blocks have the same size. Write $\mathcal{B}_x = \{y \in X : x \sim y\}$ for $x \in X$.

If $\sim$ is not a trivial equivalence relation, then $|\mathcal{B}_x| \geqslant 2$ for all $x \in X$ which shows that $|X/\!\sim| \leqslant \frac{n}{2}$. As by definition, the coordinates s_x are blockwise constant for $s \in S^{(p)}$, and can take p^v different values, we conclude that $|S^{(p)}| \leqslant p^{\frac{vn}{2}}$ and thus, $v_p(|S^{(p)}|) \leqslant \frac{vn}{2}$. This implies that

$$v_p(|\mathcal{G}^{(p)}|) = v_p\left(\frac{|\overline{G}^{(p)}|}{|S^{(p)}|}\right) = vn - \frac{vn}{2} \geqslant \frac{vn}{2}$$

if $\sim$ is nontrivial. If $p > 2$, then, by Lemma 3.4, we can estimate

$$v_p(|\mathcal{G}^{(p)}|) \leqslant \frac{n-1}{p-1} < \frac{n}{2} \leqslant \frac{vn}{2}.$$

In this case, $\sim$ is a trivial equivalence relation. If $p = 2$ and $v > 1$, we use the same lemma to conclude that

$$v_2(|\mathcal{G}^{(2)}|) \leqslant n - 1 < \frac{vn}{2}$$

which again implies that $\sim$ is trivial. We conclude that if $d > 2$, we can always find a prime $p|d$ for which the equivalence relation $\sim$ is trivial.

Finally, let $d = 2$, i.e. $p = 2$ and $v = 1$, and suppose that $|\mathcal{G}| < 2^{\frac{n}{2}}$, then also $|\mathcal{G}^{(2)}| < 2^{\frac{n}{2}}$, therefore

$$v_2(|\mathcal{G}^{(2)}|) < \frac{n}{2} \leqslant \frac{vn}{2},$$

and $\sim$ is trivial.

We have therefore proven that in both cases considered in the theorem, we can find a prime $p|d$ such that the associated equivalence relation $\sim$ is trivial on X.

For $s \in S^{(p)}$, Eq. (2.1) implies that $\overline{\Theta}(s)$ is a diagonal matrix with entries $d_{x,s} = \zeta_d^{s_x m} = \zeta_{p^v}^{s_x}$, therefore triviality of $\sim$ means that for any $x, y \in X$ with $x \neq y$, there is an $s \in S^{(p)}$ such that $d_{x,s} \neq d_{y,s}$.

Let now $0 \neq U \subseteq \mathbb{C}^X$ be a $\overline{G}$-invariant subspace with respect to the action of $\overline{\Theta}$. As U is, in particular, $S^{(p)}$-invariant, Lemma 3.5 now tells us that $e_x \in U$ for some $x \in X$. But by Lemma 3.6, it follows that $U = \mathbb{C}^X$. As U was arbitrary, it follows that $\overline{\Theta}$ is irreducible in the considered cases. □

It turns out that $l = 1$ is the only case where indecomposability of X does not always guarantee that $\overline{\Theta}_l$ is irreducible. Using way simpler techniques, we can prove:

Proposition 3.7. *Let l be a positive integer. Consider the following assertions:*

(i) X is indecomposable
(ii) $\Theta\colon G \to M_X(\mathbb{C}(q))$ is irreducible
(iii) $\overline{\Theta}_l\colon \overline{G}_l \to M_X(\mathbb{C})$ is irreducible.

Then the following hold:

a) (ii) $\Leftrightarrow$ (i)
b) If $l = 1$, then (iii) $\Rightarrow$ (i)
c) If $l > 1$, then (iii) $\Leftrightarrow$ (i).

Proof. *(ii)* $\Rightarrow$ *(i)* and *(iii)* $\Rightarrow$ *(i)* have already been dealt with in Proposition 3.1, so we are left with proving the implications *(i)* $\Rightarrow$ *(ii)* and, for $l > 1$, *(i)* $\Rightarrow$ *(iii)*.

Suppose that X is indecomposable. Let U be a non-trivial subspace of $\mathbb{C}(q)^X$ that is G-invariant. As X is of class d, we see for all $x \in X$ that $dx \in \mathrm{Soc}(G)$ which implies that $\Theta(dx) = D_x^d = \mathrm{diag}(1, \dots, q^d, \dots, 1)$ with $q^d \neq 1$ in the position of x. Considering all matrices $\Theta(dx)$ $(x \in X)$ proves that for any $x, y \in X$ there is a $g \in \mathrm{Soc}(G)$ with $d_{x,g} \neq d_{y,g}$. By Lemma 3.5, U contains a unit vector e_x and Lemma 3.6 implies that $U = \mathbb{C}(q)^X$. Therefore, Θ is irreducible.

If $l > 1$, we see for $x \in X$ that $\overline{\Theta}_l(dx) = \mathrm{diag}(1, \dots, \zeta_{ld}^d, \dots, 1)$ with $\zeta_{ld}^d = \zeta_l \neq 1$ in the position of x. If X is indecomposable, the same line of reasoning can now be applied to prove the irreducibility of $\overline{\Theta}_l$ for $l > 1$. □

Remark 3.8. Only for $l = 1$, the indecomposability of X does not necessarily imply the irreducibility of $\Theta\colon \overline{G} \to M_X(\mathbb{C})$.

Indeed, consider Example 2.2 for $n = 2$: in that case, $X = \{x_1, x_2\}$ and $x_i * x_j = x_{\sigma(j)}$ where $\sigma = (1\ 2)$. Then X is of class 2 and furthermore,

$$\overline{\Theta}(x_1) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \overline{\Theta}(x_2) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -\overline{\Theta}(x_1).$$

These matrices are simultaneously diagonalizable over $\mathbb{C}$, the eigenvalues being $\pm i$, so $\overline{\Theta}$ is not irreducible.

We close this section with a number-theoretic application of our results.

Example 3.9. For $n > 2$, consider the cyclic cycle set $X = \{x_1, \dots, x_n\}$ from Example 2.2 with $x_i * x_j = x_{\sigma(j)}$ where $\sigma = (1\ 2 \dots\ n)$. Then X is of class n and indecomposable. As $d = n > 2$, $\overline{\Theta}$ is irreducible by Theorem 3.2. Moreover, by [13, Theorem 5], a representation ρ of a finite group G is irreducible if and only if $\frac{1}{|G|} \sum_{g \in G} |\mathrm{Tr}(\rho(g))|^2 = 1$. We now apply this formula to the representation $\overline{\Theta}$:

For any $g \in \overline{G}$, write $g = \sum_{x_i \in X} a_i x_i$ $(0 \leqslant a_i < n)$ and define its *length* as $\overline{\ell}(g) = \sum_{x_i \in X} a_i$. Then $\lambda_g = \sigma^{-\overline{\ell}(g)}$. Moreover, σ^k stabilizes a point if and only if k is a multiple of n, and in this case, λ_g stabilizes X pointwisely. Thus the trace of g is non-trivial if and only if n divides $\overline{\ell}(g)$ and in this case, $\mathrm{Tr}(\overline{\Theta}(g)) = \sum_{i=1}^n \zeta_d^{a_i}$.

As $\overline{\Theta}$ is irreducible, we have $\frac{1}{|\overline{G}|} \sum_{g \in \overline{G}} |\mathrm{Tr}(\overline{\Theta}(g))|^2 = 1$. We conclude that

$$\sum_{\substack{0 \leqslant a_1, \dots, a_n < n \\ a_1 + \cdots + a_n \equiv 0 \bmod n}} |\zeta_d^{a_1} + \cdots + \zeta_d^{a_n}|^2 = n^n.$$

4. Induction

The aim of this section is the description of monomial representations in terms of induced representations.

We now choose an element $x_0 \in X$ and define $G_0 = \{g \in G \mid \lambda_g(x_0) = x_0\}$ and $\overline{G}_{l,0} = \{g \in \overline{G}_l \mid \lambda_g(x_0) = x_0\}$ for $l \geqslant 1$. Recall that we can write any element g in the structure brace G as $g = \sum_{x \in X} g_x x$.

Proposition 4.1. *The mapping*

$$c_0 : G \to \mathbb{Z}; \quad g \mapsto g_{x_0}$$

satisfies the following property: for $g \in G_0$, $h \in G$, we have

$$c_0(gh) = c_0(g) + c_0(h).$$

In particular, the restriction $c_0|_{G_0} : G_0 \to \mathbb{Z}$ is group homomorphism.

Proof. We have $gh = g + \lambda_g(h) = \sum_{x \in X} g_x x + \sum_{x \in X} h_x \lambda_g(x)$. If $g \in G_0$, then $\lambda_g(x_0) = x_0$ which implies $(\lambda_g(h))_{x_0} = h_{x_0}$. Thus,

$$c_0(gh) = g_{x_0} + (\lambda_g(h))_{x_0} = g_{x_0} + h_{x_0} = c_0(g) + c_0(h),$$

which proves the first statement. The second statement of the proposition is now immediate. □

By Proposition 4.1, we can define the character $\chi_0 : G_0 \to \mathbb{C}[q^{\pm 1}] \subset \mathbb{C}(q)$ by $g \mapsto q^{c_0(g)} = q^{g_{x_0}}$.

Lemma 4.2. *The character $\chi_0 \colon G_0 \to \mathbb{C}[q^{\pm 1}]$ descends to a character $\overline{\chi}_{l,0} \colon \overline{G}_{l,0} \to \mathbb{C}$.*

Proof. With the specialization $\mathrm{ev}_{ld} \colon \mathbb{C}[q^{\pm 1}] \to \mathbb{C}$; $q \mapsto \zeta_{ld}$, we obtain the character $\mathrm{ev}_{ld}\chi_0 : G_0 \to \mathbb{C}$; $g \mapsto \zeta_{ld}^{g_{x_0}}$. Recall that $\overline{G}_l = G/ldG$ and $ldG \subseteq \mathrm{Soc}(G) \subseteq G_0$. Thus, $\mathrm{ev}_{ld}\chi_0$ factorizes uniquely as $\overline{\chi}_{l,0}$ through the canonical projection $G_0 \twoheadrightarrow G_0/ldG$. Furthermore,

$$\ker(G_0 \to \overline{G}_{l,0}) = G_0 \cap \ker(G \to \overline{G}_l) = G_0 \cap ldG = ldG.$$

Thus, $G_0/ldG = \overline{G}_{l,0}$ and $\overline{\chi}_{l,0}$ is well-defined. □

For a commutative ring R, a group G and a one-dimensional character $\chi : G \to R^\times$, we denote by R_χ the $R[G]$-module that is uniquely defined by the scalar multiplication $rg \cdot s = r\chi(g)s$.

We can now show that the monomial representations of indecomposable cycle sets are induced:

Theorem 4.3. *Let X be an indecomposable cycle set and x_0 be an element of X. Let $(A, \Gamma, \Gamma_0, \rho, \chi, \omega)$ be one of the following:*

a) $(\mathbb{C}(q), G, G_0, \Theta, \chi_0, q)$
b) $\left(\mathbb{C}[q^{\pm 1}], G, G_0, \Theta, \chi_0, q\right)$
c) $\left(\mathbb{C}, \overline{G}_l, \overline{G}_{l,0}, \overline{\Theta}_l, \overline{\chi}_{l,0}, \zeta_{ld}\right)$, *for* $l \geqslant 1$.

Then, there is an isomorphism of $A[\Gamma]$-modules $A^X \cong \mathrm{Ind}_{\Gamma_0}^{\Gamma} A_\chi$ where A^X is the $A[\Gamma]$-module defined by the monomial representation $\rho \colon \Gamma \to M_X(A)$.

Proof. We only deal with case b) as all other cases follow from a suitable extension/specialization of scalars. Therefore, writing $R = \mathbb{C}[q^{\pm 1}]$, it is easily seen that for $x \in X$, $g \in G$, we have $g \cdot (Rx) = R(\lambda_g(x))$, therefore G permutes the family $(Rx)_{x \in X}$. As X is indecomposable, G acts transitively on X, therefore $(Rx)_{x \in X}$ is a system of imprimitivity for the $R[G]$-module R^X. Pick an $x_0 \in X$ and observe that

$$G_0 = \{g \in G : \lambda_g(x_0) = x_0\} = \{g \in G : g \cdot (Rx_0) = Rx_0\},$$

so Proposition 2.8 implies that there is an isomorphism of $R[G]$-modules

$$R^X \cong \mathrm{Ind}_{G_0}^{G} Rx_0.$$

We are left with determining the character associated with the $R[G_0]$-module Rx_0. Let $g \in G_0$ and write $g = \sum_{x\in X} g_x x$, then by Eq. (2.1),

$$g \cdot x_0 = D_g P_g x_0 = D_g x_0 = q^{g_{x_0}} x_0 = \chi_0(g) x_0.$$

This proves that $Rx_0 \cong A_{\chi_0}$, as $R[G_0]$-modules. Therefore,

$$R^X \cong \mathrm{Ind}_{G_0}^{G} R_{\chi_0}.$$

□

Acknowledgements

This work is partially supported by the project OZR3762 of Vrije Universiteit Brussel, by FWO and CNRS via the International Emerging Actions project 328226 and by Fonds Wetenschappelijk Onderzoek - Vlaanderen, via the Senior Research Project G004124N.

The first author expresses his gratitude to the Humboldt foundation that had supported him by means of a Feodor Lynen fellowship when beginning the research for this project.

The third author is supported by Fonds Wetenschappelijk Onderzoek - Vlaanderen, via a PhD Fellowship fundamental research, grant 11PIO24N.

References

[1] Ferran Cedó. "Left Braces: Solutions of the Yang-Baxter Equation". In: *Advances in Group Theory and Applications* 5 (2018), pp. 33–90. DOI: 10.4399/97888255161422.

[2] Ferran Cedó, Eric Jespers, and Jan Okniński. "Braces and the Yang-Baxter equation". English. In: *Communications in Mathematical Physics* 327.(DOI) 10.1007/s00220-014-1935-y (2014), pp. 101–116. ISSN: 0010-3616.

[3] Fabienne Chouraqui. "Garside Groups and Yang–Baxter Equation". In: *Communications in Algebra* 38.12 (2010), pp. 4441–4460. DOI: 10.1080/00927870903386502.

[4] Henri Cohen. *Number Theory, Volume 1: Tools and Diophantine Equations*. 1st ed. Graduate Texts in Mathematics. Springer, 2007. ISBN: 9780387499222.

[5] Charles W. Curtis and Irving Reiner. *Representation Theory of Finite Groups and Associative Algebras*. Vol. 356. AMS Chelsea Publishing, 1962. ISBN: 978-0-8218-4066-5.

[6] Patrick Dehornoy. "Set-theoretic solutions of the Yang–Baxter equation, RC-calculus, and Garside germs". In: *Advances in Mathematics* 282 (2015), pp. 93–127. ISSN: 0001-8708. DOI: https://doi.org/10.1016/j.aim.2015.05.008.

[7] Vladimir Drinfeld. "On Some Unsolved Problems in Quantum Group Theory". In: Lecture Notes in Mathematics 1510 (1992), pp. 1–8. DOI: 10.1007/BFb0101175.

[8] Pavel Etingof, Travis Schedler, and Alexandre Soloviev. "Set-Theoretical Solutions to the Quantum Yang-Baxter Equation". In: *Duke Mathematical Journal* 100 (1999), pp. 169–209. DOI: 10.1215/S0012-7094-99-10007-X.

[9] Edouard Feingesicht. "Dehornoy's Class and Sylows for Set-Theoretical Solutions of the Yang–Baxter Equation". In: *International Journal of Algebra and Computation* 34 (2024), pp. 147–173. DOI: 10.1142/S0218196724500048.

[10] Victoria Lebed, Santiago Ramírez, and Leandro Vendramin. "Involutive Yang-Baxter: cabling, decomposability, and Dehornoy class". In: *Rev. Mat. Iberoam.* 40.2 (2024), pp. 623–635. ISSN: 0213-2230,2235-0616. DOI: 10.4171/rmi/1438. URL: https://doi.org/10.4171/rmi/1438.

[11] Wolfgang Rump. "A Decomposition Theorem for Square-Free Unitary Solutions of the Quantum Yang-Baxter Equation". In: *Advances in Mathematics* 193 (2005), pp. 40–55. DOI: 10.1016/j.aim.2004.03.019.

[12] Wolfgang Rump. "Braces, Radical Rings, and the Quantum Yang–Baxter Equation". In: *Journal of Algebra* 307.1 (Jan. 2007), pp. 153–170. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2006.03.040.

[13] Jean-Pierre Serre. *Linear Representations of Finite Groups*. Vol. 42. Graduate Texts in Mathematics. New York, NY: Springer, 1977. ISBN: 978-1-4684-9460-0. DOI: 10.1007/978-1-4684-9458-7.

(Carsten Dietzel) Laboratoire de Mathématiques Nicolas Oresme, Université de Caen Normandie, Campus 2, 14000 Caen, France

Email address: carsten.dietzel@unicaen.fr

(Edouard Feingesicht) Laboratoire de Mathématiques Nicolas Oresme, Université de Caen Normandie, Campus 2, 14000 Caen, France

Email address: edouard.feingesicht@unicaen.fr

(Silvia Properzi) Department of Mathematics and Data Science, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussel, Belgium

Email address: Silvia.Properzi@vub.be