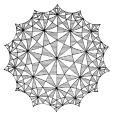
Rev. Mat. Iberoam. (Online first)
DOI 10.4171/RMI/1438



Involutive Yang–Baxter: cabling, decomposability, and Dehornoy class

Victoria Lebed, Santiago Ramírez and Leandro Vendramin

Abstract. We develop new machinery for producing decomposability tests for involutive solutions to the Yang–Baxter equation. It is based on the seminal decomposability theorem of Rump and on "cabling" operations on solutions and their effect on the diagonal map T. Our machinery yields an elementary proof of a recent decomposability theorem of Camp-Mora and Sastriques, as well as original decomposability results. It also provides a conceptual interpretation (using the language of braces) of the Dehornoy class, a combinatorial invariant naturally appearing in the Garside-theoretic approach to involutive solutions.

1. Introduction

A *finite non-degenerate involutive set-theoretic solution to the Yang–Baxter equation*, called *solution* in this paper, is a non-empty finite set X endowed with an involutive map

$$r\colon X \times X \to X \times X, \quad r(x,y) = (\sigma_x(y), \tau_y(x)),$$

satisfying

$$r_1 r_2 r_1 = r_2 r_1 r_2,$$

where the maps $r_i\colon X^3 \to X^3$ are defined by $r_1 = r \times \mathrm{Id}_X$ and $r_2 = \mathrm{Id}_X \times r$, and the maps σ_x and τ_x are bijective for all $x \in X$. Throughout the paper, we will assume that $n = |X| > 1$. The origins, applications and recent results on solutions can be found in the extensive literature which followed [16, 19].

A solution is called *decomposable* if the set X decomposes into two non-empty disjoint parts $X = Y \sqcup Z$, with $r(Y \times Y) = Y \times Y$ and $r(Z \times Z) = Z \times Z$. This is equivalent to asking the *permutation group* $\mathcal{G}(X,r)$ of (X,r), which is the group of permutations on X generated by all the σ_x, to be non-transitive [16]. A natural approach to the (as for now unattainable) problem of classifying all solutions consists in constructing all indecomposable solutions [4–7, 12, 13, 26–29], and then understanding how these building blocks can cement together [1, 2, 8, 9, 25].

2020 Mathematics Subject Classification: Primary 16T25; Secondary 17D99, 08A05.
Keywords: Yang–Baxter equation, braces, indecomposable solutions, primitive solutions, diagonal map, Dehornoy class.

The first and most famous result on decomposability is the 1996 conjecture of Gateva-Ivanova, proved by Rump in 2005 [23]: a *square-free* solution (i.e., satisfying $r(x,x) = (x,x)$ for all x) is decomposable. In general, a solution needs not be square-free; however, the *diagonal map*

$$T : x \mapsto \tau_x^{-1}(x)$$

always defines a permutation on X, satisfying

$$r(T(x),x) = (T(x),x).$$

The permutation T splits X into orbits. This induces a partition of $n = |X|$, which we call the *T-partition* of (X,r) and denote by $\mathcal{P}_T = \mathcal{P}_T(X,r)$. Two recent papers [3,22] revealed that this simple numerical datum may suffice to determine the (in)decomposability of a solution:

- $\mathcal{P}_T = (1,\dots,1) \ \Rightarrow\ (X,r)$ decomposable (Rump's theorem, Theorem 1 in [23]);
- $\mathcal{P}_T = (n-1,1) \ \Rightarrow\ (X,r)$ decomposable (Theorem 3.10 in [22]);
- $\mathcal{P}_T = (n-2,1,1)$, n odd $\ \Rightarrow\ (X,r)$ decomposable (Theorem 3.13 in [22]);
- $\mathcal{P}_T = (n-3,1,1,1)$, $3 \nmid n \ \Rightarrow\ (X,r)$ decomposable (Theorem 3.13 in [22]);
- more generally, $\gcd(|T|,n) = 1 \ \Rightarrow\ (X,r)$ decomposable (Camp-Mora–Sastriques (CMS) theorem, Theorem A in [3]);
- $\mathcal{P}_T = (n) \ \Rightarrow\ (X,r)$ indecomposable (Theorem 3.5 in [22]).

In this paper, we give a short and elementary proof of the CMS theorem (which was originally proved using advanced group theory), and present several original decomposability results. To explain them, we need the *structure group* of our solution (X,r), see [16]. It is defined by the following presentation:

$$G(X,r) = \langle X \mid xy = \sigma_x(y)\,\tau_y(x) \ \text{ for all } x,y \in X\rangle.$$

It carries a second, commutative operation $+$, satisfying the following compatibility relation:

$$a(b+c) = ab - a + ac. \tag{1.1}$$

Such ring-like structures are called *braces*. They are extensively used in order to bring ring-theoretic tools into the study of the Yang–Baxter equation: see [24] and references thereto. In the present work, we will employ braces in a very different way. Namely, given a positive integer k, consider the map

$$\begin{aligned} \iota^{(k)} : X &\to G(X,r), \\ x &\mapsto kx := x + \cdots + x \ (k \text{ summands}). \end{aligned}$$

Theorem A. *Take a solution (X,r) and a positive integer k. The map $\iota^{(k)}$ above is injective. Its image is a sub-solution of $G(X,r)$.*

Here the solution r is extended from X to $G(X,r)$ in the usual way. A push-back through $\iota^{(k)}$ then defines a new solution on X, called the *k-cabled solution* $r^{(k)}$. Equation (2.2) describes it explicitly. Some relations between a solution and its cablings are given in the following result.

Theorem B. *Take a solution (X, r) and a positive integer k.*

(1) *The diagonal map of $(X, r^{(k)})$ is T^k.*

(2) *Let $x \in X$ lie in a $\mathcal{G}(X, r)$-orbit of size m, and in a $\mathcal{G}(X, r^{(k)})$-orbit of size m'. Then m' is a multiple of the maximal divisor m_k of m which is coprime to k: $m_k \mid m$ and $\gcd(m_k, k) = 1$.*

In particular, if the solution (X, r) is indecomposable and $\gcd(|X|, k) = 1$, then $(X, r^{(k)})$ remains indecomposable (since $|X|_k = |X|$). Taking $k = |T|$, we then reduce the CMS theorem to Rump's result. On the other hand, taking $k = p$, $k = a$, and $k = 2$ respectively, we obtain new decomposability theorems:

Theorem C. *Take an indecomposable solution (X, r) of size pq, where $p \neq q$ are prime numbers. Then its T-partition cannot contain a term s satisfying $(p-1)q < s < pq$ and $\gcd(s, p) = 1$.*

For instance, for $|X| = 14$, this excludes cycles of size 9, 11 and 13, and for $|X| = 15$, this excludes cycles of size 11, 13 and 14.

Theorem D. *Take an indecomposable solution (X, r) of size ab and T-partition (a, c, c'), where the numbers a, b, c and c' are pairwise coprime, except for, possibly, c and c'. Then one cannot have $b > a + c$.*

As a consequence, indecomposable solutions (X, r) of size $2b$ with odd $b \geq 5$ cannot have T-partition $(2, b-4, b+2)$.

Theorem E. *Take an indecomposable solution (X, r) of size $2d$, where d is odd, with T-partition $(2a, b, c)$, where $\gcd(2d, abc) = 1$ and $b \leq c$. Then $2a + b = c$.*

For instance, for $|X| = 18$ this excludes the T-partition $(10, 7, 1)$, and for $|X| = 22$ this excludes the T-partitions $(10, 9, 3)$, $(10, 7, 5)$, and $(6, 7, 9)$. Neither of these are covered by Theorems C and D.

In parallel with its decomposition into T-cycles, a solution carries several other relevant decompositions: into imprimitivity blocks, and also into $\mathcal{G}(X, r^{(k)})$-orbits (for well chosen k). Comparing them, and using the recent classification of primitive solutions from [11], we obtain the following.

Theorem F. *Take an indecomposable solution (X, r) of size pq, with $p < q$ prime. Then its T-partition contains either only multiples of q, or at least one multiple of p.*

In particular, for an indecomposable solution of size $n = 2q$, with q an odd prime, the only possible T-partition with only odd terms is (q, q).

More generally, Theorem B allows one to considerably reduce the list of possible T-partitions for indecomposable solutions. This has the potential to speed up algorithms constructing all indecomposable solutions of small size.

In another vein, cabling can produce new indecomposable solutions out of old ones: see Example 4.2.

In the final part of the paper, cabling and brace ideas are used to explore an important invariant of a solution (X, r), which we propose to call its *Dehornoy class*. It is the smallest

positive integer m such that

$$\forall x \in X, \quad \sigma_{T^{m-1}(x)} \cdots \sigma_{T(x)} \sigma_x = \mathrm{Id}. \tag{1.2}$$

Such an m always exists, and is $< (n^2)!$. The elements mx, $x \in X$, then generate a normal free abelian subgroup of $G(X,r)$ of finite index. The corresponding finite quotient plays the same role as Coxeter groups play for Artin groups. In particular, it suffices for reconstructing the Garside structure on the whole $G(X,r)$. For details, see [14, 15]. A partial generalisation to non-involutive solutions is proposed in [21].

The permutation group $\mathcal{G}(X,r)$ inherits the brace structure from $G(X,r)$, see [10]. We then give a new conceptual interpretation of the Dehornoy class in terms of the abelian group $(\mathcal{G}(X,r),+)$:

Theorem G. *The Dehornoy class m of a solution (X,r) is the least common multiple of the orders of the generators σ_x, $x \in X$, of the group $(\mathcal{G}(X,r),+)$. If the solution is indecomposable, m is the order of any σ_x.*

Another type of problems where cabling can be useful is the structural study of braces. Since these questions are out of the focus of the present work, we simply illustrate this approach with a quick proof of two important properties of finite braces at the end of Section 3.

2. Cabling a solution

In this section, we prove Theorem A.

Recall that, with respect to the operation $+$, $G(X,r)$ is a free abelian group, and the elements $x \in X$ yield its basis [24]. Therefore the map $\iota^{(k)}$ is injective.

To get the second assertion of the theorem, we will prove an explicit formula for the extension R of r to $G(X,r)$:

$$R(kx, ly) = (l\sigma_{kx}(y), k\, T^{k-1}\, \tau_{ly}\, T^{-k+1}(x)), \tag{2.1}$$

where k and l are positive integers. This yields

$$r^{(k)}(x,y) = (\sigma_{kx}(y), T^{k-1}\, \tau_{ky}\, T^{-k+1}(x)), \tag{2.2}$$

and finishes the proof of Theorem A.

Recall that the operation $+$ on $G(X,r)$ is a natural extension of the law

$$x + y = x\sigma_x^{-1}(y), \quad x, y \in X.$$

In particular,

$$kx = x\, U(x)\, U^2(x) \cdots U^{k-1}(x), \tag{2.3}$$

where

$$U : x \mapsto \sigma_x^{-1}(x)$$

is the inverse of the diagonal map T. One recognises the frozen words from [14] (for $k = 2$), and the twisted powers $x^{[k]}$ from [15] (for general k).

Let us look at

$$r_{k,l}(x\, U(x)\, U^2(x) \cdots U^{k-1}(x)\ ,\ y\, U(y)\, U^2(y) \cdots U^{l-1}(y)) = (\overline{u}, \overline{w}), \tag{2.4}$$

where the tuples $(x_1, \dots, x_s)$ are denoted by $x_1 \cdots x_s$ for simplicity, and the solution r is extended, this time, to the powers of X:

$$r_{k,l} = (r_l \cdots r_1) \cdots (r_{k+l-2} \cdots r_{k-1})(r_{k+l-1} \cdots r_k) : X^k \times X^l \to X^l \times X^k.$$

These maps induce the solution R on $G(X, r)$, as explained in [18] with an inductive argument, and in [20] with a graphical argument. Both entries in (2.4) are *frozen* tuples, that is, they remain unchanged when r is applied to any neighbouring positions, since $r(z, U(z)) = (z, U(z))$ for all $z \in X$. But the Yang–Baxter equation for r guarantees that

$$r_i\, r_{k,l} = \begin{cases} r_{k,l}\, r_{k+i} & \text{if } 1 \le i \le l-1, \\ r_{k,l}\, r_{i-l} & \text{if } l+1 \le i \le l+k-1. \end{cases}$$

Here r_i is the solution r applied at the positions i and $i+1$ of a tuple. As a result, $\overline{u}$ and $\overline{w}$ are also frozen:

$$\overline{u} = y' U(y') \cdots U^{l-1}(y') = ly', \qquad \overline{w} = x' U(x') \cdots U^{k-1}(x') = kx'.$$

Thus $R(kx, ly) = (ly', kx')$. Further, (2.4) implies

$$\begin{aligned} y' &= \sigma_{x\, U(x)\, U^2(x) \cdots U^{k-1}(x)}(y) = \sigma_{kx}(y), \\ U^{k-1}(x') &= \tau_{y\, U(y)\, U^2(y) \cdots U^{l-1}(y)}\, U^{k-1}(x) = \tau_{ly}\, U^{k-1}(x), \end{aligned}$$

and hence

$$x' = U^{-k+1}\, \tau_{ly}\, U^{k-1}(x) = T^{k-1}\, \tau_{ly}\, T^{-k+1}(x),$$

as announced.

3. Properties of cabled solutions

In this section, we first prove Theorem B, and then turn to other properties of cabled solutions.

Proof of Theorem B. For all positive integer k and $x \in X$, the tuple

$$x\, U(x)\, U^2(x) \cdots U^{2k-1}(x) \in X^{2k}$$

is frozen. Since applying the solution $r_{k,k}$ to a $2k$-tuple boils down to applying r repeatedly at different positions, one gets

$$\begin{aligned} r_{k,k}\big(x U(x) U^2(x) \cdots U^{k-1}(x),\, U^k(x) U^{k+1}(x) \cdots U^{2k-1}(x)\big) \\ = \big(x\, U(x)\, U^2(x) \cdots U^{k-1}(x),\, U^k(x)\, U^{k+1}(x) \cdots U^{2k-1}(x)\big). \end{aligned}$$

In other words,

$$R(kx, kU^k(x)) = (kx, kU^k(x)),$$

that is,

$$r^{(k)}(x, U^k(x)) = (x, U^k(x)).$$

Since T is the inverse of U, this yields

$$r^{(k)}(T^k(x), x) = (T^k(x), x).$$

Therefore, T^k is the diagonal map for $r^{(k)}$.

Now let $x \in X$ lie in the $\mathcal{G}(X,r)$-orbit of size m and in the $\mathcal{G}(X,r^{(k)})$-orbit of size m'. Denote by $\mathcal{G}(X,r)_x$ and $\mathcal{G}(X,r^{(k)})_x$ their stabilisers in the two groups. One has

$$|\mathcal{G}(X,r)| = m\,|\mathcal{G}(X,r)_x| \quad \text{and} \quad |\mathcal{G}(X,r^{(k)})| = m'\,|\mathcal{G}(X,r^{(k)})_x|.$$

The permutation groups $\mathcal{G}(X,r)$ and $\mathcal{G}(X,r^{(k)})$ inherit brace structures from the corresponding structure groups $G(X,r)$ and $G(X,r^{(k)})$ (see [10]). Moreover, the abelian group $(\mathcal{G}(X,r^{(k)}),+)$ is obtained from the abelian group $(\mathcal{G}(X,r),+)$ by multiplying each of its generators σ_x, $x \in X$, by k. Thus its size is the size of $(\mathcal{G}(X,r),+)$ divided by some product $p_1^{d_1}\cdots p_l^{d_l}$ of powers of prime divisors of k. Also, since the permutation group $\mathcal{G}(X,r^{(k)})$ is the subgroup of $\mathcal{G}(X,r)$ generated by the permutations σ_{kx}, $x \in X$, the stabiliser $\mathcal{G}(X,r^{(k)})_x$ is a subgroup of $\mathcal{G}(X,r)_x$. Hence

$$|\mathcal{G}(X,r^{(k)})_x| = \frac{|\mathcal{G}(X,r)_x|}{t}$$

for some positive integer t. Summarising, we obtain

$$m' = \frac{|\mathcal{G}(X,r^{(k)})|}{|\mathcal{G}(X,r^{(k)})_x|} = \frac{|\mathcal{G}(X,r)|\,/\,(p_1^{d_1}\cdots p_l^{d_l})}{|\mathcal{G}(X,r)_x|\,/\,t} = \frac{mt}{p_1^{d_1}\cdots p_l^{d_l}}.$$

Since this fraction is an integer, it is a multiple of an integer of the form $m/(p_1^{d_1'}\cdots p_l^{d_l'})$. Recalling that the p_i are prime divisors of k, we see that $m/(p_1^{d_1'}\cdots p_l^{d_l'})$ is a multiple of the maximal divisor m_k of m which is coprime to k, as announced. ∎

Proposition 3.1. *The iteration of cablings remains a cabling. More precisely, given a solution (X,r) and positive integers k and k', one has*

$$(r^{(k)})^{(k')} = r^{(kk')}.$$

Proof. Formula (2.2) implies

$$(r^{(k)})^{(k')}(x,y) = (\sigma_{k'kx}(y),\cdot) \quad \text{and} \quad r^{(kk')}(x,y) = (\sigma_{kk'x}(y),\cdot).$$

Recall the relation

$$T\sigma_x = \tau_x^{-1} T \tag{3.1}$$

connecting the σ's and the τ's (see for instance Proposition 2.2 in [16]). It implies that the σ-component uniquely determines a solution. We are done. ∎

Recall that a solution (X,r) is called *retractable* if, for some $x \neq x' \in X$, one has $\sigma_x = \sigma_{x'}$ (and hence $\tau_x = \tau_{x'}$). Identifying all such x and x', one gets the *retraction* $\mathrm{Ret}(X,r)$ of (X,r); it is a solution again, as explained in [16]. This is an important property of solutions: see [17] and references thereto.

Proposition 3.2. *If a solution (X, r) is retractable, then so are all its cablings. More precisely,* $\mathrm{Ret}(X, r^{(k)})$ *is a quotient of* $\mathrm{Ret}(X, r)^{(k)}$ *for all positive integers k.*

Proof. Using the brace structure $\mathcal{G}(X, r)$ inherits from $G(X, r)$, we can write $\sigma_{kx} = k\sigma_x$. Thus the relation $\sigma_x = \sigma_{x'}$ implies $\sigma_{kx} = \sigma_{kx'}$. From (2.2), one then concludes that elements x and x' identified in $\mathrm{Ret}(X, r)$ are necessarily identified in $\mathrm{Ret}(X, r^{(k)})$ as well. ∎

Until now, all connections between solutions and braces that we used went through the brace structures on the structure and permutation groups of a solution. But one can go the other way round, and define a solution on any brace [24]. This gives one the intuition on how to cable a brace. Concretely, take a brace $(B, +, \circ)$ and a positive integer k. The elements ka, $a \in B$, form a sub-brace $B^{(k)}$ of B, called its *k-cabling*. Indeed, we have

$$\begin{aligned} ka + kb &= k(a + b), \\ ka \circ kb &= k((ka) \circ b - (k-1)a), \end{aligned}$$

as follows from the commutativity of $+$ and from relation (1.1), respectively. The additive structure of $B^{(k)}$ is obtained from $(B, +)$ by multiplication by k. One can thus easily determine its size. The multiplicative group $(B, \circ)$ then has a subgroup of the same size. Here are two direct applications:

(1) A quick proof of the solvability of the multiplicative group of a finite brace (first established in Theorem 2.15 of [16]). Indeed, let $(B, +, \circ)$ be a brace of size ab with $\gcd(a, b) = 1$. Looking at the additive structure, one sees that $B^{(a)}$ is of size b. Therefore $(B^{(a)}, \circ)$ is a b-Hall subgroup of $(B, \circ)$. Thus $(B, \circ)$ is solvable.

(2) Let B be a finite brace with cyclic additive group, and let d be a divisor of its size $|B|$. Then $(B, \circ)$ contains a subgroup of size d. Indeed, looking at the additive structure and using the cyclicity of $(B, +)$, one sees that $B^{(|B|/d)}$ is of size d.

4. Applications: (in)decomposability results

We now turn to applications of Theorem B. Its assertion is particularly transparent when the solution (X, r) is indecomposable, and the cabling parameter k is coprime to its size $|X|$, which is now the size of the only $\mathcal{G}(X, r)$-orbit. Since $|X|_k = |X|$, the theorem implies that the solution $(X, r^{(k)})$ remains indecomposable, with diagonal map T^k. Here are some interesting particular cases.

(1) If $\gcd(|T|, |X|) = 1$, then $(X, r^{(|T|)})$ has to be indecomposable, with diagonal map Id, which is impossible by Rump's theorem. We thus recover the Camp-Mora–Sastriques (CMS) theorem.

(2) If the cycle decompositions of T and T^k are different, we get a new indecomposable solution on the same set X. For instance, if (X, r) is the indecomposable solution with T-partition $(2, 6)$ (cf. Table 3.2 in [22]), we have $|X| = 2 + 6 = 8$, which is comprime with $k = 3$. Then $(X, r^{(3)})$ is an indecomposable solution with T-partition $(2, 2, 2, 2)$, and hence not isomorphic to (X, r).

To treat other cases, we need the following elementary observation.

Lemma 4.1. *Given a solution (X, r) with diagonal map T, any T-orbit in X lies entirely within a single $\mathcal{G}(X, r)$-orbit.*

Proof. Take an element $x \in X$ from a $\mathcal{G}(X, r)$-orbit Y. By [16], r restricts to $Y \times Y$ and defines a solution on Y. The diagonal map of this restricted solution has to be the restriction of T to Y. Thus the T-orbit of x lies entirely within Y. ∎

Now, take an indecomposable solution (X, r) and a cabling parameter k which is not coprime to $|X|$, but which makes $|X|_k$ big enough. Then the sizes of all $\mathcal{G}(X, r^{(k)})$-orbits are multiples of $|X|_k$. On the other hand, by the above lemma, all the T^k-orbits lie entirely inside these $\mathcal{G}(X, r^{(k)})$-orbits. In several cases, for numerical reasons, this can happen only when there is only one $\mathcal{G}(X, r^{(k)})$-orbit. The solution $(X, r^{(k)})$ is then indecomposable, which imposes some constraints on the sizes of the T^k-orbits, for instance by the CMS theorem. This leads to a contradiction in various cases which are not themselves covered by the CMS theorem. Here are some of them.

(1) Take an indecomposable solution (X, r) of size pq, where $p \neq q$ are primes. Assume that a T-orbit is of size $(p-1)q < s < pq$, with $\gcd(s, p) = 1$. We will show that this is impossible, and thus we shall prove Theorem C. For any $t \in \mathbb{N}$, the diagonal map T^{p^t} of $(X, r^{(p^t)})$ inherits this orbit, since $\gcd(s, p) = 1$. Thus this T^{p^t}-orbit of size s lies entirely within a $\mathcal{G}(X, r^{(p^t)})$-orbit, whose size is a multiple of $|X|_{p^t} = q$. Since $(p-1)q < s < pq$, this $\mathcal{G}(X, r^{(p^t)})$-orbit has to be the whole set X. In other words, the p^t-cabled solution $(X, r^{(p^t)})$ is indecomposable. But, for t big enough, the sizes of all T^{p^t}-orbits are coprime to p. But they are also coprime to q since there is one orbit of size $(p-1)q < s < pq$ and several smaller orbits of total size $pq - s < q$. As a consequence, $\gcd(|X|, |T^{p^t}|) = \gcd(pq, |T^{p^t}|) = 1$. By the CMS theorem, the solution $(X, r^{(p^t)})$ is then decomposable, contradiction.

(2) Take an indecomposable solution (X, r) of size ab and T-partition (a, c, c'), where $b > a + c$, and the numbers a, b, c, c' are pairwise coprime, except for, possibly, c and c'. We will show that this is impossible, and thus we shall prove Theorem D. The a-cabling of (X, r) has T-partition $(c, c', 1, \dots, 1)$, with a ones. Since $\gcd(|X|, |T^a|)$ divides $\gcd(ab, cc') = 1$, the CMS theorem says that $(X, r^{(a)})$ is decomposable, and that there are at least two $\mathcal{G}(X, r^{(a)})$-orbits. One of them does not contain the T^a-orbit of size c', hence its size is $\leq c + a < b$, which is impossible for a multiple of $|X|_a = |ab|_a = b$.

(3) Take an indecomposable solution (X, r) of size $2d$, with d odd, and T-partition $(2a, b, c)$, where $\gcd(2d, abc) = 1$ and $b \leq c$. We will show that this imposes heavy restrictions on a, b, c, and thus we shall prove Theorem E. The 2-cabling of (X, r) has T-partition (a, a, b, c), since b and c are odd. The sizes of its $\mathcal{G}(X, r^{(2)})$-orbits are multiples of $(2d)_2 = d$, as d is odd. Since $\gcd(|X|, |T^2|)$ divides $\gcd(2d, abc) = 1$, the CMS theorem says that $(X, r^{(2)})$ is decomposable, so there are precisely two $\mathcal{G}(X, r^{(2)})$-orbits, each of size d. Each of the four T^2-orbits lies entirely in one of these two $\mathcal{G}(X, r^{(2)})$-orbits. Since the numbers a, b, c and d are all odd, this is possible only if $d = 2a + b = c$.

(4) Assume that (X, r) is an indecomposable solution of size 30. We will show that its T-partition cannot be $(21, 7, 1, 1)$. Indeed, the 3-cabled solution $(X, r^{(3)})$ would then have T-partition $(7, 7, 7, 7, 1, 1)$, and would be decomposable by the CMS theorem. On the other hand, its $\mathcal{G}(X, r^{(3)})$-orbits are multiples of $30_3 = 10$. However, the only way to divide the multiset $(7, 7, 7, 7, 1, 1)$ into parts whose total sums are all divisible by 10 is to take the whole multiset. Thus the solution $(X, r^{(3)})$ is indecomposable, contradiction. As in the above situations, this example generalises to an infinite family.

In another vein, cabling can produce new indecomposable solutions out of old ones.

Example 4.2. Consider the indecomposable solution (X, r) (found by a computer), where $X = \{1, \dots, 8\}$, $r(x, y) = (\sigma_x(y), \sigma^{-1}_{\sigma_x(y)}(x))$, and

$$\sigma_1 = (12)(34)(56)(78), \quad \sigma_2 = (12)(36)(47)(58), \quad \sigma_3 = (1543)(2678),$$
$$\sigma_4 = (1367)(2854), \quad \sigma_5 = (17)(24)(38)(56), \quad \sigma_6 = (1763)(2458),$$
$$\sigma_7 = (1345)(2876), \quad \sigma_8 = (15)(26)(38)(47).$$

Its diagonal map is

$$T = (12)(345678),$$

so its T-partition is $(2, 6)$. According to Theorem B, its 3-cabling $(X, r^{(3)})$ is still indecomposable (as $\gcd(3, 8) = 1$) and has T-partition $(2, 2, 2, 2)$. It is thus not isomorphic to (X, r).

5. Primitivity and further (in)decomposability results

A solution (X, r) is called *imprimitive* if the $\mathcal{G}(X, r)$-action on X is so, and *primitive* otherwise. That is, an imprimitive solution X admits a non-trivial decomposition into blocks which is preserved by the $\mathcal{G}(X, r)$-action. A recent result from [11] asserts that, up to isomorphism, the only primitive solutions are the permutation solutions $(\mathbb{Z}/p\mathbb{Z},\ r(a, b) = (b - 1, a + 1))$, with p prime. By [16], these are the only indecomposable solutions of prime size. Thus, in the interesting case of non-prime size, an indecomposable solution can be split into imprimitivity blocks. Their interaction with T-cycles is quite intricate. We will now analyse this interaction in the particular settings of Theorem F, and deduce a proof of that theorem.

Consider an indecomposable solution (X, r) of size pq, with primes $p < q$. Assume that its T-partition contains no multiples of p, and at least one term which is not a multiple of q. We will obtain a contradiction, proving Theorem F.

By Theorem B, one can choose a suitable k coprime with pq such that the solution $(X, r^{(k)})$ is still indecomposable, has T-partition with all terms of the form $p^\alpha q^\beta$, and permutation group $\mathcal{G}(X, r^{(k)})$ of size $p^a q^b$. (For the latter property, recall that the k-cabling multiplies all the elements of $(\mathcal{G}(X, r), +)$ by k.) Since the cabling can only split T-orbits into equal parts, the T-partition of $(X, r^{(k)})$ still contains no multiples of p, and at least one term which is not a multiple of q. Thus it suffices to work with solutions having these properties.

Summarizing all the constraints on the T-partition we obtained, one sees that it has to be of the form $(q, \dots, q, 1, \dots, 1)$, with at least one term 1 and one term q (otherwise Rump's theorem applies).

Since pq is not prime, our solution is imprimitive. Thus X non-trivially decomposes into blocks preserved by the $\mathcal{G}(X, r)$-action. Since (X, r) is indecomposable, $\mathcal{G}(X, r)$ permutes these blocks in a transitive manner, hence they are all of the same size. This leaves us with two possibilities.

Case 1. There are p blocks of size q.

Since our solution is indecomposable, some map σ_x permutes $1 < p' \leq p$ blocks in a cyclic manner. It thus has an orbit of size $p'q'$, with $1 \leq q' \leq q$. Since this size is of the form $p^\alpha q^\beta$ (the group $\mathcal{G}(X, r)$ having the size of this form), and since $p < q$ are primes, one necessarily has $p' = p$. Thus σ_x permutes all the p blocks in a cyclic manner. As a result, x and $U(x) = \sigma_x^{-1}(x)$ lie in different blocks. Since $U = T^{-1}$, one obtains a T-cycle which does not entirely lie in a single block. Now, again by Theorem B, one can choose a suitable m such that the solution $(X, r^{(p^m)})$ is decomposable, with orbits whose sizes are multiples of q. The permutation group $\mathcal{G}(X, r^{(p^m)})$ is a subgroup of the group $\mathcal{G}(X, r)$ of size $p^a q^b$. Its size, as well as the sizes of all the $\mathcal{G}(X, r^{(p^m)})$-orbits, are then of the same form. Being multiples of q, the sizes of the $\mathcal{G}(X, r^{(p^m)})$-orbits are then all precisely q. One of them has to entirely contain our T-cycle of size q (which is also a $T^{(p^m)}$-cycle). This $\mathcal{G}(X, r^{(p^m)})$-orbit then intersects several blocks. Since the subgroup $\mathcal{G}(X, r^{(p^m)})$ of $\mathcal{G}(X, r)$ permutes these blocks, our $\mathcal{G}(X, r^{(p^m)})$-orbit has to be of size $p'q'$, with $1 < p' \leq p$ and $1 \leq q' \leq q$. But q cannot be written in this way.

Case 2. There are q blocks of size p.

The permutations τ_x of X, for $x \in X$, generate a transitive group, since so do the σ_x, and the two are related by the conjugation by T (see relation (3.1)). Therefore some element $f \in X$ fixed by T is moved to an element c from a T-cycle of size q by some τ_x. That is, $c = \tau_x(f)$. We will use the relation

$$T(\tau_x(f)) = \tau_{\sigma_f(x)}(f)$$

from Lemma 3.8 in [22]. Applied k times, it yields

$$T^k(c) = \tau_{\sigma_f^k(x)}(f).$$

As a result, the size of the σ_f-orbit containing x is a multiple of the size of the T-orbit containing c, which is q. Since $p < q$, it intersects $q' > 1$ blocks of size p. On the other hand, since σ_f fixes f, it fixes at least one block. Thus $q' < q$. Summarizing, the size q of our orbit decomposes as $p'q'$, with $1 \leq p' \leq p$ and $1 < q' < q$. But this is impossible.

Remark 5.1. Along the lines of the proof of Lemma 3.8 in [22], one can establish the relation

$$T^k(\tau_x(y)) = \tau_{\sigma_{k_y}(x)}(T^k(y)),$$

valid for all $x, y \in X$ (not necessarily T-fixed) and all k.

6. Applications: Dehornoy class

In this section, we will prove Theorem G. The main ingredient is:

Lemma 6.1. *For all elements x from the same $\mathcal{G}(X,r)$-orbit of a solution (X,r), the order of σ_x in the finite abelian group $(\mathcal{G}(X,r),+)$ is the same.*

Proof. Relation (2.1) specialised at $k=1$ yields the relation

$$\sigma_x(ly) = l\sigma_x(y) \tag{6.1}$$

in the structure group $G(X,r)$. In its quotient $\mathcal{G}(X,r)$, it becomes

$$\sigma_{\sigma_x}(l\sigma_y) = l\sigma_{\sigma_x(y)}.$$

Thus $l\sigma_y$ vanishes if and only if $l\sigma_{\sigma_x(y)}$ does. As a consequence, σ_y and $\sigma_{\sigma_x(y)}$ have the same order in $(\mathcal{G}(X,r),+)$ for all $x,y\in X$. ∎

Remark 6.2. Relation (6.1) means that the cabling operation $\iota^{(l)}\colon x\mapsto lx$ is equivariant with respect to the left $G(X,r)$-actions induced by the maps σ_x. It thus behaves better than the diagonal map T, which instead of the equivariance obeys the less tractable rule (3.1).

Proof of Theorem G. Relation (1.2) can be rewritten as

$$\forall x\in X,\quad \sigma_x\sigma_{U(x)}\cdots\sigma_{U^{m-1}(x)} = \mathrm{Id},$$

which, by (2.3), simply means $m\sigma_x = 0$. This yields the first assertion of the theorem. The second then directly follows from Lemma 6.1. ∎

We finish with the following observation, relating the Dehornoy class of a solution to its diagonal map:

Proposition 6.3. *Let (X,r) be a solution. Then the order $|T|$ of its diagonal map divides its Dehornoy class m.*

Proof. We need to prove the relation $T^m=\mathrm{Id}$, or, equivalently, $U^m=\mathrm{Id}$. Let us compute

$$r_{m,1}(xU(x)U^2(x)\cdots U^{m-1}(x), U^m(x)) \tag{6.2}$$

in two ways. On the one hand, the definition of the Dehornoy class allows one to simplify (6.2) as

$$r_{m,1}(mx, U^m(x)) = (\sigma_{mx}(U^m(x)),\cdot) = ((m\sigma_x)(U^m(x)),\cdot) = (U^m(x),\cdot).$$

On the other hand, since the tuple $xU(x)U^2(x)\cdots U^m(x)$ is frozen, (6.2) equals

$$(x, U(x)U^2(x)\cdots U^{m-1}(x)U^m(x)).$$

Hence $U^m(x)=x$ for all $x\in X$. ∎

Acknowledgements. The authors are grateful to Arpan Kanrar who suggested a stronger version of Theorem E, and to the reviewers for a thorough reading of the paper.

Funding. This work was partially supported by Conicet and the project OZR3762 of Vrije Universiteit Brussel.

References

[1] Bachiller, D., Cedó, F., Jespers, E. and Okniński, J.: Iterated matched products of finite braces and simplicity; new solutions of the Yang–Baxter equation. *Trans. Amer. Math. Soc.* **370** (2018), no. 7, 4881–4907.

[2] Bachiller, D., Cedó, F., Jespers, E. and Okniński, J.: Asymmetric product of left braces and simplicity; new solutions of the Yang–Baxter equation. *Commun. Contemp. Math.* **21** (2019), no. 8, article no. 1850042, 30 pp.

[3] Camp-Mora, S. and Sastriques, R.: A criterion for decomposabilty in QYBE. *Int. Math. Res. Not. IMRN* (2023), no. 5, 3808–3813.

[4] Castelli, M.: Classification of uniconnected involutive solutions of the Yang–Baxter equation with odd size and a Z-group permutation group. To appear in *Int. Math. Res. Not. IMRN*, DOI: 10.1093/imrn/rnac185.

[5] Castelli, M., Catino, F. and Pinto, G.: Indecomposable involutive set-theoretic solutions of the Yang–Baxter equation. *J. Pure Appl. Algebra* **223** (2019), no. 10, 4477–4493.

[6] Castelli, M., Mazzotta, M. and Stefanelli, P.: Simplicity of indecomposable set-theoretic solutions of the Yang–Baxter equation. *Forum Math.* **34** (2022), no. 2, 531–546.

[7] Castelli, M., Pinto, G. and Rump, W.: On the indecomposable involutive set-theoretic solutions of the Yang–Baxter equation of prime-power size. *Comm. Algebra* **48** (2020), no. 5, 1941–1955.

[8] Catino, F., Colazzo, I. and Stefanelli, P.: The matched product of set-theoretical solutions of the Yang–Baxter equation. *J. Pure Appl. Algebra* **224** (2020), no. 3, 1173–1194.

[9] Catino, F., Colazzo, I. and Stefanelli, P.: The matched product of the solutions to the Yang–Baxter equation of finite order. *Mediterr. J. Math.* **17** (2020), no. 2, article no. 58, 22 pp.

[10] Cedó, F., Jespers, E. and Okniński, J.: Braces and the Yang–Baxter equation. *Comm. Math. Phys.* **327** (2014), no. 1, 101–116.

[11] Cedó, F., Jespers, E. and Okniński, J.: Primitive set-theoretic solutions of the Yang–Baxter equation. *Commun. Contemp. Math.* **24** (2022), no. 9, article no. 2150105, 10 pp.

[12] Cedó, F. and Okniński, J.: Constructing finite simple solutions of the Yang–Baxter equation. *Adv. Math.* **391** (2021), article no. 107968, 40 pp.

[13] Cedó, F. and Okniński, J.: New simple solutions of the Yang–Baxter equation and solutions associated to simple left braces. *J. Algebra* **600** (2022), 125–151.

[14] Chouraqui, F. and Godelle, E.: Finite quotients of groups of I-type. *Adv. Math.* **258** (2014), 46–68.

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

[16] Etingof, P., Schedler, T. and Soloviev, A.: Set-theoretical solutions to the quantum Yang–Baxter equation. *Duke Math. J.* **100** (1999), no. 2, 169–209.

[17] Gateva-Ivanova, T. and Cameron, P.: Multipermutation solutions of the Yang–Baxter equation. *Comm. Math. Phys.* **309** (2012), no. 3, 583–621.

[18] Gateva-Ivanova, T. and Majid, S.: Matched pairs approach to set theoretic solutions of the Yang–Baxter equation. *J. Algebra* **319** (2008), no. 4, 1462–1529.

[19] Gateva-Ivanova, T. and Van den Bergh, M.: Semigroups of I-type. *J. Algebra* **206** (1998), no. 1, 97–112.

[20] Lebed, V. and Vendramin, L.: Homology of left non-degenerate set-theoretic solutions to the Yang–Baxter equation. *Adv. Math.* **304** (2017), 1219–1261.

[21] Lebed, V. and Vendramin, L.: On structure groups of set-theoretic solutions to the Yang–Baxter equation. *Proc. Edinb. Math. Soc. (2)* **62** (2019), no. 3, 683–717.

[22] Ramírez, S. and Vendramin, L.: Decomposition theorems for involutive solutions to the Yang–Baxter equation. *Int. Math. Res. Not. IMRN* (2022), no. 22, 18078–18091.

[23] Rump, W.: A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation. *Adv. Math.* **193** (2005), no. 1, 40–55.

[24] Rump, W.: Braces, radical rings, and the quantum Yang–Baxter equation. *J. Algebra* **307** (2007), no. 1, 153–170.

[25] Rump, W.: Semidirect products in algebraic logic and solutions of the quantum Yang–Baxter equation. *J. Algebra Appl.* **7** (2008), no. 4, 471–490.

[26] Rump, W.: Classification of indecomposable involutive set-theoretic solutions to the Yang–Baxter equation. *Forum Math.* **32** (2020), no. 4, 891–903.

[27] Rump, W.: One-generator braces and indecomposable set-theoretic solutions to the Yang–Baxter equation. *Proc. Edinb. Math. Soc. (2)* **63** (2020), no. 3, 676–696.

[28] Rump, W.: Uniconnected solutions to the Yang–Baxter equation arising from self-maps of groups. *Canad. Math. Bull.* **65** (2022), no. 1, 225–233.

[29] Smoktunowicz, A. and Smoktunowicz, A.: Set-theoretic solutions of the Yang–Baxter equation and new classes of R-matrices. *Linear Algebra Appl.* **546** (2018), 86–114.

Received September 23, 2022; revised June 16, 2023. Published online July 12, 2023.

Victoria Lebed
Normandie Univ, UNICAEN, CNRS, LMNO, 14000 Caen, France;
victoria.lebed@unicaen.fr

Santiago Ramírez
IMAS–CONICET and Departamento de Matemática, FCEN, Universidad de Buenos Aires, Pabellón 1, Ciudad Universitaria, C1428EGA, Buenos Aires, Argentina;
sramirez@dm.uba.ar

Leandro Vendramin
Department of Mathematics and Data Science, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussel, Belgium;
Leandro.Vendramin@vub.be