COXETER-LIKE GROUPS FOR GROUPS OF SET-THEORETIC SOLUTIONS OF THE YANG–BAXTER EQUATION

PATRICK DEHORNOY

Abstract. We attach with every finite, involutive, nondegenerate set-theoretic solution of the Yang–Baxter equation a finite group that plays for the associated structure group the sale role as a finite Coxeter group plays for the associated Artin–Tits group.

1. Introduction

A *set-theoretic solution of the Yang–Baxter equation* (YBE) is a pair (X, R) where R is a bijection from X^2 to itself satisfying $R^{12}R^{23}R^{12} = R^{23}R^{12}R^{23}$, in which $R^{ij} : X^3 \to X^3$ corresponds to R acting in positions i and j. Set-theoretic solutions of YBE provide particular solutions of the (quantum) Yang–Baxter equation, and received some attention in recent years.

A set-theoretic solution (X, R) of YBE is called *involutive* for$R^2 = \mathrm{id}$, and *nondegenerate* if, writing $R(x, y) = (R_1(x, y), R_2(x, y))$, the maps $y \mapsto R_1(x, y)$ and $x \mapsto R_2(x, y)$ are one-to-one. In this case, the group (*resp.* monoid) presented by $\langle X \mid \{xy = z, t \mid x, y, z, t \in X \text{ and } R(x, y) = (z, t)\}\rangle$ is called the *structure group* (*resp. structure monoid*) of (X, R) [5].

Such structure groups happen to admit a number of alternative definitions and make an interesting family. Among others, every structure group is a *Garside group* [1], meaning that there exists a pair (M, Δ) such that M is a cancellative monoid in which left-divisibility—defined by $g \preccurlyeq h \Leftrightarrow \exists h' {\in} M (h = gh')$—is a lattice, Δ is a *Garside element* in M—meaning that the left- and right-divisors coincide, are finite in number, and generate M—and G is a group of fractions for M [3].

In the case of Artin's braid group B_n, the seminal example of a Garside group, the Garside structure (B_n^+, Δ_n) is connected with the exact sequence $1 \to P_n \to B_n \to \mathfrak{S}_n \to 1$, where P_n is the pure braid group: B_n^+ is the monoid of positive braids, the lattice made by the divisors of Δ_n in B_n^+ is isomorphic to the weak order on $\mathfrak{S}_n$. A presentation of $\mathfrak{S}_n$ is obtained by adding $n - 1$ relations $\sigma_i^2 = 1$ to the standard presentation of B_n, and the germ derived from $\mathfrak{S}_n$ and the transpositions σ_i, meaning the substructure of $\mathfrak{S}_n$ where multiplication is restricted to the cases when lengths add, generates B_n^+ [4] and its Cayley graph is the Hasse diagram of the divisors of Δ_n. The results extend to all types in the Cartan classification, connecting spherical Artin–Tits groups with the associated finite Coxeter group.

As Garside groups extend spherical type Artin–Tits groups in many respects, it is natural to ask:

Question 1.1. *Assume that G is a Garside group, with Garside structure (M, Δ). Does there exist a finite quotient W of G such that W provides a Garside germ* *for M and the Cayley graph of W with respect to the atoms of M is isomorphic to the lattice of divisors of Δ in M ?*

In other words, does every Garside group admit some Coxeter-like group? The general question remains open. The aim of this note is to establish a positive answer for structure groups of set-theoretic solutions of YBE. We attach with every such solution a number called its *class* and establish:

Theorem 1.2. *Assume that G (resp. M) is the structure group (resp. monoid) of an involutive, nondegenerate solution (X, R) of YBE with X of size n and class p. Then there exist a Garside element Δ in M and a finite group W of order p^n entering a short exact sequence $1 \to \mathbb{Z}^n \to G \to W \to 1$ such that (W, X) provides a germ for M whose Cayley graph is the Hasse diagram of the divisors of Δ in M. A presentation of W is obtained by adding n relations $w_x = 1$ to that of G, with w_x an explicit length p word beginning with x.*

Theorem 1.2 extends the results of [2], in which solutions of class 2 are addressed by a different method. Our approach relies on the connection with the *right-cyclic law* of [8] and on the existence of an *I-structure* [6] [7] which enables one to carry to arbitrary structure monoids results that are trivial in the case of $\mathbb{Z}^n$.

2. The class of a finite RC-quasigroup

The first step consists in switching from solutions of YBE to RC-quasigroups.

Definition 2.1. An *RC-system* is a pair $(X, \star)$ with $\star$ a binary operation on X that obeys the *RC-law* $(x{\star}y){\star}(x{\star}z) = (y{\star}x){\star}(y{\star}z)$. An *RC-quasigroup* is an RC-system in which the maps $y \mapsto x{\star}y$ are bijections. An RC-quasigroup is *bijective* if the map $(x, y) \mapsto (x{\star}y, y{\star}x)$ from X^2 to X^2 is bijective. The *associated group* (*resp. monoid*) is presented by $\langle X \mid \{x(x{\star}y) = y(y{\star}x) \mid x, y \in X\}\rangle$.

As proved in [8], if (X, R) is an involutive, nondegenerate set-theoretic solution of YBE, then defining $x{\star}y$ to be the (unique) z satisfying $R_1(x, z) = y$ makes X into a bijective RC-quasigroup and the group and monoid associated with $(X, \star)$ coincide with those of (X, R). Conversely, every bijective RC-quasigroup $(X, \star)$ comes associated with a set-theoretic solution of YBE. Thus investigating structure groups of set-theoretic solutions of YBE and groups of bijective RC-quasigroups are equivalent tasks.

Definition 2.2. Inductively define $\Pi_1(x_1) = x_1$ and

$$\Pi_n(x_1, ..., x_n) = \Pi_{n-1}(x_1, ..., x_{n-1}){\star}\Pi_{n-1}(x_1, ..., x_{n-2}, x_n). \tag{1}$$

An RC-quasigroup $(X, \star)$ is said to be of *class* p if $\Pi_{p+1}(x, ..., x, y) = y$ holds for all x, y in X.

Lemma 2.3. *Every finite RC-quasigroup is of class p for some p.*

Proof. Let $(X, \star)$ be a finite RC-quasigroup. First, $(X, \star)$ must be bijective, that is, the map $\Psi : (x, y) \mapsto (x{\star}y, y{\star}x)$ is bijective on X^2 [8] (or [7] for a different argument). Now, consider the map $\Phi : (x, y) \mapsto (x{\star}x, x{\star}y)$ on X^2. Assume $(x, y) \neq (x', y')$. For $x \neq x'$, $\Psi(x, x) \neq \Psi(x', x')$ implies $x{\star}x \neq x'{\star}x'$; for $x = x'$, we have $y \neq y'$, whence $x{\star}y \neq x{\star}y'$ since left-translations are injective; so $\Phi(x, y) \neq \Phi(x', y')$ always holds. So Φ is injective, hence bijective on X^2, and $\Phi^{p+1} = \mathrm{id}$ holds for some $p \geq 1$. An induction gives $\Phi^r(x, y) = (\Pi_r(x, ..., x, x), \Pi_r(x, ..., x, y))$. So $\Phi^{p+1} = \mathrm{id}$ implies $\Pi_{p+1}(x, ..., x, y) = y$ for all x, y, that is, $(X, \star)$ is of class p. □

3. Using the I-structure

From now on, assume that M (*resp.* G) is the structure group of some finite RC-quasigroup $(X, \star)$ of size n and class p. The form of the defining relations of M implies that the Cayley graph of M with respect to X is an n-dimensional lattice. It was proved in [6] that M admits a *(right) I-structure*, defined to be a bijection $\nu : \mathbb{N}^n \to M$ satisfying $\nu(1) = 1$ and $\{\nu(ux) \mid x \in X\} = \{\nu(u)x \mid x \in X\}$ for every u in $\mathbb{N}^n$, that is, equivalently, $\nu(ux) = \nu(u)\pi(u)(x)$ for some permutation $\pi(u)$ of X. The monoid M is then called *of right-I-type*. Our point is that the I-structure (which is unique) is connected with $\star$. Without loss of generality, we shall assume that X is the standard basis of $\mathbb{N}^n$ and that $\nu(x) = x$ holds for x in X.

Lemma 3.1. *For all $x_1, ..., x_r$ in X, we have $\nu(x_1 \cdots x_r) = \Sigma_r(x_1, ..., x_r)$, with Σ_r inductively defined by $\Sigma_1(x_1) = x_1$ and*

$$\Sigma_r(x_1, ..., x_r) = \Sigma_{r-1}(x_1, , ..., x_{r-1}) \cdot \Pi_r(x_1, ..., x_r).$$

Proof. The result can be established directly by developing a convenient RC-calculus and proving that $\Sigma_r(x_1, ..., x_r)$ satisfies all properties required for an I-structure. A shorter proof is to start from the existence of the I-structure ν and just connect it with the values of Σ_r. As established in [6] (see also [7, Chapter 8, Lemma 8.2.2]), the following inductive relations are satisfied for all u, v in $\mathbb{N}^n$:

$$\nu(uv) = \nu(u)\,\nu(\pi(u)[v]) \quad \text{and} \quad \pi(uv) = \pi(\pi(u)[v]) \circ \pi(u) \tag{2}$$

where $\pi[u]$ is the result of applying π to u componentwise.

We then use induction on r. For $r = 1$, the result is obvious. Assume $r = 2$ and $x_1 \neq x_2$. By definition, we have $\nu(x_1x_2) = x_1\pi(x_1)(x_2) = \nu(x_2x_1) = x_2\pi(x_2)(x_1)$. This shows that $\nu(x_1x_2)$ must be the right-lcm (least common right-multiple) of x_1 and x_2 in M. On the other hand, $x_1(x_1 \star x_2) = x_2(x_2 \star x_1)$ holds in M by definition, and this must also represent the right-lcm of x_1 and x_2. By uniqueness of the right-lcm and left-cancellativity, we deduce $\pi(x_1)(x_2) = x_1 \star x_2$. Next, for $x_1 = x_2$, the value of $\pi(x_1)(x_2)$, as well as that of $x_1 \star x_2$, must be the unique element of X that is not of the form $\pi(x_1)(x)$ or $x_1 \star x$ with $x \neq x_1$, respectively. This forces $\pi(x_1)(x_2) = x_1 \star x_2$ in this case as well, implying $\nu(x_1x_2) = x_1(x_1 \star x_2) = \Sigma_2(x_1, x_2)$ in every case. Assume now $r \geq 3$. We find

$$\begin{aligned}\nu(x_1 \cdots x_r) &= x_1\,\nu(\pi(x_1)[x_2 \cdots x_r]) = x_1\,\nu((x_1 \star x_2) \cdots (x_1 \star x_r))\\ &= x_1\,\Sigma_{r-1}(x_1 \star x_2, ..., x_1 \star x_r) = \Sigma_r(x_1, x_2, ..., x_r),\end{aligned}$$

the first equality by (2), the second by the case $r = 2$, the third by the induction hypothesis, and the last one by expanding the terms. □

Lemma 3.2. *For $x \in X$ and $r \geq 0$, let $x^{[r]} = \nu(x^r)$. For all $x \in X$ and $u \in \mathbb{N}^n$, we have $\nu(x^p u) = x^{[p]}\nu(u)$ in M. In particular, we have $\pi(x^p) = \mathrm{id}$ and, for all x, y in X, the elements $x^{[p]}$ and $y^{[p]}$ commute in M.*

Proof. Let $y_1 \cdots y_q$ be a decomposition of u in terms of elements of X. By Lemma 3.1, we have

$$\begin{aligned}\nu(x^p u) &= \Sigma_{p+q}(x, ..., x, y_1, ..., y_q)\\ &= \Sigma_p(x, ..., x)\Sigma_q(\Pi_{p+1}(x, ..., x, y_1), ..., \Pi_{p+1}(x, , ..., x, y_q))\\ &= \Sigma_p(x, ..., x)\Sigma_q(y_1, ..., y_q) = \nu(x^p)\nu(y_1 \cdots y_q) = x^{[p]}\nu(u),\end{aligned}$$

in which the second equality comes from expanding the terms and the third one from the assumption that M is of class p. Applying with $u = y$ in X and merging with $\nu(x^p y) = \nu(x^p)\,\pi(x^p)(y)$, we deduce $\pi(x^p) = \mathrm{id}$. On the other hand, applying with $u = y^{[p]}$, we find $x^{[p]}y^{[p]} = \nu(x^p y^p) = \nu(y^p x^p) = y^{[p]}x^{[p]}$. □

Lemma 3.3. *Assume $p \geq 2$ and define $\Delta = \nu(\prod_{x\in X} x^{p-1})$. Then Δ is a Garside element in M, and its family of divisors is $\nu(\{0, ..., p-1\}^n)$), which has p^n elements. Moreover Δ^p is central in M.*

Proof. The map ν is compatible with $\preccurlyeq$: for all u, v in $\mathbb{N}^n$, we have $u \preccurlyeq v$ in $\mathbb{N}^n$ if and only if $\nu(u) \preccurlyeq \nu(v)$ holds in M. Indeed, by (2), $v = ux$ with x in X implies $\nu(v) = \nu(u)\pi(u)(x)$, whence $\nu(u) \preccurlyeq \nu(v)$ in M. Conversely, for $\nu(v) = \nu(u)x$ with x in X, as $\pi(u)$ is bijective, we have $\pi(u)(y) = x$ for some y in X, whence $\nu(uy) = \nu(u)\pi(u)(y) = \nu(u)x = \nu(v)$, and $v = uy$ since ν is injective, that is, $u \preccurlyeq v$ in $\mathbb{N}^n$. Hence the left-divisors of Δ in M are the image under ν of the p^n divisors of δ^{p-1} in $\mathbb{N}^n$, with $\delta = \prod_{x\in X} x$. For right-divisors, the maps $\pi(u)$ are bijective, so every right-divisor of Δ must be a left-divisor of Δ. Then the duality map $g \mapsto h$ for $gh = \Delta$ is a bijection from the left- to the right-divisors of Δ. So the left- and right-divisors of Δ coincide, and they are p^n in number. Since every element of X divides Δ, the latter is a Garside element in M. Finally, by Lemma 3.1, Δ^p is the product of the elements $x^{[p]}$ repeated $p-1$ times; as $\sigma[\delta] = \delta$ holds for every permutation σ, we deduce $x\Delta^p = \Delta^p x$ for every x. □

For $u \in \mathbb{N}^n$ and $x \in X$, write $|u|_x$ for the (well-defined) number of x in an X-decomposition of u.

Lemma 3.4. *For u, u' in $\mathbb{N}^n$, say that $u \equiv_p u'$ holds if, for every x in X, we have $|u|_x = |u'|_x \bmod p$, and, for g, g' in M, say that $g \equiv g'$ holds for $\nu^{-1}(g) \equiv_p \nu^{-1}(g')$. Then $\equiv$ is an equivalence relation on M that is compatible with left- and right-multiplication.*

Proof. As ν is bijective, carrying the equivalence relation $\equiv_p$ of $\mathbb{N}^n$ to M yields an equivalence relation. Assume $\nu(u) \equiv \nu(u')$. Without loss of generality, we may assume $u' = ux^p = x^p u$ with x in X. Applying (2) and Lemma 3.2, we deduce $\pi(u) = \pi(u')$ and, therefore, $\nu(u)\pi(u)(y) = \nu(uy) \equiv \nu(u'y) = \nu(u')\pi(u)(y)$. As $\pi(u)(y)$ takes every value in X when y varies, $\equiv$ is compatible with right-multiplication by X. On the other hand, $u \equiv_p u'$ implies $\sigma[u] \equiv_p \sigma[u']$ for every permutation σ in $\mathfrak{S}_X$, so we obtain $y\nu(u) = \nu(y\pi(y)^{-1}[u]) \equiv \nu(y\pi(y)^{-1}[u']) = y\nu(u')$, and $\equiv$ is compatible with left-multiplication by X. □

Lemma 3.5. *For $g = \Delta^{pe}h$, $g' = \Delta^{pe'}h'$ in G with $h, h' \in M$, say that $g \equiv g'$ holds if $h \equiv h'$ does. Then $\equiv$ is a congruence on G with p^n classes, and the kernel of $G \to G/{\equiv}$ is the Abelian subgroup of G generated by the elements $x^{[p]}$ with $x \in X$.*

Proof. As Δ is a Garside element in M, every element of G admits a (non-unique) expression $\Delta^{pe}h$ with $e \in \mathbb{Z}$ and $h \in M$. Assume $g = \Delta^{pe}h = \Delta^{pe_1}h_1$ with $e > e_1$. As M is left-cancellative, we find $h_1 = \Delta^{p(e-e_1)}h$, whence $h_1 \equiv h$. So, for every h' in M, we have $h \equiv h' \Leftrightarrow h_1 \equiv h'$ and $\equiv$ is well-defined on G. That $\equiv$ is compatible with multiplication on G follows from the compatibility on M and the fact that Δ^p lies in the centre of G. Next, by definition, every element of G is $\equiv$-equivalent to some element of M, so the number of $\equiv$-classes in G equals the number of $\equiv$-classes in M, hence the number p^n of $\equiv_p$-classes in $\mathbb{N}^n$.

Finally, $u \equiv_p x^p u$ holds for all x in X and u in $\mathbb{N}^n$. This, together with Lemma 3.1, implies $x^{[p]} \equiv 1$. Conversely, assume $g \equiv 1$ in M. By definition, $\nu^{-1}(g)$ lies in the $\equiv_p$-class of 1, hence one can go from $\nu^{-1}(g)$ to 1 by multiplying or dividing by elements x^p with $x \in X$. By Lemma 3.1 again, this means that one can go from g to 1 by multiplying or dividing by elements $x^{[p]}$ with $x \in X$. In other words, the latter elements generate the kernel of the projection of G to $G/{\equiv}$. □

Now Theorem 1.2 readily follows. Indeed, define W to be the finite quotient-group $G/{\equiv}$. We saw that the kernel of the projection of G onto W is the free Abelian group generated by the n elements $x^{[p]}$ with $x \in X$, thus giving an exact sequence $1 \to \mathbb{Z}^n \to G \to W \to 1$. A presentation of W is obtained by adding to the presentation of G in Definition 2.1 the n relations $x^{[p]} = 1$, that is, $x(x{\star}x)((x{\star}x){\star}(x{\star}x))... = 1$. By construction, the Hasse diagram of the lattice made of the p^n divisors of Δ is the image under ν of the sublattice of $\mathbb{N}^n$ made of the p^n divisors of δ in $\mathbb{N}^n$, whereas the Cayley graph of the germ derived from (W, X)—that is, W equipped with the partial product obtained by restricting to the cases when the X-lengths add—is the image under ν of the Cayley graph of the germ derived from the quotient-group $\mathbb{Z}^n/{\equiv_p}$: the (obvious) equality in the case of $\mathbb{N}^n$ implies the equality in the case of M.

4. An example

For an RC-quasigroup of class 1, that is, satisfying $x{\star}y = y$ for all x, y, the group G is a free Abelian group, the group W is trivial, and the short exact sequence of Theorem 1.2 reduces to $1 \to \mathbb{Z}^n \to G \to 1$.

Class 2, that is, when $(x{\star}x){\star}(x{\star}y) = y$ holds for all x, y, is addressed in [2] (with no connection with RC-quasigroups). The element Δ is the right-lcm of X, it has 2^n divisors which are the right-lcms of subsets of X, and the group W is the order 2^n quotient of G obtained by adding the relations $x(x{\star}x) = 1$.

For one example in class 3, consider $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$ with $x{\star}y = f(y)$, $f : \mathtt{a} \mapsto \mathtt{b} \mapsto \mathtt{c} \mapsto \mathtt{a}$. The associated presentation is $\langle \mathtt{a}, \mathtt{b}, \mathtt{c} \mid \mathtt{ac} = \mathtt{b}^2, \mathtt{ba} = \mathtt{c}^2, \mathtt{cb} = \mathtt{a}^2 \rangle$. The smallest Garside element is $\mathtt{a}^3$, but, here, in class 3, we consider the next one, namely $\Delta = \mathtt{a}^6$. Adding to the above presentation of G the three relations $x(x{\star}x)((x{\star}x){\star}(x{\star}x)) = 1$, namely $\mathtt{abc} = \mathtt{bca} = \mathtt{cab} = 1$, here reducing to $\mathtt{abc} = 1$, one obtains for W

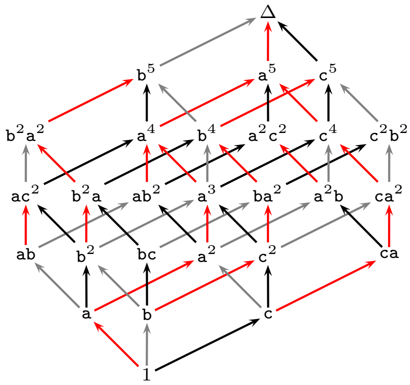

Figure 1. An example in class 3: here W has $3^3 = 27$ elements, and its Cayley graph is a cube with edges of length $3 - 1$.

the presentation $\langle \mathtt{a}, \mathtt{b}, \mathtt{c} \mid \mathtt{ac} = \mathtt{b}^2, \mathtt{ba} = \mathtt{c}^2, \mathtt{cb} = \mathtt{a}^2, \mathtt{abc} = 1\rangle$. The lattice $\mathrm{Div}(\Delta)$ has 27 elements, its diagram is the cube shown on the right. The latter is also the Cayley graph of the germ derived from (W, X).

References

[1] F. Chouraqui, *Garside groups and Yang-Baxter equations*, Comm. Algebra 38 (2010) 4441-4460.

[2] F. Chouraqui and E. Godelle, *Finite quotients of groups of I-type*, arXiv:1301.3707.

[3] P. Dehornoy, *Groupes de Garside*, Ann. Scient. Ec. Norm. Sup. 35 (2002) 267-306.

[4] P. Dehornoy, F. Digne, and J. Michel, *Garside families and Garside germs*, J. of Algebra, to appear, arXiv:1208.3362.

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

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

[7] E. Jespers and J. Okninski, Noetherian semigroup algebras, Algebra and Applications vol. 7, Springer-Verlag (2007).

[8] W. Rump, *A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation*, Adv. in Math. 193 (2005) 4055.

E-mail address: `patrick.dehornoy@unicaen.fr`

Laboratoire de Mathématiques Nicolas Oresme, CNRS UMR6139, Université de Caen, 14032 Caen cedex