



HAL
open science

Set-theoretic solutions of the Yang-Baxter equation, RC-calculus, and Garside germs

Patrick Dehornoy

► **To cite this version:**

Patrick Dehornoy. Set-theoretic solutions of the Yang-Baxter equation, RC-calculus, and Garside germs. 2014. hal-00958299v2

HAL Id: hal-00958299

<https://hal.science/hal-00958299v2>

Preprint submitted on 18 Mar 2014 (v2), last revised 6 May 2014 (v3)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

SET-THEORETIC SOLUTIONS OF THE YANG–BAXTER EQUATION, RC-CALCULUS, AND GARSIDE GERMS

PATRICK DEHORNOY

ABSTRACT. Building on a result by W. Rump, we show how to exploit the right-cyclic law $(x * y) * (x * z) = (y * x) * (y * z)$ in order to investigate the structure groups and monoids attached with (involutive nondegenerate) set-theoretic solutions of the Yang–Baxter equation. We develop a sort of right-cyclic calculus, and use it to obtain short proofs for the existence both of the Garside structure and of the I -structure of such groups. We describe finite quotients that play for the considered groups the role that Coxeter groups play for Artin–Tits groups.

The Yang–Baxter equation (YBE) is a fundamental equation occurring in integrable models in statistical mechanics and quantum field theory [23]. Among its many solutions, some simple ones called set-theoretic turn out to be connected with several interesting algebraic structures. In particular, a group and a monoid are attached with every set-theoretic solution of YBE [14], and the family of all groups and monoids arising in this way is known to have rich properties: as shown by T. Gateva–Ivanova and M. Van den Bergh in [18] and by E. Jespers and J. Okniński in [21], they admit an I -structure, meaning that their Cayley graph is isometric to that of a free Abelian group, and, as shown by F. Chouraqui in [4], they admit a Garside structure, (roughly) meaning that they are groups of fractions of monoids in which divisibility relations are lattice orders.

It was shown by W. Rump in [24] that (involutive nondegenerate) set-theoretic solutions of YBE are in one-to-one correspondence with algebraic structures consisting of a set equipped with a binary operation $*$ that obeys the right-cyclic law $(x*y)*(x*z) = (y*x)*(y*z)$ and has bijective left-translations. What we do in this paper is to develop the investigation of the right-cyclic law (RC-law) and show how to use it to reprove the above mentioned results in a more simple and explicit way. In terms of divisibility relations, calling a structure as above an *RC-quasigroup*, we observe that, starting with any RC-quasigroup, the formulas of RC-calculus imply the existence of least common multiples in the associated monoid and, conversely, starting with a monoid in which atoms admit least common multiples of length two, the derived right-complement operation obeys the RC-law. Similarly, we observe that the bijection that witnesses for an I -structure can be computed explicitly using sorts of polynomials involving the RC-operation; the equivalence between the existence of an I -structure and the property of being associated with a finite RC-quasigroup can then be established using arguments that are shorter and arguably more simple than those of [22]. One can also note that the approach via RC-calculus never requires to restrict to squarefree solutions of YBE as do some of

2010 *Mathematics Subject Classification.* 20N02, 20F38, 20M30, 20F55, 57M25.

Key words and phrases. Yang–Baxter equation, set-theoretic solution, Garside monoid, Garside group, monoid of I -type, right-cyclic law, RC-quasigroup, birack.

the developments of [20] or [24] (a solution ρ is called squarefree if $\rho(s, s) = (s, s)$ holds for every s —corresponding to RC-quasigroups $(S, *)$ that satisfy $s * s = s$ for every s).

However, the main benefit of the current approach is to provide a simple and complete solution to the problem of finding what is called a *Garside germ* for every group associated with a finite RC-quasigroup (that is, with the structure group of a finite involutive nondegenerate set-theoretic solution of YBE), namely a finite quotient of the group that encodes the whole structure in the way a finite Coxeter group encodes the associated Artin–Tits group. The precise statement (Proposition 6.2) says that, if we start with the canonical presentation of the group G associated with an RC-quasigroup $(S, *)$ that has cardinality n and class d (a certain numerical parameter attached with every finite RC-quasigroup) and add the “RC-torsion relations” $s^{[d]} = 1$ with s in S (where $s^{[d]}$ is an explicit polynomial involving $*$), then one obtains a finite group \overline{G} of order d^n such that the whole Garside structure of G can be retrieved from the “Coxeter-like group” \overline{G} . Partial results in this direction, corresponding to the special case of RC-quasigroups of class 2, namely those satisfying the law $(x * x) * (x * y) = y$, were obtained by hand in [5]. Our current approach based on RC-calculus and the I -structure enables one to address the general case directly.

At the moment, no exhaustive classification of the finite (involutive, nondegenerate) set-theoretic solutions of the Yang–Baxter equation is in view. As will be recalled in Proposition 5.7, the monoids associated with solutions based on S embeds in the wreath product $\mathbb{N} \wr \mathfrak{S}_S$ and it was suggested in [3] to use the second projections of the images, called involutive Yang–Baxter (IYB) \overline{G} groups for such a classification. The above mentioned finite Coxeter-like groups \overline{G} provide natural alternative options for the classification problem. At the moment, no complete description of these groups is known, but it is easy to characterize them as those finite groups that admit a “modular I -structure”, namely the counterpart of an I -structure where the free Abelian group \mathbb{Z} is replaced with a cyclic group $\mathbb{Z}/d\mathbb{Z}$ (Proposition 6.12). We also observe that these Coxeter-like groups can be realized as isometries of a finite-dimensional Hermitian space (Corollary 6.17). We hope that further properties will be discovered soon.

The paper is organized as follows. In Section 1, we recall the connection between set-theoretic solutions of the Yang–Baxter equation and algebraic systems that obey the RC-law. In Section 2, we establish various formulas that follow from the RC-law and will be heavily used in the sequel. In Section 3, we recall the definition of the structure group and monoid attached with an set-theoretic solution of YBE and use the formulas of Section 2 to show that such monoids are Garside monoids, meaning that the associated divisibility relations have nice lattice properties. Next, in Section 4, we use the RC-calculus again to show that, conversely, every Garside monoid that admits a presentation of a certain syntactic type comes from an RC-quasigroup (hence a solution of the YBE). Then, in Section 5, we use the RC-calculus once more to show that every structure monoid admits what is called an I -structure and that, conversely, every monoid with an I -structure comes from an RC-quasigroup. Finally, in Section 6, we merge the RC-calculus and the I -structure to construct a finite quotient that encodes the whole structure of the group attached to a finite RC-quasigroup and gives several descriptions of this “Coxeter-like” group, in particular as a group of isometries of an Hermitian space.

Sections 3 and 4 on the one hand, and Section 5 are independent (except for the definition of the structure group and monoid) and can be read in any order. By contrast, all sections from Section 3 heavily use the formulas of Section 2.

ACKNOWLEDGMENTS

The author wishes to thank Tatiana Gateva-Ivanova, Eric Jespers, Gilbert Levitt, and Jan Okniński for discussions about the content of this paper.

1. SEVERAL EQUIVALENT FRAMEWORKS

In this introductory section, we recall the definition of set-theoretic solutions of the Yang–Baxter equation [14] and their connection with what we shall call *RC-quasigroups*, which are sets equipped with a binary operation obeying the right-cyclic law $(x * y) * (x * z) = (y * x) * (y * z)$, as established by W. Rump in [24].

Definition 1.1. A *set-theoretic solution of YBE* (or *braided quadratic set*) is a pair (S, ρ) where S is a set and ρ is a bijection of $S \times S$ into itself that satisfies

$$(1.1) \quad \rho^{12} \rho^{23} \rho^{12} = \rho^{23} \rho^{12} \rho^{23}.$$

where ρ^{ij} is the map of S^3 to itself obtained when ρ acts on the i th and j th entries.

If (S, ρ) is a set-theoretic solution of YBE and V is a vector space based on S , then the (unique) linear operator R on $V \otimes V$ that extends ρ is a solution of the (non-parametric, braid form of) the (quantum) Yang–Baxter equation

$$(1.2) \quad R^{12} R^{23} R^{12} = R^{23} R^{12} R^{23},$$

and, conversely, every solution of YBE such that there exists a basis S of the ambient vector space such that $S^{\otimes 2}$ is globally preserved is of this type.

Definition 1.2. A set-theoretic solution (S, ρ) of YBE is called *nondegenerate* if, writing $\rho_1(s, t)$ and $\rho_2(s, t)$ for the first and second entries of $\rho(s, t)$, the left-translation $y \mapsto \rho_1(s, y)$ is one-to-one for every s in S and the right-translation $x \mapsto \rho_2(x, t)$ is one-to-one for every t in S .

On the other hand, a solution (S, ρ) is called *involution* if $\rho \circ \rho$ is the identity of $S \times S$. There exist six set-theoretic solutions of YBE based on the 2-element set $\{\mathbf{a}, \mathbf{b}\}$, among which two are nondegenerate and involutive, namely

$$\begin{array}{c|cc} & \mathbf{a} & \mathbf{b} \\ \hline \mathbf{a} & (\mathbf{a}, \mathbf{a}) & (\mathbf{b}, \mathbf{a}) \\ \mathbf{b} & (\mathbf{a}, \mathbf{b}) & (\mathbf{b}, \mathbf{b}) \end{array} \quad \text{and} \quad \begin{array}{c|cc} & \mathbf{a} & \mathbf{b} \\ \hline \mathbf{a} & (\mathbf{b}, \mathbf{b}) & (\mathbf{a}, \mathbf{b}) \\ \mathbf{b} & (\mathbf{b}, \mathbf{a}) & (\mathbf{a}, \mathbf{a}) \end{array} .$$

A map from $S \times S$ to itself is a pair of maps from $S \times S$ to S , hence a pair of binary operations on S . Translating into the language of binary operations the constraints that define set-theoretic solutions of YBE is straightforward.

Lemma 1.3. Define a birack to be an algebraic system (S, \rfloor, \lceil) consisting of a set S equipped with two binary operations \rfloor and \lceil that satisfy

$$(1.3) \quad (a \rfloor b) \lceil ((a \lceil b) \rfloor c) = a \lceil (b \rfloor c),$$

$$(1.4) \quad (a \rfloor b) \lceil ((a \lceil b) \rfloor c) = (a \lceil (b \rfloor c)) \lceil (b \lceil c),$$

$$(1.5) \quad (a \lceil b) \rfloor c = (a \lceil (b \rfloor c)) \lceil (b \lceil c),$$

and are such that the left-translations of \rfloor and the right-translations of \lceil are one-to-one, and call a birack involutive if it satisfies in addition

$$(1.6) \quad (a \rfloor b) \rfloor (a \lceil b) = a \quad \text{and} \quad (a \lceil b) \lceil (a \rfloor b) = b.$$

(i) If (S, ρ) is a nondegenerate set-theoretic solution of YBE, then defining $a \rfloor b = \rho_1(a, b)$ and $a \lceil b = \rho_2(a, b)$ yields a birack (S, \rfloor, \lceil) . If (S, ρ) is involutive, then the birack (S, \rfloor, \lceil) is involutive.

(ii) Conversely, if (S, \rfloor, \lceil) is a birack, then defining $\rho(a, b) = (a \rfloor b, a \lceil b)$ yields a nondegenerate set-theoretic solution (S, ρ) of YBE. If the birack (S, \rfloor, \lceil) is involutive, then (S, ρ) is involutive.

Lemma 1.3 appears as Remark 1.6 in [19], using the notation $({}^a b, a^b)$ for $(a \rfloor b, a \lceil b)$. Biracks appeared in low-dimensional topology as a natural algebraic counterpart of Reidemeister move III [15]. When \lceil is trivial in the sense that $a \lceil b = a$ always holds, (1.3)–(1.5) reduce to the left-selfdistributivity law $(a \rfloor b) \rfloor (a \rfloor c) = a \rfloor (b \rfloor c)$, corresponding, when left-translations are bijective, to (S, \rfloor) being what is known as a rack [16]. Note that a birack obtained from a rack is involutive only if $s \rfloor t = t$ holds for all s, t (trivial birack).

Thus, investigating involutive nondegenerate set-theoretic solutions of YBE and investigating involutive biracks are equivalent tasks.

We now make a second step and move to a new framework according to the approach of [24]. The point is that, if \rfloor is a binary operation on S and its left-translations are one-to-one, then putting

$$a * b = \text{the unique } c \text{ satisfying } a \rfloor c = b$$

provides a well-defined binary operation on S , which can be viewed as a left-inverse of \rfloor . The seminal observation of [24] is that, if (S, \rfloor, \lceil) is a birack, then the left-inverse $*$ of the operation \rfloor obeys a simple algebraic law and the whole structure can be recovered from the unique operation $*$, that is, there is no need to simultaneously consider the right-inverse of the second operation \lceil , as could be expected *a priori*.

Definition 1.4 (Rump [24]). A *right-cyclic system*, or *RC-system*, is a pair $(S, *)$ where $*$ is a binary operation on the set S that obeys the *right-cyclic law* RC

$$(1.7) \quad (x * y) * (x * z) = (y * x) * (y * z).$$

An *RC-quasigroup* is an RC-system whose left-translations are one-to-one, that is, for every s in S , the map $t \mapsto s * t$ is one-to-one. An RC-system is called *bijective* if the map $(s, t) \mapsto (s * t, t * s)$ is a bijection of $S \times S$ to itself.

In [24], RC-quasigroups are called “cycle sets” (and RC-systems are called “cycloids”), but the current terminology may seem more convenient in view of the subsequent variants (and of the widely used convention that “quasigroup” refers to bijective translations).

Example 1.5. A typical (semi-trivial) example of a bijective RC-quasigroup is provided by every operation of the form $s * t = f(t)$ where f is a permutation of S .

Another example (that will be important in Section 3 below) is provided by the right-complement operation in a monoid: if M is a left-cancellative monoid in which any two elements admit a unique least common right-multiple—see Section 3 below—then the operation \setminus defined by the condition that $f(f \setminus g)$ is the least common right-multiple of f and g obeys the law (1.7), as easily follows from

the commutativity and associativity of the right-lcm operation. So (M, \setminus) is an RC-system (but, in general, not an RC-quasigroup).

The following result, which is essentially [24, Prop. 4.1] shows that the context of a bijective RC-quasigroup is entirely equivalent to that of an involutive nondegenerate set-theoretic solution of the YBE.

Proposition 1.6. (i) *Assume that (S, ρ) is an involutive nondegenerate set-theoretic solution of YBE. Let $*$ be the binary operation on S defined by*

$$(1.8) \quad s * t = \text{the unique } r \text{ satisfying } \rho_1(s, r) = t.$$

*Then $(S, *)$ is a bijective RC-quasigroup.*

(ii) *Conversely, assume that $(S, *)$ is a bijective RC-quasigroup. Define a map $\rho : S^2 \rightarrow S^2$ by*

$$(1.9) \quad \rho(a, b) = \text{the unique } (a', b') \text{ satisfying } a * a' = b \text{ and } a' * a = b'.$$

Then (S, \lceil, \rfloor) is an involutive birack.

As our approach below is slightly different from that of [24], we indicate a proof of Proposition 1.6. Before completing the argument, it is convenient to first introduce the following two-operation version of RC-quasigroups.

Definition 1.7. An *RLC-system* is a triple $(S, *, \tilde{*})$ such that $(S, *)$ is an RC-system, $\tilde{*}$ is a second binary operation on S that obeys the *left-cyclic law LC*

$$(1.10) \quad (z \tilde{*} x) \tilde{*} (y \tilde{*} x) = (z \tilde{*} y) \tilde{*} (x \tilde{*} y),$$

and both operations are connected by

$$(1.11) \quad (y * x) \tilde{*} (x * y) = x = (y \tilde{*} x) * (x \tilde{*} y).$$

An *RLC-quasigroup* is an RLC-system $(S, *, \tilde{*})$ such that the left-translations of $*$ and the right-translations of $\tilde{*}$ are one-to-one.

The next result says that, in an RLC-quasigroup, the operations determine one another and, as a consequence, RLC-quasigroups and bijective RC-quasigroups are equivalent structures.

Lemma 1.8. *For all binary operations $*, \tilde{*}$ on S , the following are equivalent:*

- (i) *The system $(S, *, \tilde{*})$ obeys the involutivity laws (1.11).*
- (ii) *The map $\Psi : (s, t) \mapsto (s * t, t * s)$ is a bijection of $S \times S$ to itself and $\tilde{*}$ is the unique operation on S such that the map $(s, t) \mapsto (s \tilde{*} t, t \tilde{*} s)$ is the inverse of Ψ*

Proof. Assume that $(S, *, \tilde{*})$ satisfies (1.11). Let (s', t') belong to $S \times S$. Put $s = t' \tilde{*} s'$ and $t = s' \tilde{*} t'$. Then, the right-hand equality in (1.11) gives $s * t = s'$ and $t * s = t'$, whence $\Psi(s, t) = (s', t')$. So Ψ is surjective. Conversely, assume $\Psi(s, t) = (s', t')$. Then the left-hand equality in (1.11) gives $s = t' * s'$ and $t = s' * t'$. So Ψ is injective. Moreover, the equalities show that the map $(s, t) \mapsto (s \tilde{*} t, t \tilde{*} s)$ is Ψ^{-1} . So (i) implies (ii).

Conversely, assume that Ψ is a bijection from $S \times S$ to itself. Then there exists a unique operation $\tilde{*}$ on S such that the map $(s, t) \mapsto (s \tilde{*} t, t \tilde{*} s)$ is Ψ^{-1} , namely the operation defined by

$$(1.12) \quad s' \tilde{*} t' = \text{the unique } t \text{ such that } s * t = s' \text{ and } t * s = t' \text{ hold for some } s.$$

Then (1.11) is satisfied by definition, that is, (ii) implies (i). \square

We can now complete the argument.

Proof of Proposition 1.6. (i) Owing to Lemma 1.3, we can use a birack language. So we start with an involutive birack (S, \lrcorner, \lceil) and consider $*$ defined by

$$(1.13) \quad s * t = \text{the unique } r \text{ satisfying } s \lrcorner r = t.$$

By definition, the left-translations of \lrcorner are bijective, which guarantees the existence of $*$, and the fact that the left-translations of $*$ are one-to-one. We will show that the satisfaction of (1.3)–(1.6) in (S, \lrcorner, \lceil) implies that $*$ obeys the RC-law (1.7).

Claim 1.— For all x, y, z , the relation $y = x \lrcorner z$ is equivalent to $x * y = z$ and it implies $y * x = x \lceil z$.

Proof of Claim 1. Assume $y = x \lrcorner z$. First, by definition of $*$, this relation is equivalent to $x * y = z$. Next, (1.6), implies $(x \lrcorner z) \lceil (x \lrcorner z) = x$, so we deduce $y \lceil (x \lrcorner z) = x$. By definition of $*$, the latter relation is equivalent to $y * x = x \lceil z$. \square

Now let r, s, t belong to S . Put $a = t$, $b = t * s$, and $c = (t * s) * (t * r)$. We shall step by step compute the expressions $(r * s) * (r * t)$ and $(s * r) * (s * t)$ in terms of a , b , and c and, using (1.3)–(1.5), establish that these expressions are equal. The proof consists in repeatedly using Claim 1 for various relations $z = x * y$. The corresponding diagrams are displayed in Figure 3. The latter shows that we are completing a cube and it should make the order of the verifications clear.

Applying Claim 1 to the definition $b = t * s$ with $t = a$ gives $s = a \lrcorner b$ and $s * t = a \lceil b$.

Next, applying Claim 1 to $c = (t * s) * (t * r)$ with $t * s = b$ gives $t * r = b \lrcorner c$ and $(r * t) * (r * s) = b \lceil c$.

Then, applying Claim 1 to $b \lrcorner c = t * r$ with $t = a$ gives $r = a \lrcorner (b \lrcorner c)$, hence also $r = (a \lrcorner b) \lceil ((a \lrcorner b) \lrcorner c)$ by (1.3), and $r * t = a \lceil (b \lrcorner c)$.

Next, the relations $s = a \lrcorner b$ and $r = (a \lrcorner b) \lceil ((a \lrcorner b) \lrcorner c)$ imply $s * r = (a \lrcorner b) \lrcorner c$, and Claim 1 implies $r * s = s \lceil (s * r) = (a \lrcorner b) \lceil ((a \lrcorner b) \lrcorner c)$, hence also $r * s = (a \lrcorner (b \lrcorner c)) \lceil (b \lrcorner c)$ by (1.4).

Next, the relations $r * t = a \lceil (b \lrcorner c)$ and $r * s = r * s = (a \lrcorner (b \lrcorner c)) \lceil (b \lrcorner c)$ imply $(r * t) * (r * s) = b \lrcorner c$, and Claim 1 implies $(r * s) * (r * t) = (a \lrcorner (b \lrcorner c)) \lceil (b \lrcorner c)$, hence $(r * s) * (r * t) = (a \lrcorner b) \lrcorner c$ by (1.5).

Finally, the relations $s * t = a \lceil b$ and $s * r = (a \lrcorner b) \lrcorner c$ imply $(s * t) * (s * r) = c$, and Claim 1 implies $(s * r) * (s * t) = (a \lrcorner b) \lrcorner c$.

We thus established the three equalities $(r * t) * (r * s) = b \lrcorner c = (t * r) * (t * s)$, $(t * s) * (t * r) = c = (s * t) * (s * r)$, and $(r * s) * (r * t) = (a \lrcorner b) \lrcorner c = (s * r) * (s * t)$. We thus proved that $(S, *)$ is an RC-quasigroup (of course, one equality would be sufficient as r, s, t are arbitrary).

Now, consider the binary operation $\tilde{*}$ on S such that $x \tilde{*} y = z$ is equivalent to $z \lrcorner x = y$, that is, in an obvious sense, the right-inverse of \lrcorner , which makes sense since, by assumption, the right-translations of \lrcorner are one-to-one. Then a symmetric verification shows that the operation $\tilde{*}$ satisfies the LC-law.

Finally, we consider (1.11). Let r, s belong to S . Put $a = s$ and $b = s * r$. Then the definition of $*$ gives $r = a \lrcorner b$, and the claim then implies $r * s = b \lrcorner a$. Now, owing to the relations $s * r = b$ and $r * s = b \lrcorner a$, the definition of $\tilde{*}$ gives $(r * s) \tilde{*} (s * r) = a$, and the symmetric counterpart of the claim then implies $(s * r) \tilde{*} (r * s) = a \lrcorner b$. We

deduce $(r * s) \tilde{*} (s * r) = s$ and $(s * r) \tilde{*} (r * s) = r$. So (1.11) is satisfied, $(S, *, \tilde{*})$ is an RLC-quasigroup, and, by Lemma 1.8, $(S, *)$ is a bijective RC-quasigroup.

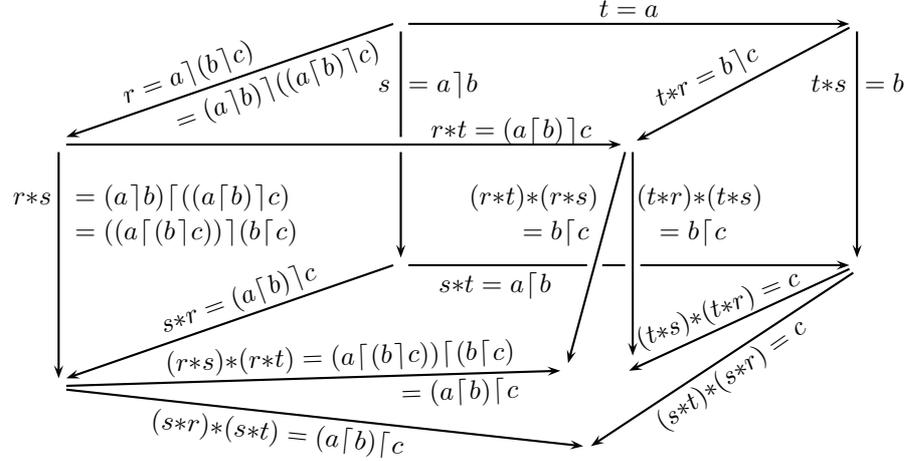


FIGURE 1. Proof of Proposition 1.6(i): one successively evaluates the edges of the cube in terms of a, b, c and the relations (1.3)–(1.5) guarantee that the cube closes. Our convention is to draw a square diagram

$$\begin{array}{ccc} & \xrightarrow{a'} & \\ a \downarrow & & \downarrow b' \\ & \xrightarrow{b} & \end{array} \quad \text{whenever } a' = a \rfloor b \text{ and } b' = a \rfloor b \text{ hold, that is, equivalently,}$$

when $b = a * a'$ and $b' = a' * a$ do. The same diagram can be used to follow the proof of (ii) below, except that one starts with a closed cube and evaluates some edges in two different ways to establish (1.3)–(1.5).

(ii) The argument is similar to that for (i). Owing to Lemma 1.3, it is enough to show that, if \rfloor and \rfloor are defined by

$$(1.14) \quad a \rfloor b = \text{the unique } a' \text{ satisfying } a * a' = b,$$

$$(1.15) \quad a \rfloor b = \text{the unique } b' \text{ satisfying } b' \tilde{*} b = a.$$

where $\tilde{*}$ is determined by the equalities $(s \tilde{*} t) * (t \tilde{*} s) = s$ and $(t \tilde{*} s) * (s \tilde{*} t) = t$ for all s, t , then (S, \rfloor, \rfloor) is an involutive birack. We shall repeatedly use

Claim 2.— For all x, y, z , the relation $z = x * y$ is equivalent to $x \rfloor z = y$ and it implies $x \rfloor z = y * x$.

Proof of Claim 2. Assume $z = x * y$. By definition of \rfloor , this relation is equivalent to $x \rfloor z = y$. Then, by definition of Ψ , we have $\Psi(x, y) = (z, y * x)$, hence $(x, y) = \Psi^{-1}(z, y * x)$. By definition of $\tilde{*}$, this implies $z \tilde{*} (y * x) = x$, whence $z \rfloor x = y * x$ by definition of the operation \rfloor . \square

Now, let a, b, c belong to S . Put $r = a \rfloor (b \rfloor c)$, $s = a \rfloor b$, and $t = a$. We shall now compute the expressions involved in (1.3)–(1.5) in terms of r, s, t , and establish the expected equalities.

First, applying Claim 2 to $s = a \rfloor b$ with $t = a$ gives $b = t * s$ and $a \rfloor b = s * t$.

Next, applying Claim 2 to $r = a \rfloor (b \rfloor c)$ with $t = a$ gives $b \rfloor c = t * r$ and $a \rfloor (b \rfloor c) = r * t$.

Then, applying Claim 2 to $t*r = b]c$ with $t*s = b$ gives $c = (t*s)*(t*r)$, hence also $c = (s*t)*(s*r)$ by (1.7), and $b]c = (t*r)*(t*s)$, hence also $b]c = (r*t)*(r*s)$ by (1.7) again.

Next, the relation $(s*t)*(s*r) = c$ with $(s*t = a]b$ implies $(a]b]c = s*r$, and Claim 2 then implies $(a]b]c = (s*r)*(s*t)$, whence also $(a]b]c = (r*s)*(r*t)$ by (1.7).

Then, the relation $(a]b]c = s*r$ with $s = a]b$ implies $(a]b]((a]b]c) = r$, which, together with the previously established relation $r = a](b]c)$, gives (1.3). By Claim 2, we deduce $(a]b]((a]b]c) = r*s$.

Now, $b]c = (r*t)*(r*s)$ with $r*t = a](b]c)$ implies $r*s = ((a](b]c)](b]c)$ which, together the previously established relation $(a]b]((a]b]c) = r*s$ gives (1.4). Moreover, Claim 2 then implies $(r*s)*(r*t) = (a](b]c)](b]c$ which, together the previously established relation $(a]b]c = (r*s)*(r*t)$ gives (1.5). This completes the proof that $(S,], \lceil, \rceil)$ is a birack.

We conclude with involutivity. Let a, b belong to S . Put $r = a$ and $s = a]b$. By Claim 2, we have $r*s = b$ and $s*r = a]b$, that is, $(a]b)*a = a]b$. By Claim 2 again, the latter is equivalent to $(a]b](a]b) = a$. The argument for $(a]b]((a]b) = b$ is symmetric. \square

Summarizing the results, we conclude that nondegenerate involutive set-theoretic solutions of the Yang–Baxter equation, involutive biracks, and bijective RC-quasi-groups are equivalent frameworks.

Convention 1.9. From now on, we shall write “solution of YBE” for “involutive nondegenerate set-theoretic solution of YBE”.

2. RC-CALCULUS

Our main claim in this paper is that using the formalism of RC-quasigroups significantly helps investigating the solutions of YBE and the derived monoids and groups that will be introduced in Section 3 below. At the technical level, the point is to exploit the RC-law, what we shall do here by introducing sorts of polynomials involving the operation that is supposed to obey the RC-law, plus possibly a symmetric operation obeying the LC-law and a third, associative operation. So our point in this section is to establish some preliminary algebraic relations which altogether make a sort of right-cyclic calculus. Most verifications are easy, but introducing convenient notation is important to obtain simple formulas and perform computations that, otherwise, would require tedious developments.

Everywhere in the sequel, $\tilde{*}$, $*$, and \cdot refer to binary operations.

Definition 2.1. For $n \geq 1$, we inductively define formal expressions $\Omega_n(x_1, \dots, x_n)$ and $\tilde{\Omega}_n(x_n, \dots, x_1)$ by $\Omega_1(x_1) = \tilde{\Omega}_1(x_1) = x_1$ and

$$(2.1) \quad \Omega_n(x_1, \dots, x_n) = \Omega_{n-1}(x_1, \dots, x_{n-1}) * \Omega_{n-1}(x_1, \dots, x_{n-2}, x_n),$$

$$(2.2) \quad \tilde{\Omega}_n(x_1, \dots, x_n) = \tilde{\Omega}_{n-1}(x_1, x_3, \dots, x_n) \tilde{*} \tilde{\Omega}_{n-1}(x_2, \dots, x_n).$$

The expression $\Omega_n(x_1, \dots, x_n)$ —a term in the language of model theory—should be seen as a sort of n -variable monomial and an iteration of the operation $*$. For instance, we find $\Omega_2(x_1, x_2) = x_1 * x_2$, then $\Omega_3(x_1, x_2, x_3) = (x_1 * x_2) * (x_1 * x_3)$, etc. It should be clear that 2^{n-1} variables x_i occur in $\Omega_n(x_1, \dots, x_n)$, with brackets corresponding to a balanced binary tree. For instance, for $n = 4$, the variables occur in the order 12131214 and, for $n = 5$, in the order 1213121412131215.

Of course, whenever $(S, \tilde{*})$ is an algebraic system, we write $\Omega_n(s_1, \dots, s_n)$ for the evaluation of $\Omega_n(x_1, \dots, x_n)$ when x_i is given the value s_n . The next result is an iterated version of the RC-law, which, in terms of the expressions Ω_i , is $\Omega_3(x, y, z) = \Omega_3(y, x, z)$.

Lemma 2.2. *Assume that $(S, *)$ is an RC-system. Then, for all s_1, \dots, s_n in S and π in \mathfrak{S}_{n-1} , we have*

$$(2.3) \quad \Omega_n(s_{\pi(1)}, \dots, s_{\pi(n-1)}, s_n) = \Omega_n(s_1, \dots, s_n).$$

Proof. An induction on n . For $n = 1$ and $n = 2$, there is nothing to prove. For $n = 3$, the equality $\Omega_3(s_1, s_2, s_3) = \Omega_3(s_2, s_1, s_3)$ is the RC-law. Assume $n \geq 4$. As transpositions of adjacent entries generate the symmetric group \mathfrak{S}_n , it is sufficient to prove the result when π is a transposition $(i, i+1)$. For $i < n-2$, the definition plus the induction hypothesis give

$$\begin{aligned} & \Omega_n(s_1, \dots, s_i, s_{i+1}, \dots, s_n) \\ &= \Omega_{n-1}(s_1, \dots, s_i, s_{i+1}, \dots, s_{n-1}) * \Omega_{n-1}(s_1, \dots, s_i, s_{i+1}, \dots, s_{n-2}, s_n) \\ &= \Omega_{n-1}(s_1, \dots, s_{i+1}, s_i, \dots, s_{n-1}) * \Omega_{n-1}(s_1, \dots, s_{i+1}, s_i, \dots, s_{n-2}, s_n) \\ &= \Omega_n(s_1, \dots, s_{i+1}, s_i, \dots, s_n). \end{aligned}$$

For $i = n-2$, writing \vec{s} for s_1, \dots, s_{n-3} , the definition plus the RC-law give

$$\begin{aligned} & \Omega_n(s_1, \dots, s_n) = \Omega_n(\vec{s}, s_{n-2}, s_{n-1}, s_n) \\ &= \Omega_{n-1}(\vec{s}, s_{n-2}, s_{n-1}) * \Omega_{n-1}(\vec{s}, s_{n-2}, s_n) \\ &= (\Omega_{n-2}(\vec{s}, s_{n-2}) * \Omega_{n-2}(\vec{s}, s_{n-1})) * (\Omega_{n-2}(\vec{s}, s_{n-2}) * \Omega_{n-2}(\vec{s}, s_n)) \\ &= (\Omega_{n-2}(\vec{s}, s_{n-1}) * \Omega_{n-2}(\vec{s}, s_{n-2})) * (\Omega_{n-2}(\vec{s}, s_{n-1}) * \Omega_{n-2}(\vec{s}, s_n)) \\ &= \Omega_{n-1}(\vec{s}, s_{n-1}, s_{n-2}) * \Omega_{n-1}(\vec{s}, s_{n-1}, s_n) = \Omega_n(\vec{s}, s_{n-2}, s_{n-1}, s_n). \quad \square \end{aligned}$$

Of course, the counterpart of (2.3) involving $\tilde{\Omega}_n$ is valid when $\tilde{*}$ satisfies the LC-law (1.10). Further results appear when the monomials Ω_n are evaluated in an RC-quasigroup, that is, when left-translations are one-to-one.

Lemma 2.3. *Assume that $(S, *)$ is an RC-quasigroup and s_1, \dots, s_n lie in S .*

- (i) *The map $s \mapsto \Omega_{n+1}(s_1, \dots, s_n, s)$ is a bijection of S into itself.*
- (ii) *There exist r_1, \dots, r_n in S satisfying $\Omega_i(r_1, \dots, r_i) = (s_1, \dots, s_i)$ for $1 \leq i \leq n$.*
- (iii) *Put $\tilde{s}_i = \Omega_n(s_1, \dots, \hat{s}_i, \dots, s_n, s_i)$ for $1 \leq i \leq n$. Then, for all i, j , the relations $s_i = s_j$ and $\tilde{s}_i = \tilde{s}_j$ are equivalent.*

Proof. (i) We use induction on n . For $n = 1$, the considered map is the left-translation $s \mapsto s_1 * s$, a bijection of S into itself by assumption. Assume $n \geq 2$. By definition of Ω_{n+1} , we have $\Omega_{n+1}(s_1, \dots, s_n, s) = t * \Omega_n(s_1, \dots, s_{n-1}, s)$ with $t = \Omega_n(s_1, \dots, s_{n-1})$. By induction hypothesis, the map $s \mapsto \Omega_n(s_1, \dots, s_{n-1}, s)$ is bijective. Hence composing it with the left-translation by t yields a bijection.

(ii) Use once more induction on n . For $n = 1$, take $t_1 = s_1$. Assume $n \geq 2$. By induction hypothesis, there exist r_1, \dots, r_{n-1} satisfying $\Omega_i(r_1, \dots, r_i) = (s_1, \dots, s_i)$ for $1 \leq i \leq n-1$. Then, by definition of Ω_n and owing to $\Omega_{n-1}(r_1, \dots, r_{n-1}) = s_{n-1}$, we have $\Omega_n(r_1, \dots, r_{n-1}, x) = s_{n-1} * \Omega_{n-1}(r_1, \dots, r_{n-2}, x)$. As the left-translation by s_{n-1} is surjective, there exists s satisfying $s_{n-1} * s = s_n$. Then, by (i), there exists r_n satisfying $\Omega_{n-1}(r_1, \dots, r_{n-2}, r_n) = s$, whence $\Omega_n(r_1, \dots, r_n) = s_n$.

(iii) Again an induction on n . For $n = 1$ there is nothing to prove. For $n = 2$, we find $\tilde{s}_1 = s_2 * s_1$ and $\tilde{s}_2 = s_1 * s_1$. It is clear that $s_1 = s_2$ implies $\tilde{s}_1 = \tilde{s}_2$.

Conversely, assume $s_1 * s_2 = s_2 * s_1$. Using the assumption, the RC-law, and the assumption again, we obtain

$$(s_1 * s_2) * (s_2 * s_2) = (s_2 * s_1) * (s_2 * s_2) = (s_1 * s_2) * (s_1 * s_2) = (s_1 * s_2) * (s_2 * s_1).$$

As the left-translations associated with $s_1 * s_2$ and s_2 are injective, we first deduce $s_2 * s_2 = s_2 * s_1$, and then $s_2 = s_1$. Assume now $n \geq 3$. Fix i, j , write \vec{s} for $s_1, \dots, \widehat{s}_i, \dots, \widehat{s}_j, \dots, s_n$ and put $t_k = \Omega_{n-1}(\vec{s}, s_k)$. Then, by (i) and by definition, we have

$$\widetilde{s}_i = \Omega_n(\vec{s}, s_j, s_i) = \Omega_{n-1}(\vec{s}, s_j) * \Omega_{n-1}(\vec{s}, s_i) = t_j * t_i,$$

and, similarly, $\widetilde{s}_j = t_i * t_j$. If $s_i = s_j$ holds, we have $t_i = t_j$, whence $\widetilde{s}_i = \widetilde{s}_j$. Conversely, assume $\widetilde{s}_i = \widetilde{s}_j$, that is, $t_j * t_i = t_i * t_j$. By the result for $n = 2$, we deduce $t_i = t_j$, that is, $\Omega_{n-1}(\vec{s}, s_i) = \Omega_{n-1}(\vec{s}, s_j)$, which is an equality of the form $r_1 * (\dots * (r_{n-2} * s_i) \dots) = r_1 * (\dots * (r_{n-2} * s_j) \dots)$. By applying $n - 2$ times the assumption that the left-translations of $(S, *)$ are injective, we deduce $s_i = s_j$. \square

Further results appear when two operations connected under the involutivity laws (1.11) are involved. In the language of Ω_1 and Ω_2 , (1.11) says that, if we put $\widetilde{s}_1 = \Omega_2(s_1, s_2)$ and $\widetilde{s}_2 = \Omega_2(s_2, s_1)$, then we have $s_1 = \widetilde{\Omega}_2(\widetilde{s}_1, \widetilde{s}_2)$ and $s_2 = \widetilde{\Omega}_2(\widetilde{s}_2, \widetilde{s}_1)$: two elements can be retrieved from their Ω_2 images using the monomial $\widetilde{\Omega}_2$. Here is an n -variable version of this result.

Lemma 2.4. *Assume that $(S, *, \tilde{*})$ is an RLC-system and s_1, \dots, s_n belong to S . For $1 \leq i \leq n$, put $\widetilde{s}_i = \Omega_n(s_1, \dots, \widehat{s}_i, \dots, s_n, s_i)$. Then, for $1 \leq i \leq n$, and for every permutation π in \mathfrak{S}_n , we have*

$$(2.4) \quad \Omega_i(s_{\pi(1)}, \dots, s_{\pi(i)}) = \widetilde{\Omega}_{n+1-i}(\widetilde{s}_{\pi(i)}, \dots, \widetilde{s}_{\pi(n)}).$$

Proof. For $n = 1$, (2.4) reduces to the tautology $s_{\pi(1)} = s_{\pi(1)}$. Now we fix $n \geq 2$ and use induction on i decreasing from n to 1. Assume first $i = n$. Then (2.4) is $\Omega_n(s_{\pi(1)}, \dots, s_{\pi(i)}) = \widetilde{\Omega}_1(\widetilde{s}_{\pi(i)})$. By Lemma 2.2, the left-hand term is also $\Omega_n(s_1, \dots, \widehat{s}_i, \dots, s_{n-1}, s_{\pi(i)})$, which is $\widetilde{s}_{\pi(i)}$ by definition, so (2.4) is satisfied.

Assume now $i < n$. Put

$$\begin{aligned} s &= \Omega_i(s_{\pi(1)}, \dots, s_{\pi(i)}), & s' &= \Omega_i(s_{\pi(1)}, \dots, s_{\pi(i-1)}, s_{\pi(i+1)}), \\ t &= \Omega_{i+1}(s_{\pi(1)}, \dots, s_{\pi(i)}, s_{\pi(i+1)}), & t' &= \Omega_{i+1}(s_{\pi(1)}, \dots, s_{\pi(i-1)}, s_{\pi(i+1)}, s_{\pi(i)}). \end{aligned}$$

Using the definition of Ω_{i+1} from Ω_i , we find $t = s * s'$ and $t' = s' * s$, whence $s = t' \tilde{*} t$ and $s' = t \tilde{*} t'$ by the involutivity law. Now the induction hypothesis gives

$$t = \widetilde{\Omega}_{n-i}(\widetilde{s}_{\pi(i+1)}, \dots, \widetilde{s}_{\pi(n)}), \quad t' = \widetilde{\Omega}_{n-i}(\widetilde{s}_{\pi(i)}, \widetilde{s}_{\pi(i+2)}, \dots, \widetilde{s}_{\pi(n)}).$$

Using the definition of Π_{n+1-i} from Π_{n-i} , we find $s = t' \tilde{*} t = \widetilde{\Omega}_{n+1-i}(\widetilde{s}_{\pi(i)}, \dots, \widetilde{s}_{\pi(n)})$ (and $s' = t \tilde{*} t' = \widetilde{\Omega}_{n+1-i}(\widetilde{s}_{\pi(i+1)}, \widetilde{s}_{\pi(i)}, \widetilde{s}_{\pi(i+2)}, \dots, \widetilde{s}_{\pi(n)})$), which is (2.4). \square

We now introduce terms that involve, in addition to $\tilde{*}$ and $\tilde{\tilde{*}}$, a third operation \cdot that will be evaluated into an associative product.

Definition 2.5. For $n \geq 1$, we introduce the formal expressions

$$(2.5) \quad \Pi_n(x_1, \dots, x_n) = \Omega_1(x_1) \cdot \Omega_2(x_1, x_2) \cdot \dots \cdot \Omega_n(x_1, \dots, x_n)$$

$$(2.6) \quad \widetilde{\Pi}_n(x_1, \dots, x_n) = \widetilde{\Omega}_n(x_1, \dots, x_n) \cdot \widetilde{\Omega}_{n-1}(x_2, \dots, x_n) \cdot \dots \cdot \widetilde{\Omega}_1(x_n).$$

Note that (2.5) implies $\Pi_n(x_1, \dots, x_n) = \Pi_{n-1}(x_1, \dots, x_{n-1}) \cdot \Omega_n(x_1, \dots, x_n)$ for $n \geq 2$. We shall subsequently consider monoids generated by S in which the relations $s(s * t) = t(t * s)$, that is, $\Pi_2(s, t) = \Pi_2(t, s)$, are satisfied. Then we have the following iterated version.

Lemma 2.6. *Assume that $(S, *)$ is an RC-system and M is a monoid including S in which $\Pi_2(s, t) = \Pi_2(t, s)$ holds for all s, t in S . Then the evaluation of Π_n in M is a symmetric function, meaning that, for all s_1, \dots, s_n in S and π in \mathfrak{S}_n , we have*

$$(2.7) \quad \Pi_n(s_{\pi(1)}, \dots, s_{\pi(n)}) = \Pi_n(s_1, \dots, s_n).$$

Proof. We use induction on n . For $n = 1$, there is nothing to prove. For $n = 2$, (2.7) is the equality $s_1(s_1 * s_2) = s_2(s_2 * s_1)$, which is valid in M by assumption. Assume $n \geq 3$. As in Lemma 2.2, it is sufficient to consider transpositions $(i, i+1)$, that is, to compare $\Pi_n(s_1, \dots, s_n)$ and $\Pi_n(s_1, \dots, s_{i+1}, s_i, \dots, s_n)$. By definition, $\Pi_n(s_1, \dots, s_n)$ is the product of the values $\Omega_j(s_1, \dots, s_j)$ for j increasing from 1 to n , whereas $\Pi_n(s_1, \dots, s_{i+1}, s_i, \dots, s_n)$ is a similar product of $\Omega_j(s'_1, \dots, s'_j)$ with $s'_i = s_{i+1}$, $s'_{i+1} = s_i$, and $s'_k = s_k$ for $k \neq i, i+1$. For $j < i$, the entries s_i and s_{i+1} do not occur in $\Omega_j(s_1, \dots, s_j)$ and $\Omega_j(s'_1, \dots, s'_j)$, which are therefore equal. For $j > i+1$, the expressions $\Omega_j(s_1, \dots, s_j)$ and $\Omega_j(s'_1, \dots, s'_j)$ differ by the permutation of two non-final entries, so they are equal by Lemma 2.2. There remains to compare the central entries

$$t = \Omega_i(s_1, \dots, s_i) \cdot \Omega_{i+1}(s_1, \dots, s_{i+1}) \quad \text{and} \quad t' = \Omega_i(s'_1, \dots, s'_i) \cdot \Omega_{i+1}(s'_1, \dots, s'_{i+1}).$$

Now put $r = \Omega_i(s_1, \dots, s_i)$ and $r' = \Omega_i(s_1, \dots, s_{i-1}, s_{i+1})$. By definition of s'_k , we have also $r = \Omega_i(s'_1, \dots, s'_{i-1}, s'_{i+1})$ and $r' = \Omega_i(s'_1, \dots, s'_i)$. Then, by definition of Ω_i and Ω_{i+1} , we have $t = r(r * r')$ and $t' = r'(r' * r)$, whence $t = t'$ in M . \square

Lemma 2.6 says in particular that, when we start with n elements s_1, \dots, s_n and, starting from s_1, \dots, s_n , construct in the Cayley graph of the monoid M the n -cube displayed in Figure 2, then the cube converges to a unique final vertex and all paths from the initial to the final vertex represent the element $\Pi(s_1, \dots, s_n)$.

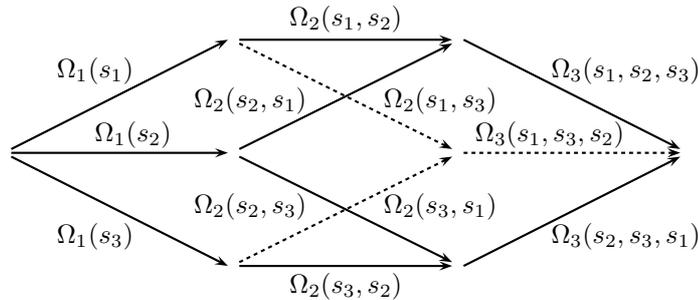


FIGURE 2. The monomials Ω_i occur at the i th level in an n -cube built from s_1, \dots, s_n using $*$ to form elementary squares (here $n = 3$).

Lemma 2.7. *Assume that $(S, *, \tilde{*})$ is an involutive RLC-system and M is a monoid including S in which $\Pi(s, t) = \Pi_2(t, s)$ holds for all s, t in S . Then, for all s_1, \dots, s_n in S , the equality*

$$(2.8) \quad \Pi_n(s_1, \dots, s_n) = \tilde{\Pi}_n(\tilde{s}_1, \dots, \tilde{s}_n).$$

holds for $\tilde{s}_i = \Omega_n(s_1, \dots, \hat{s}_i, \dots, s_n, s_i)$.

Proof. Using (2.4) and the definitions of Π_n and $\tilde{\Pi}_n$, we obtain

$$\begin{aligned} \Pi_n(s_1, \dots, s_n) &= \Omega_1(s_1) \cdot \Omega_2(s_1, s_2) \cdot \dots \cdot \Omega_n(s_1, \dots, s_n) \\ &= \tilde{\Omega}_n(\tilde{s}_1, \dots, \tilde{s}_n) \cdot \tilde{\Omega}_{n-1}(\tilde{s}_2, \dots, \tilde{s}_n) \cdot \dots \cdot \tilde{\Omega}_1(\tilde{s}_n) = \tilde{\Pi}_n(\tilde{s}_1, \dots, \tilde{s}_n). \quad \square \end{aligned}$$

3. STRUCTURE MONOIDS AND GROUPS

According to [14], a group and a monoid can be associated with every (involutive nondegenerate set-theoretic) solution of YBE, hence, equivalently, with every (bijective) RC-quasigroup. As shown by F. Chouraqui in [4], the monoids arising in this way turn out to be Garside monoids [8] and, conversely, every Garside monoid with a certain syntactic type of presentation arises in this way—see also [17]. What we do here is to show how to easily derive such results from the computations of Section 2.

Definition 3.1. The *structure group* (*resp. monoid*) associated with a solution (S, ρ) of YBE is the group (*resp. monoid*) defined by the presentation

$$(3.1) \quad \langle S \mid \{ab = a'b' \mid a, b, a', b' \in S \text{ satisfying } \rho(a, b) = (a', b')\} \rangle.$$

The *structure group* (*resp. monoid*) associated with an RC-quasigroup $(S, *)$ is the group (*resp. monoid*) defined by the presentation

$$(3.2) \quad \langle S \mid \{s(s * t) = t(t * s) \mid s \neq t \in S\} \rangle.$$

As all relations in (3.1) and (3.2) involve positive words only (no inverse), it makes sense to consider the monoid defined by the presentations. Note that (3.1) is redundant and contains trivial relations: as ρ is bijective, most relations occur twice and $\rho_1(a, b) = a$ implies $\rho_2(a, b) = b$ and, in this case, we obtain the trivial relation $ab = ab$.

We know that solutions of YBE and bijective RC-quasigroups are equivalent data. The first observation is that, as can be expected, the associated monoids and groups coincide.

Lemma 3.2. *Assume that a solution (S, ρ) of YBE and a bijective RC-quasigroup are connected as described in Proposition 1.6, that is, $s * t$ is the unique element r of S satisfying $\rho_1(s, r) = t$. Then the structure monoids of (S, ρ) and $(S, *)$ coincide, and so do the corresponding groups.*

Proof. Assume that $ab = a'b'$ is a relation of (3.1). Then, by definition of $*$ from ρ , we have $b = a * a'$ and $b' = a' * a$. If a and a' coincide, the assumption that ρ is nondegenerate implies that b and b' coincide as well, and the relation $ab = a'b'$ is trivial. Otherwise, the relation rewrites as $a(a * a') = a'(a' * a)$, and it is a relation of (3.2).

Conversely, consider a relation $s(s * t) = t(t * s)$ of (3.2). Put $a = s$, $a' = t$, $b = s * t$ and $b' = t' * s'$. Then, by the claim in the proof of Proposition 1.6, we have $a' = a \rfloor b$ and $t' = a \lceil b$ in the language of biracks, that is, $(a', b') = \rho(a, b)$ in the language of solutions of YBE. So the relation $s(s * t) = t(t * s)$, which is $ab = a'b'$, is a relation of (3.1). \square

Thus establishing results for the structure monoids of solutions of YBE and for the structure monoids of bijective RC-quasigroups are equivalent tasks. We shall see now that the second framework is specially convenient.

In the sequel, we often appeal to the divisibility relations of a monoid. If M is a (left)-cancellative monoid and f, g belong to M , we say that f *left-divides* g or, equivalently, that g is a *right-multiple* of f , denoted $f \preceq g$, if $fg' = g$ holds for some g' in M . If 1 is the only invertible element in M , the relation \preceq is a partial ordering on M . We say that h is a *least common right-multiple*, or *right-lcm*, of f and g if h is a least upper bound of f and g with respect to \preceq , that is, if h is a common right-multiple of f and g and every common right-multiple of f and g is a right-multiple of h . Always under the assumption that 1 is the only invertible element in the ambient monoid, the right-lcm is unique when it exists. If f and g admit a right-lcm, the *right-complement* $f \setminus g$ of f in g is the unique element g' such that fg' is the right-lcm of f and g . As already mentioned in Example 1.5, the operation \setminus obeys the RC-law whenever any two elements of the ambient monoid admit a right-lcm. Of course, we have symmetric counterparts involving the right-divisibility relation, where f is said to *right-divide* g if $g = g'f$ holds for some g' .

Here is the result we shall establish. The definitions of a Garside family and a Garside monoid will be recalled below.

Proposition 3.3. *Assume that $(S, *)$ is a bijective RC-quasigroup and M, G are the associated structure monoid and group.*

- (i) *The monoid M contains no nontrivial invertible element, it is Noetherian, and its atoms are the elements of S .*
- (ii) *The monoid M is a Ore monoid, it admits unique left- and right-lcms and left- and right-gcds, and G is a group of left- and right-fractions for M ; this group is torsion-free.*
- (iii) *The structure $(S, *)$ can be retrieved from M : the set S is the set of atoms of M and, for s, t in S , $s * t$ is the right-complement $s \setminus t$ for $s \neq t$, and is the unique element of $S \setminus \{s \setminus t \mid t \neq s \in S\}$ otherwise.*
- (iv) *The right-lcm Δ_I of a cardinal n subset I of S belongs to S^n , it is the left-lcm of (another) cardinal n subset of S , the map $I \mapsto \Delta_I$ is injective, and its image is the smallest Garside family containing 1 in M .*
- (v) *If S is finite with n elements and Δ is the right-lcm of S in M , then M is a Garside monoid with Garside element Δ , and G is its group of fractions; the family of divisors of Δ in M has 2^n elements, and Δ is also the left-lcm of S .*

Of course, there exists a similar statement starting from the assumption that M and G are associated with a solution (S, ρ) of YBE, the only difference being that, in (iii) becomes “For a, b in S , the value of $\rho(a, b)$ is determined by $\rho(a, b) = (a', a' \setminus a)$ if there exists a' in M satisfying $a \setminus a' = b$, and $\rho(a, b) = (a, b)$ otherwise”.

Most of the properties listed in Proposition 3.3 appear in a close form in [4]. Our point here is to observe that using the RC-calculus of Section 2 gives short arguments, a large part of which do not require the assumption that the considered RC-quasigroup is bijective. We shall go in several steps.

Lemma 3.4. *Assume that $(S, *)$ is an RC-quasigroup and M is the associated monoid.*

- (i) *The monoid M has no nontrivial invertible element and is Noetherian, that is, there is no infinite descending sequence with respect to left- or right-divisibility.*
- (ii) *It is left-cancellative, and any two elements of M admit a unique right-lcm and a unique left-gcd.*

(iii) *The system $(S, *)$ can be retrieved from M : the set S is the set of atoms of M and, for $s \neq t$, the value of $s * t$ is the right-complement $s \setminus t$ in M and the value of $s * s$ is the unique element of $S \setminus \{s \setminus t \mid t \neq s \in S\}$.*

Proof. (i) The relations of the presentation (3.2) preserve the length, that is, an S -word can be equivalent to another S -word of the same length only. In particular, if u is a nonempty S -word, then uv cannot be equivalent to the empty word and, therefore, the element of M represented by u cannot be invertible. More generally, the length of S -words induces a well-defined length for the elements of M : if f is a proper left- or right-divisor of g , then the length of f must be strictly less than the length of g , so no infinite descending sequence with respect to left- or right-divisibility may exist in M .

(ii) The presentation (3.2) contains exactly one relation of the form $s... = t...$ for each pair of generators s, t in S . There exists for such presentations, which are called *right-complemented*, a general approach that enables one to easily establish properties of the associated monoid provided the latter is Noetherian, as is the case for M by (i). The point is as follows. Assume we consider a monoid generated by a set S and relations of the form $s\theta(s, t) = t\theta(t, s)$ where θ is a map from $S \times S$ to S (or, more generally to the family S^* of all S -words). Then, by [9, Prop. 6.1 and 6.9] (or [11, Prop. II.4.16]), it is known that, whenever the ‘‘cube condition’’

$$(3.3) \quad \theta(\theta(r, s), \theta(r, t)) = \theta(\theta(s, r), \theta(s, t))$$

holds for all r, s, t in S , the involved monoid is left-cancellative, any two of its elements admit a right-lcm, and the right-lcm of distinct elements s, t of S is $s(s * t)$ (and $t(t * s)$). In the current case of M , the map θ coincides with the operation $*$, and the assumption that $(S, *)$ obeys the RC-law guarantees that (3.3) is satisfied. Hence M is left-cancellative and any two elements of M admit a right-lcm. In a Noetherian context, this implies that any two elements also admit a left-gcd, that is, a greatest lower bound with respect to the left-divisibility relation.

(iii) As there is no relation involving a word of length one in (3.2), the elements of S are atoms, and every element not lying in $S \cup \{1\}$ is not an atom. So S is the atom set of M . Next, for distinct s, t in S , the right-lcm of s and t is $s(s * t)$, so, by definition, $s \setminus t$ is equal to $s * t$. Thus all nondiagonal values $s * t$ can be retrieved from M . Finally, all left-translations of $(S, *)$ are one-to-one, so $s * s$ must be the unique element of $S \setminus \{s * t \mid s, t \in S, s \neq t\}$, that is, of $S \setminus \{s \setminus t \mid t \neq s \in S\}$. \square

At this point, we can establish the first three items in Proposition 3.3.

Proof of Proposition 3.3(i)–(iii). Points (i) and (iii) directly appear in Lemma 3.4. As for (ii), Lemma 3.4(ii) guarantees left-cancellativity and existence of right-lcms and left-gcds, so what is missing is the symmetric counterpart involving right-cancellativity and right-divisibility. For this, we use the assumption that the RC-quasigroup $(S, *)$ is bijective. Indeed, let $\tilde{*}$ be the operation on S provided from $*$ by Lemma 1.8. Then $(S, *, \tilde{*})$ is an RLC-quasigroup, and $(S, \tilde{*})$ is a bijective LC-quasigroup. Moreover the presentation

$$(3.4) \quad \langle S \mid \{(s \tilde{*} t)t = (t \tilde{*} s)s \mid s \neq t \in S\} \rangle^+$$

coincides with the one of (3.2), and therefore it is a presentation of M . Indeed, let $(s \tilde{*} t)t = (t \tilde{*} s)s$ be a relation of (3.4). Put $s' = s \tilde{*} t$ and $t' = t \tilde{*} s$. As $(S, *, \tilde{*})$ is involutive, we obtain $s' * t' = (s \tilde{*} t) * (t \tilde{*} s) = t$ and $t' * s' = (t \tilde{*} s) * (s \tilde{*} t) = s$ by (1.11), so the above relation is the relation $s'(s' * t') = t'(t' * s')$ of (3.2). A symmetric

argument shows that every relation of (3.2) is a relation of (3.4). Then, by the counterpart of Lemma 3.4—or by Lemma 3.4 applied to the opposed monoid M^{opp} and to the RC-quasigroup $(S, \tilde{*}^{\text{opp}})$ — M must be right-cancellative and admit left-lcms and right-gcds. Hence M is in particular a Ore monoid (that is, a cancellative monoid where any two elements admit common left- and right-multiples). By a classical theorem of Ore [6], its enveloping group G , which admits as a group the presentation (3.2), is a group of left- and right-fractions for M . It is then known [10] that the group of fractions of a torsion-free monoid is torsion-free. \square

For the next properties, we use RC-calculus. The point is that the “polynomials” Π_n characterize right-lcms.

Lemma 3.5. *Assume that $(S, *)$ is an RC-quasigroup and M is the associated monoid. Then, for all s_1, \dots, s_n in S , the following are equivalent:*

- (i) *The elements s_1, \dots, s_n are pairwise distinct;*
- (ii) *The element $\Pi_n(s_1, \dots, s_n)$ is the right-lcm of s_1, \dots, s_n in M .*

*If the above relations hold and, in addition, $(S, *)$ is bijective, $\Pi_n(s_1, \dots, s_n)$ is also the left-lcm of the elements $\tilde{s}_1, \dots, \tilde{s}_n$ defined by $\tilde{s}_i = \Omega_n(s_1, \dots, \widehat{s}_i, \dots, s_n, s_i)$.*

Proof. Assume first that s_1, \dots, s_n are pairwise distinct in S . Let Ω'_n and Π'_n be the counterparts of Ω_n and Π_n respectively where the right-complement operation \setminus replaces $*$. We first prove using induction on i the equality

$$(3.5) \quad \Omega_i(s_{\pi(1)}, \dots, s_{\pi(i)}) = \Omega'_i(s_{\pi(1)}, \dots, s_{\pi(i)})$$

for every i and every permutation π in \mathfrak{S}_i . For $i = 1$, we have $\Omega_1(s_{\pi(1)}) = s_{\pi(1)} = \Omega'_1(s_{\pi(1)})$, and the result is straightforward. Assume $n \geq 2$. Put

$$\begin{aligned} s &= \Omega_i(s_{\pi(1)}, \dots, s_{\pi(i)}) & \text{and} & & s' &= \Omega_i(s_{\pi(1)}, \dots, s_{\pi(i-2)}, s_{\pi(i)}, s_{\pi(i-1)}), \\ t &= \Omega_i(s_{\pi(1)}, \dots, s_{\pi(i)}) & \text{and} & & t' &= \Omega_{i-1}(s_{\pi(1)}, \dots, s_{\pi(i-2)}, s_{\pi(i)}). \end{aligned}$$

By definition of Ω_i from Ω_{i-1} , we have $s = t * t'$ and $s' = t' * t$. By Lemma 2.3 applied to $(s_{\pi(1)}, \dots, s_{\pi(i)})$, the assumption $s_{\pi(i-1)} \neq s_{\pi(i)}$ implies $s \neq s'$, which implies $t * t' \neq t' * t$. By Lemma 3.4, the latter relation implies $t * t' = t \setminus t'$ and $t' * t = t' \setminus t$ in M . The induction hypothesis implies

$$t = \Omega'_i(s_{\pi(1)}, \dots, s_{\pi(i)}) \quad \text{and} \quad t' = \Omega'_{i-1}(s_{\pi(1)}, \dots, s_{\pi(i-2)}, s_{\pi(i)}),$$

so we deduce $s = t \setminus t' = (\Omega'_i(s_{\pi(1)}, \dots, s_{\pi(i)})) \setminus (\Omega'_{i-1}(s_{\pi(1)}, \dots, s_{\pi(i-2)}, s_{\pi(i)}))$, that is, $s = \Omega'_i(s_{\pi(1)}, \dots, s_{\pi(i)})$.

Now, (3.5) implies the equalities $\Pi_n(s_1, \dots, s_n) = \Pi'_n(s_1, \dots, s_n)$, which is (ii). Indeed, a trivial induction using the defining property of the right-complement operation shows that $\Pi'_n(s_1, \dots, s_n)$ is the right-lcm of s_1, \dots, s_n for every n . So (i) implies (ii).

For the other direction, let n' be the cardinal of $\{s_1, \dots, s_n\}$. Point (i) implies that, if I is a cardinal n' subset of S , then the right-lcm Δ_I of I has length n' in M . So, if $n' < n$ holds, the right-lcm of $\{s_1, \dots, s_n\}$ is an element of M that has length n' , and it cannot be $\Pi_n(s_1, \dots, s_n)$ which, by definition, has length n . So (ii) implies (i).

Finally, assume that $(S, *)$ is bijective and (i)–(ii) are satisfied. Let $\tilde{*}$ be the second operation provided by Lemma 1.8. Then $(S, *, \tilde{*})$ is an RLC-quasigroup. By Lemma 2.3, the assumption that s_1, \dots, s_n are pairwise distinct implies that $\tilde{s}_1, \dots, \tilde{s}_n$ are pairwise distinct. Then $(S, \tilde{*})$ is an LC-quasigroup, so the counterpart

of the above results implies that $\tilde{\Pi}_n(\tilde{s}_1, \dots, \tilde{s}_n)$ is a left-lcm of $\tilde{s}_1, \dots, \tilde{s}_n$ in M . Now, by (2.8), $\tilde{\Pi}_n(\tilde{s}_1, \dots, \tilde{s}_n)$ is equal to $\Pi_n(s_1, \dots, s_n)$. \square

We recall from [12] that a Garside family in a monoid M is a generating family Σ such that every element of M admits a (unique) Σ -normal decomposition, meaning a decomposition $s_1 \cdots s_p$ such that, for every i , the element s_i is the greatest left-divisor of $s_i \cdots s_p$ lying in Σ .

Lemma 3.6. *Assume that $(S, *)$ is an RC-quasigroup and M is the associated monoid. Then there exists a smallest Garside family containing 1 in M , namely the family Σ of all right-lcms of finite subsets of S . Mapping a finite subset of S to its right-lcm defines a bijection from $\mathfrak{F}_{fin}(S)$ to Σ .*

Proof. We know that the monoid M is left-cancellative, Noetherian, and that any two elements of M admit a right-lcm. Hence, by [12, Prop. 3.25] (or [11, Prop. IV.2.46]), M admits a smallest Garside family Σ , namely the closure of the atoms, that is, of S , under the right-lcm and right-complement operations. We claim that Σ coincides with the closure Σ' of S under the sole right-lcm operation.

By definition, Σ' is included in Σ , and the point is to prove that Σ' is closed under the right-complement operation. Now, this will follow from the formula

$$(3.6) \quad f \setminus \text{lcm}(g_1, \dots, g_n) = \text{lcm}(f \setminus g_1, \dots, f \setminus g_n),$$

which holds in a monoid that admits unique right-lcms as shows an easy induction from $f \setminus \text{lcm}(g, h) = \text{lcm}(f \setminus g, f \setminus h)$, which itself follows from the fact that the right-lcm of f, g, h is both the right-lcm of $\text{lcm}(f, g)$ and $\text{lcm}(f, h)$, and that of f and $\text{lcm}(g, h)$. So assume that g belongs to Σ' , that is, g is a right-lcm of elements t_1, \dots, t_n of S . If f lies in S , then, for every i , the element $f \setminus t_i$ belongs to $S \cup \{1\}$ since it is either $f * t_i$, if f and t_i are distinct, or 1, if f and t_i coincide. Then (3.6) shows that $f \setminus g$ belongs to Σ' for every f in S . Using induction on the length of f , we deduce a similar result for every f in M from the formula $(f_1 f_2) \setminus g = f_2 \setminus (f_1 \setminus g)$. So Σ' is closed under \setminus , it coincides with Σ , and it is the smallest Garside family containing 1 in M .

For I a finite subset of S , write Δ_I for the right-lcm of I . Lemma 3.5 implies that, if I has p elements, say s_1, \dots, s_p , then Δ_I is equal to $\Pi_p(s_1, \dots, s_p)$. So, in particular, Δ_I has length p . Now, assume that I, J are finite subsets of S and $\Delta_I = \Delta_J$ holds. Then every element of $I \cup J$ left-divides Δ_I , so we must have $\Delta_{I \cup J} = \Delta_I = \Delta_J$. It follows that $I \cup J$ has the same cardinal as I and J , implying $I = I \cup J = J$. So the map $I \mapsto \Delta_I$ is a bijection of $\mathfrak{F}_{fin}(S)$ to Σ . \square

Finally, we turn to the property of being a Garside monoid. We recall from [8] that a monoid M is said to be a *Garside monoid* if it is cancellative, Noetherian, every two elements admit left- and right-lcms and gcds, and it admits a Garside element, defined to be an element Δ such that the left- and right-divisors of Δ coincide, generate the monoid, and are finite in number. In such a case, the family consisting of all divisors of Δ is a (finite) Garside family in M .

Lemma 3.7. *Assume that $(S, *)$ is a finite bijective RC-quasigroup of cardinal n and M is the associated monoid. Then the right-lcm Δ of S is a Garside element in M , it admits 2^n (left- or right-) divisors, and M is a Garside monoid.*

Proof. As in Lemma 3.6, write Δ_I for the right-lcm of I for $I \subseteq S$, and write Δ for Δ_S . By Lemma 3.6, the family Σ of all elements Δ_I is the smallest Garside

family containing 1 in M , and it has 2^n elements. By definition, Δ_I left-divides Δ_S , that is, every element of Σ left-divides Δ , and, moreover, Δ lies in Σ . By definition, this means that the Garside family Σ is what is called right-bounded by Δ [11, Def. VI.1.1], and Δ is a right-Garside element in M .

Now, by Lemma 1.8, the assumption that $(S, *)$ is bijective guarantees the existence of a second operation $\tilde{*}$ such that $(S, *, \tilde{*})$ is an RLC-quasigroup, and M is then also associated (in the obvious symmetric sense) with $(S, \tilde{*})$. The counterparts of the above results are therefore satisfied and, in particular, M is right-cancellative. So M is a cancellative monoid with no nontrivial invertible element, every two elements of M admit a right-lcm, and S is a finite subset of M that generates M and is closed under the right-complement operation. By [8, Prop. 2.1], M is a Garside monoid. \square

Completing the proof of Proposition 3.3 is now straightforward.

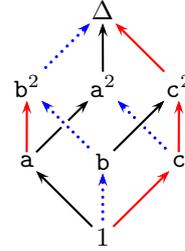
Proof of Proposition 3.3(iv) and (v). Lemma 3.6 gives most results in (iv), with the exception of the property involving left-lcms. Now the latter follows from the last sentence in Lemma 3.5: if s_1, \dots, s_n are pairwise distinct elements of S , then $\Pi_n(s_1, \dots, s_n)$ is the right-lcm of s_1, \dots, s_n and the latter is also the left-lcm of the elements $\tilde{s}_1, \dots, \tilde{s}_n$ defined by $\tilde{s}_i = \Omega_n(s_1, \dots, \hat{s}_i, \dots, s_n, s_i)$.

Finally, (v) follows from Lemma 3.7 directly. \square

Example 3.8. Let $S = \{a, b, c\}$, and let $*$ be determined by $x * y = f(y)$ where f is the cycle $a \mapsto b \mapsto c \mapsto a$. Then, as seen in Example 1.5, $(S, *)$ is a bijective RC-quasigroup, and it is eligible for the above results. The associated monoid admits the presentation

$$\langle a, b, c \mid ac = b^2, a^2 = cb, ba = c^2 \rangle.$$

The right-lcm Δ of S is then a^3 , which is also b^3 and c^3 , and the lattice of the 8 divisors of Δ is shown on the right.



Remark 3.9. The notion of a Garside family is *not* symmetric: it involves normal decompositions based on a largest left-divisor, and it need not coincide with its symmetric counterpart. So, for instance, the uniqueness of the smallest Garside family in M cannot be invoked in Lemma 3.7 to establish that the right-lcm of S must coincide with the left-lcm of S without using the finiteness of Σ and Garside theory. On the other hand, observe that the proof of Lemma 3.7 does not require that $(S, *)$ be bijective.

4. THE OTHER DIRECTION

We saw in Section 3 that, if (S, ρ) is a solution of the YBE or, equivalently, $(S, *)$ is a bijective RC-quasigroup, and S has cardinality n , then the associated monoid is a Garside monoid with a Garside element Δ admitting 2^n elements. Moreover, by definition, this Garside monoid admits a presentation containing $\binom{n}{2}$ relations involving length two words, and the assumption that the left-translations of $(S, *)$ are one-to-one implies that no word may appear in two relations simultaneously. What we shall see now is that, conversely, every Garside monoid with the above properties is associated with a (bijective) RC-quasigroup (hence with a solution of YBE). Once again, the YBE part of the result is essentially present in [4]

and the point here is to show that using the RC-law provides simple arguments (different from those of [4]).

Proposition 4.1. *Assume that M is a monoid with atom set S of cardinal n . Then the following are equivalent:*

- (i) *There exists a map ρ such that (S, ρ) is a solution of YBE and M is isomorphic to the structure monoid of (S, ρ) ;*
- (ii) *There exist two operations $*$, $\tilde{*}$ such that $(S, *, \tilde{*})$ is an RLC-quasigroup and M is the monoid associated with $(S, *)$;*
- (iii) *There exists an operation $*$ such that $(S, *)$ is a bijective RC-quasigroup and M is the monoid associated with $(S, *)$;*
- (iv) *The monoid M is a Garside monoid and admits a presentation in terms of S consisting of $\binom{n}{2}$ relations $u = v$ with u, v of length two such that every length two S -word appears in at most one relation.*

Proof. We proved in Section 1 that (i) and (ii) are equivalent, and that (ii) and (iii) are equivalent. Hence, in order to complete the proof, it is sufficient to show that (iv) implies (ii). So we assume that M is a Garside monoid satisfying (iv) and R is the list of relations involved in the considered presentation. We shall construct operations $*$ and $\tilde{*}$ that make S into an RLC-quasigroup whose associated monoid is M . To this end, we use the right- and left-complement operations of M : we recall that, for f, g in M , we denote by $f \setminus g$ the (unique) element (right-complement of f in g) such that $f(f \setminus g)$ is the right-lcm of f and g . Symmetrically, we denote by f / g the (unique) element such that $(f / g)g$ is the left-lcm of f and g . Then the operation \setminus obeys the RC-law, whereas $/$ obeys the LC-law. We shall define $*$ as a slight variation of \setminus , and $\tilde{*}$ as a slight variation of $/$, the point being to take care of the exceptional values where the operations \setminus and $*$ do not coincide.

First, we observe that the list of relations R must contain exactly one relation of the form $s\dots = t\dots$ for all distinct s, t in S . Indeed, assume that s, t are distinct elements of Σ and R contains at least two relations $s\dots = t\dots$, say $st' = ts'$ and $st'' = ts''$ with $(s', t') \neq (s'', t'')$. As M is cancellative, we have $st' \neq st''$, so st' and st'' are two common right-multiples of s and t of length 2: this contradicts the existence of a right-lcm for s and t , as the latter can have neither length 1 nor length 2. Hence R contains at most one relation $s\dots = t\dots$ for all distinct s, t in S . On the other hand, R contains no relation $s\dots = s\dots$ since M is left-cancellative and $st = st'$ would imply $t = t'$. As there are $\binom{n}{2}$ pairs of distinct elements of S , we deduce that R contains exactly one relation of the form $s\dots = t\dots$ for all distinct s, t in S . By symmetric arguments using left-lcms and right-cancellativity (or by applying the previous result to the opposite monoid), we see that (S, R) contains exactly one relation of the form $\dots s = \dots t$ for all distinct s, t in S .

We now define a binary operation $*$ on S . First, we put $s * t = s \setminus t$ for $s \neq t$, that is, we define $s * t$ to be the unique element t' such that st' is the right-lcm of s and t . Then $t \neq t'$ implies $s * t \neq s * t'$ since, otherwise, there would be two relations of the form $s(s * t) = \dots$ in R . So the map $x \mapsto s * x$ is injective on $\Sigma \setminus \{s\}$ and, therefore, the complement of $\{s * x \mid x \neq s\}$ in S consists of a unique element: we define $s * s$ to be that element. In this way, we obtained a binary operation $*$ whose left-translations are one-to-one. Of course, we define the operation $\tilde{*}$ symmetrically using $/$, and its right-translations are one-to-one.

We claim that $*$ and $\tilde{*}$ satisfy the involutivity laws (1.11). First, assume $s \neq t$. Then $s(s * t) = t(t * s)$ is a relation of R , hence we must have $s * t \neq t * s$. Next, by

definition of $*$ and $\tilde{*}$, the element $s(s*t)$ is the right-lcm of s and t , and, as $s*t$ and $t*s$ are distinct, $s(s*t)$ is also the left-lcm of $s*t$ and $t*s$. This means that $(s*t)\tilde{*}(t*s) = t$ holds in this case. Now, put $s' = s*s$ and $r = s'\tilde{*}s'$. For $t \neq s$, we have $s*t \neq s'$, whence $r = s'/(s\backslash t)$. Then $r(s\backslash t) = ((s\backslash t)/s')s'$ is a relation of R , which implies $(s\backslash t)/s' \neq s$ since, by assumption, R contains no relation $ss' = \dots$. Since $(s\backslash t)/s' \neq s$ holds for every t distinct of s , we deduce $s'\tilde{*}s' = s$ since, by definition, $s'\tilde{*}s'$ is the only element of S that is not of the form $(s\backslash t)\tilde{*}s'$ with $t \neq s$. In other words, $(s*s)\tilde{*}(s*s) = s$ holds, and the first involutivity law is satisfied in $(S, *, \tilde{*})$. By a symmetric argument, the second involutivity law is satisfied as well.

Next, we claim that $(S, *)$ satisfies the RC-law. Let r, s, t lie in S . Assume first that r, s, t are pairwise distinct. Then we have $r*s \neq r*t$ and $s*r \neq s*t$, whence

$$(r*s)*(r*t) = (r\backslash s)\backslash(r\backslash t) = (s\backslash r)\backslash(s\backslash t) = (s*r)*(s*t),$$

the second equality because, as observed in Example 1.5, the right-complement operation \backslash always satisfies the RC-law. Assume now that r and s coincide. Then the RC-law tautologically holds. So there only remains the cases when $r \neq s$ and t is either r or s , that is, we would like to establish the equalities

$$(r*s)*(r*s) = (s*r)*(s*s) \text{ and } (s*r)*(s*r) = (r*s)*(r*r),$$

that is, owing to $r \neq s$,

$$(4.1) \quad (r\backslash s)*(r\backslash s) = (s\backslash r)\backslash(s*s) \text{ and } (s\backslash r)*(s\backslash r) = (r\backslash s)\backslash(r*r).$$

Assume $z \neq r, s$ and put $z' = (r\backslash s)\backslash(r\backslash z)$, which is also $z' = (s\backslash r)\backslash(s\backslash z)$ since \backslash satisfies the RC-law. Then we have $r\backslash z \neq r\backslash s$, whence $z' \neq (r\backslash s)*(r\backslash s)$. Also, we have $s\backslash z \neq s*s$, whence $z' \neq (s\backslash r)\backslash(s*s)$. Arguing similarly with r and s exchanged, we find $z' \neq (s\backslash r)*(s\backslash r)$ and $z' \neq (r\backslash s)\backslash(r*r)$. So, it follows that z' is distinct from the four expressions occurring in (4.1) and, therefore, that the only possible values for the latter are the two elements of S that are not of the form $(r\backslash s)\backslash(r\backslash z)$ with $z \neq r, s$. Now, as left-translations of $*$ are injective, we must have $(r\backslash s)*(r\backslash s) \neq (r\backslash s)\backslash(r*r)$ and $(s\backslash r)\backslash(s*s) \neq (s\backslash r)*(s\backslash r)$. So, in order to conclude that (4.1) is true, it is sufficient to show that $(r\backslash s)*(r\backslash s) = (s\backslash r)*(s\backslash r)$ is impossible. Now $r \neq s$ implies $r*s \neq s*s$, so it is enough to prove that $x \neq y$ implies $x*x \neq y*y$: this follows from the above established involutivity relation $(x*x)\tilde{*}(x*x) = x$.

We are done: $(S, *)$ is an RC-quasigroup, by a symmetric argument $(S, \tilde{*})$ is an LC-quasigroup, and $(S, *, \tilde{*})$ is an RLC-quasigroup. Now, by construction, M admits the presentation (S, R) , so it is (isomorphic to) the monoid associated with $(S, *)$. \square

5. THE I -STRUCTURE

It has been known since [18] and [21] that the monoids associated with solutions of YBE admit a nice geometric characterization as those monoids that admit an I -structure, meaning that their Cayley graph is a twisted copy of that of a free abelian monoid. We observe below that these results can be easily established using the framework of RC-quasigroups and the computational formulas of Section 2. In particular, we shall see that the I -structure can be explicitly determined using the polynomials Π_n .

In view of the final results in Section 6, it is convenient to start with a slightly extended definition in which the reference monoid need not be free Abelian.

Definition 5.1. Assume that M_\bullet and M are monoids generated by a set S . A *right- I -structure of shape (M_\bullet, S)* for M is a bijective map $\nu : M_\bullet \rightarrow M$ satisfying $\nu(1) = 1$, $\nu(s) = s$ for s in S and, for every a in M_\bullet ,

$$(5.1) \quad \{\nu(as) \mid s \in S\} = \{\nu(a)s \mid s \in S\}.$$

When the reference monoid M_\bullet is the S -power of a monoid, we skip S and just say “right- I -structure of shape M_\bullet ”; if M_\bullet is a free Abelian monoid, we also skip M_\bullet and—as is usual—say “right- I -structure”. A monoid is said to be *of right- I -type* if it admits a right I -structure.

The existence of a right- I -structure of shape (M_\bullet, S) on a monoid M provides a bijection from the Cayley graph of M_\bullet relative to S onto that of M that preserves the length of paths but changes the labels. Note that (5.1) is equivalent to the existence, for every a in the reference monoid M_\bullet , of a permutation $\psi(a)$ of S such that, for every s in S , one has

$$(5.2) \quad \nu(as) = \nu(a) \cdot \psi(a)(s).$$

We shall use ψ with this meaning everywhere in the sequel.

If M_\bullet is a free Abelian monoid based on S and, more generally, if every permutation of S induces an automorphism of M_\bullet , then the condition $\nu(s) = s$ for s in S , which amounts to $\psi(1)$ being the identity of S , can be ensured by precomposing ν with the automorphism induced by $\psi(1)^{-1}$ and, therefore, it could be removed from the definition without changing the range of the latter.

Hereafter we denote by $\mathbb{N}^{(S)}$ the free Abelian monoid based on a (finite or infinite) set S , identified with the set of all finite support S -indexed sequences of elements of \mathbb{N} (we use \mathbb{N}^S when S is finite); an element s of S is identified with the sequence whose only non-zero entry is the s -entry, which is 1.

We first prove that the monoid associated with an RC-quasigroup admits a right- I -structure. We shall establish the following explicit version of the result of [18, 21]:

Proposition 5.2. *Assume that $(S, *)$ is an RC-quasigroup and M is the associated monoid. Then the map ν defined from $*$ by $\nu(s_1 \cdots s_n) = \Pi_n(s_1, \dots, s_n)$ is a right I -structure on M .*

Proof. We first define a map ν^* from the free monoid S^* to M by

$$\nu^*(\varepsilon) = 1 \quad \text{and} \quad \nu^*(s_1 | \cdots | s_n) = \Pi_n(s_1, \dots, s_n) \quad \text{for } n \geq 1$$

where $s_1 | \cdots | s_n$ is the length n word with successive letters s_1, \dots, s_n . By Lemma 2.6, the value of $\nu^*(s_1 | \cdots | s_n)$ does not depend on the order of the entries, so the map ν^* induces a well-defined map ν from the free Abelian monoid $\mathbb{N}^{(S)}$ to M . We claim that the latter provides the expected right- I -structure on M . First, the equalities $\nu(1) = 1$ and $\nu(s) = s$ for s in S are obvious. Next, let a belong to $\mathbb{N}^{(S)}$, say $a = s_1 \cdots s_n$. Then the definition of ν gives $\nu(as) = \Pi_{n+1}(s_1, \dots, s_n, s)$, whence $\nu(as) = \Pi_n(s_1, \dots, s_n) \cdot \Omega_{n+1}(s_1, \dots, s_n, s)$. So, by Lemma 2.3(i), the map $s \mapsto \nu(as)$ is a bijection of S into itself, that is, (5.1) holds.

It remains to show that ν is a bijection from $\mathbb{N}^{(S)}$ to M . Let g be an arbitrary element of M , say $g = s_1 \cdots s_n$ with s_1, \dots, s_n in S . By Lemma 2.3(ii), there exist r_1, \dots, r_n in S satisfying $\Omega_i(r_1, \dots, r_i) = (s_1, \dots, s_i)$ for $1 \leq i \leq n$, whence

$\Pi_n(r_1, \dots, r_n) = s_1 \cdots s_n = g$. By definition, this means that $\nu(r_1 \cdots r_n) = g$ holds, and ν is surjective.

Finally, assume that a, a' belong to $\mathbb{N}^{(S)}$ and $\nu(a) = \nu(a')$ holds. As the elements of M have a well-defined length, the length of a and a' must be the same. Write $a = r_1 \cdots r_n$, $a' = r'_1 \cdots r'_n$ with r_1, \dots, r'_n in S . Define $s_i = \Omega_i(r_1, \dots, r_i)$ and $s'_i = \Omega_i(r'_1, \dots, r'_i)$. By definition, $\nu(a)$ is the class of the S -word $s_1 | \cdots | s_n$ in M , whereas $\nu(a')$ is the class of $s'_1 | \cdots | s'_n$. The assumption $\nu(a) = \nu(a')$ means that these S -words are connected by a finite sequence of defining relations of M . By Lemma 2.3, the map $(x_1, \dots, x_n) \mapsto (\Omega_1(x_1), \dots, \Omega_n(x_1, \dots, x_n))$ of $S^{[n]}$ to itself is surjective, so we can assume without loss of generality that $s_1 | \cdots | s_n$ and $s'_1 | \cdots | s'_n$ are connected by one relation exactly, that is, there exist i satisfying

$$s_{i+1} = s_i * s'_i, \quad s'_{i+1} = s'_i * s_i, \quad \text{and} \quad s'_k = s_k \text{ for } k \neq i, i+1.$$

The relations $s'_k = s_k$ inductively imply $r'_k = r_k$ for $k < i$. Next, writing \vec{r} for r_1, \dots, r_{i-1} , we have $s_i = \Omega_i(\vec{r}, r_i)$ and $s'_i = \Omega_i(\vec{r}, r'_i)$. Then, we find

$$\Omega_i(\vec{r}, r_i) * \Omega_i(\vec{r}, r_{i+1}) = \Omega_{i+1}(\vec{r}, r_i, r_{i+1}) = s_{i+1} = s_i * s'_i = \Omega_i(\vec{r}, r_i) * \Omega_i(\vec{r}, r'_i).$$

As the left-translation by $\Omega_i(\vec{r}, r_i)$ is injective, we deduce $\Omega_i(\vec{r}, r_{i+1}) = \Omega_i(\vec{r}, r'_i)$, whence $r_{i+1} = r'_i$ by Lemma 2.3(i). A symmetric argument gives $r'_{i+1} = r_i$. From there, everything is easy and, for $k > i+1$, the relations $s'_k = s_k$ inductively imply $r'_k = r_k$. Indeed, we have

$$\Omega_k(\vec{r}, r_i, r'_i, r_{i+2}, \dots, r_k) = s_k = s'_k = \Omega_k(\vec{r}, r'_i, r_i, r_{i+2}, \dots, r'_k),$$

and, by Lemma 2.2, we know that switching the non-final entries r_i and r'_i in Ω_k changes nothing, and $r'_k = r_k$ follows by Lemma 2.3. We thus proved that the words $r_1 | \cdots | r_n$ and $r'_1 | \cdots | r'_n$ are obtained by switching two (adjacent) entries, hence they represent the same element in the free Abelian monoid $\mathbb{N}^{(S)}$. Hence ν is injective, hence bijective, and it provides the expected right- I -structure on M . \square

Note that Proposition 5.2 does not require the set S to be finite.

We turn to the other direction. We shall prove that every finitely generated monoid of I -type is the structure monoid of some RC-quasigroup:

Proposition 5.3. [18, 21] *If M is a finitely generated monoid of right- I -type, there exists a unique finite RC-quasigroup $(S, *)$ such that M is the structure monoid of $(S, *)$: the set S is the atom set of M and $*$ is determined by $s * t = s \setminus t$ for $s \neq t$ and $\{s * s\} = S \setminus \{s \setminus t \mid t \neq s\}$. Moreover, the right- I -structure on M is unique: it is defined from the operation $*$ by $\nu(s_1 \cdots s_n) = \Pi_n(s_1, \dots, s_n)$.*

We shall give a proof relying the RC-calculus formulas. One of the benefits is to obtain an argument that, although complete, in particular for establishing (5.7) below, may appear shorter than the exposition of [22, Chapter 8]. The other benefit is that a part of the argument (Lemma 5.4) can be extended to a reference Abelian monoid that need not be free, which will be useful in Section 6.

Lemma 5.4. *Assume that M is a left-cancellative monoid and ν is a right- I -structure of shape (M_\bullet, S) on M , where M_\bullet is Abelian and satisfies*

$$(5.3) \quad \forall s, t, s', t' \in S ((s \neq t \text{ and } st' = ts') \Rightarrow (s' = s \text{ and } t' = t)).$$

*Put $s * t = \psi(s)(t)$ for s, t in S . Then $(S, *)$ is an RC-quasigroup.*

Proof. We first claim that, for all s, t, s', t' in S with $s \neq t$, the only equality $st' = ts'$ holding in M is $s(st) = t(t*s)$. Indeed, by assumption, M_\bullet is Abelian and, in M , using (5.2), we obtain

$$s(st) = s\psi(s)(t) = \nu(st) = \nu(ts) = t\psi(t)(s) = t(t*s).$$

On the other hand, assume $st' = ts'$ in M . Let $t'_\bullet = \psi(s)^{-1}(t')$ and $s'_\bullet = \psi(t)^{-1}(s')$. Always using (5.2), we find $\nu(st'_\bullet) = st' = ts' = \nu(ts'_\bullet)$ in M , whence $st'_\bullet = ts'_\bullet$ in M_\bullet since ν is bijective. The assumption on M_\bullet implies $s'_\bullet = s$ and $t'_\bullet = t$, whence $s' = \psi(t)(s) = t*s$ and $t' = \psi(s)(t) = s*t$. This establishes the claim.

Now, let a belong to M_\bullet and s, t belong to S . Using (5.2), we find

$$\nu(ast) = \nu(as) \cdot \psi(as)(t) = \nu(a) \cdot \psi(a)(s) \cdot \psi(as)(t),$$

and, similarly, $\nu(ats) = \nu(a) \cdot \psi(a)(t) \cdot \psi(at)(s)$. By assumption, M_\bullet is Abelian, so we have $ast = ats$, whence $\nu(ast) = \nu(ats)$ and, merging the above expressions and left-cancelling $\nu(a)$, which is legal as M is assumed to be left-cancellative, we find

$$(5.4) \quad \psi(a)(s) \cdot \psi(as)(t) = \psi(a)(t) \cdot \psi(at)(s).$$

Assume first $s \neq t$. The elements $\psi(a)(s)$, $\psi(as)(t)$, $\psi(a)(t)$, and $\psi(at)(s)$ lie in S , so, by the claim above, (5.4) implies

$$(5.5) \quad \psi(as)(t) = \psi(a)(s) * \psi(a)(t) \quad \text{and} \quad \psi(at)(s) = \psi(a)(t) * \psi(a)(s).$$

When t ranges over $S \setminus \{s\}$, the element $\psi(a)(t)$ ranges over $S \setminus \{\psi(a)(s)\}$, and $\psi(a)(s) * \psi(a)(t)$ ranges over $S \setminus \{\psi(a)(s) * \psi(a)(s)\}$. As $\psi(as)$ is a bijection of S , the only possibility is therefore $\psi(as)(s) = \psi(a)(s) * \psi(a)(s)$. In other words, (5.5) is valid in S for all a in M_\bullet and s, t in S .

Now, let r lie in S . Making $a = r$ in (5.5) and applying the definition of $*$ gives $\psi(rs)(t) = (r*s)*(r*t)$ and, similarly, $\psi(sr)(t) = (s*r)*(s*t)$. Now, in M_\bullet , we have $rs = sr$, whence $\psi(rs)(t) = \psi(sr)(t)$, and this gives $(r*s)*(r*t) = (s*r)*(s*t)$, the RC-law. So $(S, *)$ is an RC-system. Moreover, by definition, $\psi(s)$ belongs to \mathfrak{S}_S , so the left-translations of $*$ are one-to-one, and $(S, *)$ is an RC-quasigroup. \square

Lemma 5.5. *Assume that M is a left-cancellative monoid and ν is a right- I -structure of shape (M_\bullet, S) on M , where M_\bullet is Abelian and satisfies (5.3). Then, for every $p \geq 1$ and for all s_1, \dots, s_p in S , we have*

$$(5.6) \quad \psi(s_1 \cdots s_{p-1})(s_p) = \Omega_p(s_1, \dots, s_p) \quad \text{and} \quad \nu(s_1 \cdots s_p) = \Pi_p(s_1, \dots, s_p),$$

where Ω_p and Π_p are associated with $*$ as in Section 2 and values are taken in M . Then, for all a, b in $\mathbb{N}^{(S)}$, we have

$$(5.7) \quad \nu(ab) = \nu(a)\nu(\psi(a)[b]) \quad \text{and} \quad \psi(ab) = \psi(\psi(a)[b]) \circ \psi(a)$$

where $\psi(a)[b]$ is the result of applying $\psi(a)$ to b componentwise.

Proof. We begin with the left equality in (5.6), which is proved using induction on p . For $p = 1$, we have $\psi(1)(s_1) = s_1 = \Omega_1(s_1)$ and, for $p = 2$, we have $\psi(s_1)(s_2) = s_1 * s_2 = \Omega_2(s_1, s_2)$. For $p \geq 3$, using (5.5), the induction hypothesis, and the inductive definition of the monomials Ω_p , we find

$$\begin{aligned} \psi(s_1 \cdots s_{p-1})(s_p) &= \psi(s_1 \cdots s_{p-2})(s_{p-1}) * \psi(s_1 \cdots s_{p-2})(s_p) \\ &= \Omega_{p-1}(s_1, \dots, s_{p-1}) * \Omega_{p-1}(s_1, \dots, s_{p-2}, s_p) = \Omega_p(s_1, \dots, s_p). \end{aligned}$$

The right equality in (5.6) then follows using a similar induction on p . For $p = 1$, we have $\nu(s_1) = s_1 = \Pi(s_1)$. For $p \geq 2$, using (5.2), the left equality in (5.6), and the inductive definition of Π_p , we find

$$\begin{aligned} \nu(s_1 \cdots s_p) &= \nu(s_1 \cdots s_{p-1}) \cdot \psi(s_1 \cdots s_{p-1})(s_p) \\ &= \Pi_{p-1}(s_1, \dots, s_{p-1}) \cdot \Omega_p(s_1, \dots, s_p) = \Pi_p(s_1, \dots, s_p). \end{aligned}$$

The definition of Ω_n implies, for $p, q \geq 1$, the formal equality

$$\Omega_{p+q}(\vec{x}, y_1, \dots, y_q) = \Omega_q(\Omega_{p+1}(\vec{x}, y_1), \dots, \Omega_{p+1}(\vec{x}, y_q)),$$

where \vec{x} stands for x_1, \dots, x_p ; this is a formal identity, not using the RC-law or any specific relation; for instance, it says that $\Omega_3(x, y_1, y_2)$, that is, $(x * y_1) * (x * y_2)$, is also $\Omega_2(\Omega_2(x, y_1), \Omega_2(x, y_2))$. With the same convention, one deduces

$$(5.8) \quad \Pi_{p+q}(\vec{x}, y_1, \dots, y_q) = \Pi_p(\vec{x}) \cdot \Pi_q(\Omega_{p+1}(\vec{x}, y_1), \dots, \Omega_{p+1}(\vec{x}, y_q)).$$

Now, assume that a, b lie in $\mathbb{N}^{(S)}$. Write $a = s_1 \cdots s_p$ and $b = t_1 \cdots t_q$ with s_1, \dots, t_q in S . The right equality in (5.6) gives $\nu(ab) = \Pi_{p+q}(s_1, \dots, s_p, t_1, \dots, t_q)$. On the other hand, we have $\nu(a) = \Pi_p(s_1, \dots, s_p)$ and the left equality in (5.6) implies $\psi(a)(t) = \Omega_{p+1}(s_1, \dots, s_p, t)$ for every t , whence in particular

$$\nu(\psi(a)(t)) = \Pi_q(\Omega_{p+1}(s_1, \dots, s_p, t_1), \dots, \Omega_{p+1}(s_1, \dots, s_p, t_q)).$$

Merging with (5.8), we obtain the left formula in (5.7).

Finally, assume $s \in S$. On the one hand, (5.2) gives $\nu(abs) = \nu(ab)\psi(ab)(s)$. On the other hand, the left formula in (5.7) gives

$$\begin{aligned} \nu(abs) &= \nu(a) \cdot \nu(\psi(a)[bs]) = \nu(a) \cdot \nu(\psi(a)[b] \cdot \psi(a)(s)) \\ &= \nu(a) \cdot \nu(\psi(a)[b]) \cdot \psi(\psi(a)[b])(\psi(a)(s)) = \nu(ab) \cdot \psi(\psi(a)[b])(\psi(a)(s)). \end{aligned}$$

Merging the two expressions and using the assumption that M is left-cancellative, we deduce $\psi(ab)(s) = \psi(\psi(a)[b])(\psi(a)(s))$, which is the right equality in (5.7). \square

Before completing the proof of Proposition 5.3, we establish a few more preparatory results, this time under the assumption that there exists a right- I -structure of shape $(\mathbb{N}^{(S)}, S)$, that is, a genuine right- I -structure.

Lemma 5.6. *Assume that ν is a right- I -structure based on S in a monoid M .*

- (i) *There exists an additive length function on M and S is the atom set in M .*
- (ii) *The map ν is compatible with left-division in the sense that, for all a, b in $\mathbb{N}^{(S)}$, we have $a \preceq b$ in $\mathbb{N}^{(S)}$ if and only if $\nu(a) \preceq \nu(b)$ holds in M .*
- (iii) *The monoid M admits right-lcms.*
- (iv) *If, moreover, S is finite, then M is left-cancellative, and it admits the presentation $\langle S \mid \{s(s \setminus t) = t(t \setminus s) \mid s \neq t \in S\}^+ \rangle$.*

Proof. (i) Defining $\lambda(g)$ to be the length of $\nu^{-1}(g)$ provides a function from M to \mathbb{N} that satisfies $\lambda(1) = 0$, $\lambda(gh) = \lambda(g) + \lambda(h)$, and $\lambda(s) = 1$ for every s in S . It follows that M contains no nontrivial invertible element, that M is Noetherian, and that S is the atom set of M .

(ii) Assume $a \preceq b$ in $\mathbb{N}^{(S)}$. For an induction on length, we may assume $b = as$ with s in S . Now, by (5.2), we have $\nu(b) = \nu(a)\psi(a)(s)$, whence $\nu(a) \preceq \nu(b)$ in M . Conversely, assume $\nu(a) \preceq \nu(b)$. Again, it is enough to consider the case $\nu(b) = \nu(a)s$ with s in S . Now, as $\psi(a)$ is bijective, there exists a unique r in S satisfying

$\psi(a)(r) = s$, and, by (5.2), we have then $\nu(ar) = \nu(a)\psi(a)(r) = \nu(a)s = \nu(b)$, whence $b = ar$ since ν is injective, and $a \preceq b$ in $\mathbb{N}^{(S)}$.

(iii) The monoid $\mathbb{N}^{(S)}$ admits right-lcms, and (ii) enables us to transfer the result to M . So, let g, h belong to M . Put $a = \nu^{-1}(g)$ and $b = \nu^{-1}(h)$. Let ab' be the right-lcm of a and b in $\mathbb{N}^{(S)}$. By (ii), $\nu(ab')$ is a common right-multiple of g and h in M . Now, assume that f is a common right-multiple of g and h in M . By (ii) again, we have $a \preceq \nu^{-1}(f)$ and $b \preceq \nu^{-1}(f)$ in $\mathbb{N}^{(S)}$, whence $ab' \preceq \nu^{-1}(f)$. By (ii) once more, this implies $\nu(ab') \preceq f$ in M . So $\nu(ab')$ is a right-lcm of g and h in M , and M admits right-lcms.

(iv) We assume now that S is finite. Fix g in M , and put $a = \nu^{-1}(g)$. For every b in $\mathbb{N}^{(S)}$, we have $g \preceq g\nu(b)$ in M , whence, by (ii), $a \preceq \nu^{-1}(g\nu(b))$ in $\mathbb{N}^{(S)}$. So, as $\mathbb{N}^{(S)}$ is left-cancellative, there exists a well-defined map ψ from $\mathbb{N}^{(S)}$ to itself such that, for every b in $\mathbb{N}^{(S)}$, we have $\nu^{-1}(g\nu(b)) = a\psi(b)$, that is, equivalently, $g\nu(b) = \nu(a\psi(b))$. Put $\mathbb{N}_{(\ell)}^{(S)} = \{b \in \mathbb{N}^{(S)} \mid \|b\| = \ell\}$. The additivity of length implies $\|\psi(b)\| = \|b\|$, so, for every ℓ , the restriction ψ_ℓ of ψ to $\mathbb{N}_{(\ell)}^{(S)}$ maps $\mathbb{N}_{(\ell)}^{(S)}$ to itself. Then ψ_ℓ is surjective. Indeed, let b' belong to $\mathbb{N}_{(\ell)}^{(S)}$. Then we have $a \preceq ab'$ in $\mathbb{N}^{(S)}$, whence, by (ii), $g \preceq \nu(ab')$ in M . So some element $\nu(b)$ of M satisfies $g\nu(b) = \nu(ab')$, whence $b' = \psi_\ell(b)$ since b must be of length ℓ . As $\mathbb{N}_{(\ell)}^{(S)}$ is finite, ψ_ℓ must be injective for every ℓ , and so is ψ . Now, assume $gh = gh'$ in M . Put $b = \nu^{-1}(h)$ and $b' = \nu^{-1}(h')$. By definition of ψ , we have $\nu(a\psi(b)) = \nu(a\psi(b'))$, whence $a\psi(b) = a\psi(b')$ in $\mathbb{N}^{(S)}$ since ν is injective, then $\psi(b) = \psi(b')$ since $\mathbb{N}^{(S)}$ is left-cancellative, $b = b'$ since ψ is injective and, finally, $h = h'$. So M is left-cancellative.

Finally, as M is Noetherian, left-cancellative, and admits right-lcms, and as S is the atom set of M , it follows from [7, Prop. 4.1] that the list of all relations $s(s \setminus t) = t(t \setminus s)$ with $s \neq t \in S$ make a presentation of M . \square

We can now easily complete the proof of Proposition 5.3.

Proof of Proposition 5.3. Assume that ν is a right- I -structure on M , based on a set S . By Lemma 5.6(i), S must be the atom set of M , and the assumption that M is finitely generated implies that S is finite.

Next, the free Abelian monoid $\mathbb{N}^{(S)}$ satisfies the assumptions of Lemma 5.4 and, therefore, the latter applies. Hence, if we define $s * t = \psi(s)(t)$, then $(S, *)$ is an RC-quasigroup. Moreover, as S is finite, Rump's theorem implies that $(S, *)$ is bijective.

Assume $s \neq t \in S$. By (5.2), we have $s(s * t) = \nu(st) = \nu(ts) = t(t * s)$, whereas, by Lemma 5.6(i), (iii) and (iv), the monoid M admits unique right-lcms and is left-cancellative. It follows that $s(s * t)$ is necessarily the right-lcm of s and t , and we must have $s * t = s \setminus t$. Then Lemma 5.6(iv) implies that M admits the presentation $\langle S \mid \{s(s * t) = t(t * s) \mid s \neq t \in S\}^+ \rangle$, so M is the structure monoid of $(S, *)$.

Finally, the connection between ν and the polynomials Π is given by the right formula in (5.6). The uniqueness of ν follows, as S is the atom set of M , and $*$ is the only possible extension of the right-complement operation outside the diagonal that admits bijective left-translations, so they only depend on M . \square

We refer to [22] for further properties of monoids of I -type. In particular, let us mention that a right- I -structure on a left-cancellative monoid M extends into

a similar map ν from the group of fractions of $\mathbb{N}^{(S)}$, that is, the free Abelian group $\mathbb{Z}^{(S)}$, to the group of fractions of M , still satisfying (5.1) and (5.2). When M is the monoid associated with an RC-quasigroup $(S, *)$, then its group of fractions is the group associated with $(S, *)$.

Relation (5.2) is reminiscent of a semi-direct product. We recall from [21] and [3] that, once the equalities (5.7) are established, one easily deduces the following connection, here in the slightly extended context of Lemma 5.4:

Proposition 5.7. *Assume that M is a left-cancellative monoid and ν is a right- I -structure of shape $N^{(S)}$ on M , where N is either \mathbb{N} or $\mathbb{Z}/d\mathbb{Z}$ for some d . Then the following are equivalent:*

- (i) *The map ν is a right- I -structure of shape $(N^{(S)}, S)$ on M ;*
- (ii) *There exists a map $\psi : N^{(S)} \rightarrow \mathfrak{S}_S$ such that $g \mapsto (\nu^{-1}(g), \psi(\nu^{-1}(g))^{-1})$ defines an injective homomorphism of M to the wreath product $N \wr \mathfrak{S}_S$ whose first component is a bijection.*

Proof. Assume that ν is a right I -structure of shape $N^{(S)}$ on M . As usual, we write ψ for the map from $N^{(S)}$ to \mathfrak{S}_S specified by (5.2). We consider the wreath product $N \wr \mathfrak{S}_S$, that is, the semidirect product $N^{(S)} \rtimes \mathfrak{S}_S$ where \mathfrak{S}_S acts on $N^{(S)}$ by permuting positions. Define $\iota : M \rightarrow N \wr \mathfrak{S}_S$ by $\iota(g) = (\nu^{-1}(g), \psi(\nu^{-1}(g))^{-1})$.

First, ι is injective and its first component is bijective, since ν^{-1} is bijective.

So, the point is to check that ι is a homomorphism. Let g, h belong to M . Putting $a = \nu^{-1}(g)$, $b = \nu^{-1}(h)$, $\sigma = \psi(a)$, and $\tau = \psi(b)$, we find $\iota(g) = (a, \sigma^{-1})$ and $\iota(h) = (b, \tau^{-1})$, whence, in $N \wr \mathfrak{S}_S$,

$$(5.9) \quad \iota(g)\iota(h) = (a\sigma^{-1}[b], \sigma^{-1} \circ \tau^{-1}).$$

On the other hand, the monoid $N^{(S)}$ satisfies (5.3), so Lemma 5.5 applies and, using the left formula in (5.7), we find

$$\nu(a\sigma^{-1}[b]) = \nu(a)\nu(\psi(a)(\sigma^{-1}[b])) = g\nu(\sigma[\sigma^{-1}[b]]) = g\nu(b) = gh,$$

whence $\nu^{-1}(gh) = a\sigma^{-1}[b]$. Using the right formula in (5.7) similarly, we find

$$\psi(a\sigma^{-1}[b]) = \psi(\psi(a)[\sigma^{-1}[b]]) \circ \psi(a) = \psi(\sigma[\sigma^{-1}[b]]) \circ \sigma = \psi[b] \circ \sigma = \tau \circ \sigma.$$

We deduce $\iota(gh) = (a\sigma^{-1}[b], \sigma^{-1} \circ \tau^{-1})$. So, owing to (5.9), ι is a homomorphism, and (i) implies (ii).

Conversely, assume that ν and ψ ensure that ι is an embedding. Then the above computation gives, for all a, b in $N^{(S)}$, the equality $\nu(ab) = \nu(a)\nu(\psi(a)[b])$, whence in particular $\nu(as) = \nu(a)\psi(a)(s)$ for a in $N^{(S)}$ and s in S . So ν is a right- I -structure of shape $(N^{(S)}, S)$ on M , and (ii) implies (i) \square

6. COXETER-LIKE GROUPS

In this final section, we use the RC-calculus of Section 2 and the I -structure of Section 5 and to solve what can be called the quest of a Coxeter group, namely constructing for every group associated with a finite RC-quasigroup a finite quotient that plays the role played by Coxeter groups in the case of spherical Artin–Tits groups.

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 symmetric group \mathfrak{S}_n . Precisely,

the group B_n and the monoid B_n^+ admit the (Artin) presentation

$$(6.1) \quad \left\langle \sigma_1, \dots, \sigma_{n-1} \mid \begin{array}{ll} \sigma_i \sigma_j = \sigma_j \sigma_i & \text{for } |i-j| \geq 2 \\ \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j & \text{for } |i-j| = 1 \end{array} \right\rangle,$$

and \mathfrak{S}_n is the quotient of B_n obtained by adding to (6.1) the relations $\sigma_i^2 = 1$. Then there exists a map σ from \mathfrak{S}_n to B_n that is a set-theoretic section for the projection of B_n to \mathfrak{S}_n , the image of σ is the family $\text{Div}(\Delta_n)$ of all divisors of Δ_n in the monoid B_n^+ , and a presentation both of the group B_n and the monoid B_n^+ in terms of the image of σ consists of all relations $\sigma(f)\sigma(g) = \sigma(h)$ with f, g, h in \mathfrak{S}_n satisfying $\|f\| + \|g\| = \|h\|$, where $\|f\|$ is the length of f , that is, the minimal number of adjacent transpositions in a decomposition of f . Thus the (infinite) group B_n appears as a sort of unfolded version of the group \mathfrak{S}_n where the length of permutations is used to get rid of torsion.

This is the situation we wish to obtain in our current context. To make things precise, we introduce a notion of a germ [12]. If a set S positively generates a group G (that is, every element of G can be expressed as a product of elements of S), we denote by $\|g\|_S$ the length of a shortest S -decomposition of g .

Definition 6.1. Assume that M is a Garside monoid with Garside element Δ and G is its group of fractions. We say that a surjective homomorphism $\pi : G \rightarrow \overline{G}$ provides a Garside germ for (G, M, Δ) if there exists a map $\sigma : \overline{G} \rightarrow M$ such that $\pi \circ \sigma$ is the identity, the image of σ is the family of all divisors of Δ in M , and M admits the presentation

$$(6.2) \quad \langle \sigma(\overline{G}) \mid \{ \sigma(f)\sigma(g) = \sigma(fg) \mid f, g \in \overline{G} \text{ and } \|f\|_{\overline{S}} + \|g\|_{\overline{S}} = \|fg\|_{\overline{S}} \} \rangle,$$

where \overline{S} is the image under π of the atom set of M .

In the context of Definition 6.1, the assumption that Δ is a Garside element in M implies that every element of G can be written as $\Delta^p g$ for some p in \mathbb{Z} and some g in M , implying that \overline{S} positively generates \overline{G} and making $\|g\|_{\overline{S}}$ meaningful. The term *germ* stems from [13, 12] where the *germ* derived from $(\overline{G}, \overline{S})$ is defined to the structure (\overline{G}, \bullet) where \bullet is the partial binary operation such that $f \bullet g = h$ holds if and only if we have $fg = h$ and $\|f\|_{\overline{S}} + \|g\|_{\overline{S}} = \|h\|_{\overline{S}}$. The monoid and the group defined by (6.2) are then said to be generated by the germ (\overline{G}, \bullet) . So the situation described in Definition 6.1 corresponds to (\overline{G}, \bullet) being a germ generating G , which makes the terminology coherent. When it is so, the maps π and σ induce mutually inverse isomorphisms between the finite lattice made by the divisors of Δ in M and $(\overline{G}, \leq_{\overline{S}})$ where $f \leq_{\overline{S}} g$ means $\|f\|_{\overline{S}} + \|f^{-1}g\|_{\overline{S}} = \|g\|_{\overline{S}}$. The Hasse diagram of these partial orders then coincides with the Cayley graph of the germ (\overline{G}, \bullet) with respect to the generating set \overline{S} .

Thus, the above mentioned results for the braid group B_n and the symmetric group \mathfrak{S}_n can be summarized into the statement that collapsing σ_i^2 to 1 for every i provides a Garside germ for (B_n, B_n^+, Δ_n) , with associated quotient \mathfrak{S}_n .

More generally, it is known—see [1] or [11, Chapter IX]—that similar results hold for every Artin–Tits group of spherical type: if (W, S) is a spherical Coxeter system (that is, W and S are finite), and G and M are the associated Artin–Tits group and monoid, and Δ is the smallest Garside element in M , then collapsing s^2 to 1 for every s in S provides a Garside germ for (G, M, Δ) , with associated quotient W .

The above groups are Garside groups, and it is natural to ask whether similar results hold for every Garside group, namely whether some finite quotient provides

a Garside germ, that is, in other words, whether there exists an associated Coxeter-like group enjoying all the nice properties known in the Artin–Tits case. No answer is known so far, but we shall now establish a complete positive answer in the case of groups associated with finite RC-quasigroups. Indeed, we shall attach with every finite RC-quasigroup a parameter called its *class* and prove:

Proposition 6.2. *Assume that $(S, *)$ is an RC-quasigroup of cardinal n and class d . Let G, M be the associated group and monoid, and Δ be the right-lcm of S in M . Then collapsing $s^{[d]}$ to 1 in G for every s in S , where $s^{[d]}$ stands for $\Pi_d(s, \dots, s)$, gives a finite group \overline{G} that provides a Garside germ for (G, M, Δ^{d-1}) . The group \overline{G} has d^n elements and the kernel of the projection is (isomorphic to) \mathbb{Z}^n .*

Definition 6.3. In the framework of Proposition 6.2, the finite group \overline{G} will be called the *Coxeter-like group* associated with $(S, *)$.

The proof, which is not difficult, consists in using the I -structure to carry the results from the (trivial) case of \mathbb{Z}^n to the case of an arbitrary group of I -type. It will be decomposed into several easy steps. First we define the class.

Definition 6.4. An RC-quasigroup $(S, *)$ is said to be of *class d* if it satisfies

$$(C_d) \quad \forall s, t \in S \quad (\Omega_{d+1}(s, \dots, s, t) = t).$$

So an RC-quasigroup is of class 1 if $s * t = t$ holds for all s, t , and it is of class 2 if $(s * s) * (s * t) = t$ holds for all s, t .

Lemma 6.5. *Every RC-quasigroup of cardinal n is of class d for some $d < (n^2)!$.*

Proof. Let $(S, *)$ be a finite RC-quasigroup with cardinal n . By Rump’s theorem, $(S, *)$ must be bijective, that is, the map $\Psi : (s, t) \mapsto (s * t, t * s)$ is bijective on $S \times S$. Consider the map $\Phi : (s, t) \mapsto (s * s, s * t)$ on S^2 . Assume $(s, t) \neq (s', t')$. If s and s' are distinct, we have $\Psi(s, s) \neq \Psi(s', s')$, hence $s * s \neq s' * s'$, and $\Phi(s, t) \neq \Phi(s', t')$. If s and s' coincide, we must have $t \neq t'$, whence $s * t \neq s * t'$ and, again, $\Phi(s, t) \neq \Phi(s', t')$ since left-translations of $*$ are injective. So Φ is injective, hence bijective on the finite set $S \times S$. As $S \times S$ has cardinal n^2 , then order of Φ in $\mathfrak{S}_{S \times S}$ is at most $(n^2)!$. So there exists $d < (n^2)!$ such that Φ^{d+1} is the identity. Now, an easy induction gives $\Phi^m(s, t) = (\Omega_m(s, \dots, s, s), \Omega_m(s, \dots, s, t))$ for every m . So $\Phi^{d+1} = \text{id}$ implies $\Omega_{d+1}(s, \dots, s, t) = t$ for all s, t in S , meaning that $(S, *)$ is of class at most d . \square

There exist finite RC-quasigroups with an arbitrarily high minimal class. Indeed, let $S = \{\mathbf{a}_1, \dots, \mathbf{a}_n\}$, and define $s * t = f(t)$ where f is the cyclic permutation that maps \mathbf{a}_i to $\mathbf{a}_{i+1 \pmod n}$ for every i . Then, for all p, i and s_1, \dots, s_p in S , we have $\Omega_{p+1}(s_1, \dots, s_p, \mathbf{a}_i) = \mathbf{a}_{i+p \pmod n}$. Hence $(S, *)$ is of class d if and only if d is a multiple of n , and the minimal class is n .

We shall establish Proposition 6.2 using the I -structure on the monoid M , which exists by Proposition 5.2. As in Section 5, the I -structure will be denoted by ν , and the associated map from \mathbb{N}^S to \mathfrak{S}_S as defined in (5.2) will be denoted by ψ . As mentioned at the end of Section 5, ν and ψ respectively extend into a bijection from \mathbb{Z}^S to G and a map from \mathbb{Z}^S to \mathfrak{S}_S that still satisfy (5.1) and (5.2).

Lemma 6.6. *Assume that $(S, *)$ is an RC-quasigroup of class d and M is the associated monoid. For s in S and $q \geq 0$, let $s^{[q]} = \Pi_q(s, \dots, s)$. Then*

$$(6.3) \quad \nu(s^d a) = s^{[d]} \nu(a)$$

holds for all s in S and a in $\mathbb{N}^{(S)}$. The permutation $\psi(s^d)$ is the identity and, for all s, t in S , the elements $s^{[d]}$ and $t^{[d]}$ commute in M .

Proof. Let $t_1 \cdots t_q$ be a decomposition of a in terms of elements of S . By Proposition 5.2, we have

$$\begin{aligned} \nu(s^d a) &= \Pi_{d+q}(s, \dots, s, t_1, \dots, t_q) \\ &= \Pi_d(s, \dots, s) \Pi_q(\Omega_{d+1}(s, \dots, s, t_1), \dots, \Omega_{d+1}(s, \dots, s, t_q)) \\ &= \Pi_d(s, \dots, s) \Pi_q(t_1, \dots, t_q) = \nu(s^d) \nu(t_1 \cdots t_q) = s^{[d]} \nu(a), \end{aligned}$$

in which the second equality comes from expanding the terms and the third one from the assumption that M is of class d . Applying with $a = t$ in S and merging with $\nu(s^d t) = \nu(s^d) \psi(s^d)(t)$, we deduce that $\psi(s^d)$ is the identity. On the other hand, applying with $a = t^{[d]}$, we find $s^{[d]} t^{[d]} = \nu(s^d t^d) = \nu(t^d s^d) = t^{[d]} s^{[d]}$. \square

Lemma 6.7. (i) Assume that $(S, *)$ is a finite RC-quasigroup, M is the associated monoid, and $d \geq 2$ holds. Let $\Delta_\bullet = \prod_{s \in S} s$ in \mathbb{N}^S and $\Delta_d = \nu(\Delta_\bullet^{d-1})$. Then we have $\Delta_d = \Delta^{d-1}$ where Δ is the right-lcm of S , and Δ_d is a Garside element in M .

(ii) If, moreover, $(S, *)$ is of class d , then Δ^d and $(\Delta_d)^d$ lie in the centre of M .

Proof. (i) By Lemma 3.5, we have $\Delta = \Pi_n(s_1, \dots, s_n) = \nu(\Delta_\bullet)$, where (s_1, \dots, s_n) is any enumeration of S . In other words, we have $\Delta = \Delta_2$. Now, we observe that $f[\Delta_\bullet] = \Delta_\bullet$ holds in \mathbb{N}^S for every f in \mathfrak{S}_S since every element of S occurs once in the definition of Δ_\bullet . By (5.7), we deduce

$$(6.4) \quad \nu(a \Delta_\bullet) = \nu(a) \nu(\psi(a)[\Delta_\bullet]) = \nu(a) \nu(\Delta_\bullet),$$

whence $\nu(\Delta_\bullet^k) = \nu(\Delta_\bullet)^k$ for every k and, in particular, $\Delta_d = \nu(\Delta_\bullet)^{d-1} = \Delta^{d-1}$. By Lemma 3.7, Δ is a Garside element in M . It is standard that this implies that every power of Δ is also a Garside element, hence, in particular, so is Δ_d .

(ii) Assume now that $(S, *)$ is of class d . Let t belong to S . Then, by (6.4), we obtain $\nu(t \Delta_\bullet^d) = \nu(t) \nu(\Delta_\bullet^d) = t \Delta^d$. On the other hand, (6.4) and (6.3) give

$$(6.5) \quad \Delta^d = \nu(\Delta_\bullet^d) = \prod_{s \in S} s^{[d]} \quad \text{and} \quad \nu(\Delta_\bullet^d t) = \prod_{s \in S} s^{[d]} t = \Delta^d t.$$

Merging the values of $\nu(t \Delta_\bullet^d)$ and $\nu(\Delta_\bullet^d t)$, we obtain $t \Delta^d = \Delta^d t$, so that Δ^d , hence its power $(\Delta_d)^d$ as well, lies in the centre of M . \square

We are now ready to introduce the equivalence relation on \mathbb{Z}^S that, when carried to G , will induce the expected quotient of G (and M).

Definition 6.8. For a, a' in the free Abelian group \mathbb{Z}^S and s in S , we write $a \equiv_\bullet a'$ if $\#_s(a) = \#_s(a') \pmod{d}$ holds for every s in S , where $\#_s(a)$ is the (well-defined) algebraic number of s in any S -decomposition of a .

Lemma 6.9. Assume that $(S, *)$ is an RC-quasigroup of class d and M and G are the associated monoid and group.

(i) For g, g' in M , declare $g \equiv g'$ for $\nu^{-1}(g) \equiv_\bullet \nu^{-1}(g')$. Then \equiv is an equivalence relation on M that is compatible with left- and right-multiplication. The class of 1 is the Abelian submonoid M_1 of M generated by the elements $s^{[d]}$ with s in S .

(ii) For g, g' in G , declare that $g \equiv g'$ holds if there exist h, h' in M and r, r' in \mathbb{Z} satisfying $g = \Delta^{dr} h$, $g' = \Delta^{dr'} h'$, and $h \equiv h'$. Then \equiv is a congruence on G , and the kernel of the projection of G to G/\equiv is the group of fractions of M_1 .

Proof. (i) As ν is bijective, carrying the equivalence relation \equiv_{\bullet} of \mathbb{N}^S to M yields an equivalence relation on M . Assume $g \equiv_{\bullet} g'$. Let $a = \nu^{-1}(g)$ and $a' = \nu^{-1}(g')$. Without loss of generality, we may assume $a' = as^d = s^d a$ for some s in S . Applying (5.7) and Lemma 6.6, we obtain $\psi(a') = \psi(\psi(s^d)[a] \circ \psi(s^d)) = \psi(a)$. Let t belong to S . Using (5.7) again, we deduce

$$\begin{aligned} g \cdot \psi(a)(t) &= \nu(a) \cdot \psi(a)(t) = \nu(at) \\ &\equiv \nu(a't) = \nu(a') \cdot \psi(a')(t) = \nu(a') \cdot \psi(a)(t) = g' \cdot \psi(a)(t). \end{aligned}$$

As $\psi(a)(t)$ takes every value in S when t ranges over S , we deduce that \equiv is compatible with right-multiplication. On the other hand, $a \equiv_{\bullet} a'$ implies $f[a] \equiv_{\bullet} f[a']$ for every permutation f of S . Let t belong to S . Always by (5.7), we obtain

$$t \cdot g = t \cdot \nu(a) = \nu(t \cdot \psi(t)^{-1}[a]) \equiv \nu(t \cdot \psi(t)^{-1}[a']) = t \cdot \nu(a') = t \cdot g',$$

and \equiv is compatible with left-multiplication by S .

The \equiv_{\bullet} -class of 1 in \mathbb{N}^S is the free Abelian submonoid generated by the elements s^d with s in S . The \equiv -class of 1 in M consists of the image under ν of the products of such elements s^d . By Lemma 6.6, the latter are the products of elements $s^{[d]}$.

(ii) First, \equiv is well-defined. As Δ^d is a Garside element in M , every element of G admits an expression $\Delta^{dr}h$ with r in \mathbb{Z} and h in M . This expression is not unique, but, if we have $g = \Delta^{dr}h = \Delta^{dr_1}h_1$ with, say, $r_1 < r$, then, as M is left-cancellative, we must have $h_1 = \Delta^{d(r-r_1)}h$, whence $h_1 \equiv h$ by (6.5). So, for every h' in M , the relations $h \equiv h'$ and $h_1 \equiv h'$ are equivalent.

Then the fact that \equiv is an equivalence relation on G is easy, and its compatibility with multiplication on G follows from the compatibility on M and the fact that Δ^d lies in the centre of G .

Finally, the \equiv -class of 1 in G consists of all elements $\Delta^{dr}h$ with h in M_1 . As Δ^d belongs to M_1 , this is the group of fractions of M_1 in G , hence the free Abelian subgroup of G generated by the elements $s^{[d]}$ with s in S . \square

We can now conclude.

Proof of Proposition 6.2. Let \overline{G} be the quotient-group G/\equiv . By Lemma 6.9, the kernel of the projection of G onto \overline{G} is a free Abelian group of rank n , hence it is isomorphic to \mathbb{Z}^n . The cardinality of \overline{G} is the number of \equiv -classes in G . As every element of G is \equiv -equivalent to an element of M , this number is also the number of \equiv -classes in M , hence the number of \equiv_{\bullet} -classes in \mathbb{N}^S , which is d^n .

By definition, $s^{[d]} \equiv 1$ holds for every s in S . Conversely, the congruence \equiv_{\bullet} on \mathbb{Z}^S is generated by the pairs $(s^d, 1)$ with s in Σ , hence the congruence \equiv on G is generated by the pairs $(s^{[d]}, 1)$ with s in S . Hence a presentation of \overline{G} is obtained by adding to the presentation (3.2) of G the n relations $s^{[d]} = 1$ with s in S .

By construction, the bijection ν is compatible with the congruences \equiv_{\bullet} on \mathbb{Z}^S and \equiv on G , so it induces a bijection $\overline{\nu}$ of $\mathbb{Z}^S/\equiv_{\bullet}$, which is $(\mathbb{Z}/d\mathbb{Z})^S$, onto G/\equiv , which is \overline{G} , providing a commutative diagram

$$(6.6) \quad \begin{array}{ccc} \mathbb{Z}^S & \xrightarrow{\nu} & G \\ \pi_{\bullet} \downarrow & & \downarrow \pi \\ (\mathbb{Z}/d\mathbb{Z})^S & \xrightarrow{\overline{\nu}} & \overline{G} \end{array} .$$

Now, let σ_\bullet be the section of π_\bullet from $(\mathbb{Z}/d\mathbb{Z})^S$ to \mathbb{N}^S that maps every \equiv_\bullet -class to the unique n -tuple of $\{0, \dots, d-1\}^S$ that lies in that class, and let $\sigma : \overline{G} \rightarrow M$ be defined by $\sigma(g) = \nu(\sigma_\bullet(\overline{\nu}^{-1}(g)))$. Then, for every g in \overline{G} , we obtain

$$\pi(\sigma(g)) = \pi(\nu(\sigma_\bullet(\overline{\nu}^{-1}(g))) = \overline{\nu}(\pi_\bullet(\sigma_\bullet(\overline{\nu}^{-1}(g))) = g$$

since σ_\bullet is a section of π_\bullet . Hence σ is a section of π . Next, by construction, the image of \overline{G} under σ is the image under ν of $\{0, \dots, d-1\}^S$, hence the image under ν of the family of all left-divisors of Δ_\bullet^{d-1} in \mathbb{N}^S , hence the family of all left-divisors of Δ^{d-1} , that is, of Δ_d , in M .

Finally, the relation $\sigma(f)\sigma(g) = \sigma(fg)$ holds in M if and only if the relation $\sigma_\bullet(\overline{\nu}(f))\sigma_\bullet(\overline{\nu}(g)) = \sigma_\bullet(\overline{\nu}(fg))$ holds in \mathbb{N}^S , hence if and only if, for every i , the sum of the i th coordinates of $\overline{\nu}(f)$ and $\overline{\nu}(g)$ does not exceed $d-1$. This happens if and only if $\|\overline{\nu}(f)\|_s + \|\overline{\nu}(g)\|_s = \|\overline{\nu}(fg)\|_s$ holds in $(\mathbb{Z}/d\mathbb{Z})^S$, hence if and only if $\|f\|_{\overline{s}} + \|g\|_{\overline{s}} = \|fg\|_{\overline{s}}$ holds in \overline{G} . By construction, the family S is included in the image of σ , and all length two relations of (3.2) belong to the previous list of relations, hence the latter make a presentation of M . This completes the proof. \square

Example 6.10. For an RC-quasigroup of class 1, that is, satisfying $x * y = y$ for all x, y , the group G is a free Abelian group, the group \overline{G} is trivial, and Proposition 6.2 here reduces to the isomorphism $\mathbb{Z}^S \cong G$.

For class 2, that is, when $(s * s) * (s * t) = t$ holds for all s, t , the element Δ_d is the right-lcm of S , it has 2^n divisors which are the right-lcms of subsets of S , and the group \overline{G} is the order 2^n quotient of G obtained by adding the relations $s(s * s) = 1$. For instance, in the case of $\{\mathbf{a}, \mathbf{b}\}$ with $s * t = f(t)$, $f : \mathbf{a} \mapsto \mathbf{b} \mapsto \mathbf{a}$, the group G has the presentation $\langle \mathbf{a}, \mathbf{b} \mid \mathbf{a}^2 = \mathbf{b}^2 \rangle$, the relations $\mathbf{a}^{[2]} = \mathbf{b}^{[2]} = 1$ both amount to $\mathbf{ab} = 1$, and the associated Coxeter-like group \overline{G} is a cyclic group of order 4.

For class 3, let us consider as in Example 3.8 the RC-quasigroup $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ with $s * t = f(t)$ and $f : \mathbf{a} \mapsto \mathbf{b} \mapsto \mathbf{c} \mapsto \mathbf{a}$. The presentation of the associated group G is $\langle \mathbf{a}, \mathbf{b}, \mathbf{c} \mid \mathbf{ac} = \mathbf{b}^2, \mathbf{ba} = \mathbf{c}^2, \mathbf{cb} = \mathbf{a}^2 \rangle$. With the same notation as above, the smallest Garside element Δ is \mathbf{a}^3 . As the class of $(S, *)$ is 3, we consider here $\Delta_3 = \Delta^2 = \mathbf{a}^6$. The lattice $\text{Div}(\Delta_3)$ has 27 elements, its Hasse diagram is the cube shown in Figure 3. The latter is also the Cayley graph of the germ derived from $(\overline{G}, \{\mathbf{a}, \mathbf{b}, \mathbf{c}\})$, that is, the restriction of the Cayley graph of \overline{G} to the partial product of the germ. Adding to the above presentation the relations $s^{[3]} = 1$, that is, $s(s * s)((s * s) * (s * s)) = 1$, namely $\mathbf{abc} = \mathbf{bca} = \mathbf{cab} = 1$, here reducing to $\mathbf{abc} = 1$, yields for \overline{G} the presentation $\langle \mathbf{a}, \mathbf{b}, \mathbf{c} \mid \mathbf{ac} = \mathbf{b}^2, \mathbf{ba} = \mathbf{c}^2, \mathbf{cb} = \mathbf{a}^2, \mathbf{abc} = 1 \rangle$. One can check that other presentations of \overline{G} are $\langle \mathbf{a}, \mathbf{b} \mid \mathbf{a} = \mathbf{b}^2\mathbf{ab}, \mathbf{b} = \mathbf{aba}^2 \rangle$ and $\langle \mathbf{a}, \mathbf{b} \mid \mathbf{a} = \mathbf{b}^2\mathbf{ab}, \mathbf{a}^3 = \mathbf{b}^3 \rangle$.

Remark 6.11. Applying general results of Gromov, one can show that every finitely generated group G whose Cayley graph is (quasi)-isometric to that of \mathbb{Z}^n must be virtually \mathbb{Z}^n , that is, there exists an exact sequence $1 \rightarrow \mathbb{Z}^n \rightarrow G \rightarrow \overline{G} \rightarrow 1$ with \overline{G} finite, see [2]. By definition, an I -structure is an isometry as above, and, therefore, the existence of a finite quotient \overline{G} as in Proposition 6.2 can be seen as a concrete instance of the above (abstract) result.

The question naturally arises of characterizing Coxeter-like groups associated with finite RC-quasigroups (hence, equivalently, with solutions of YBE) as described in Proposition 6.2. We shall establish now that, exactly as structure groups of solutions of YBE are those groups that admit an I -structure, their Coxeter-like

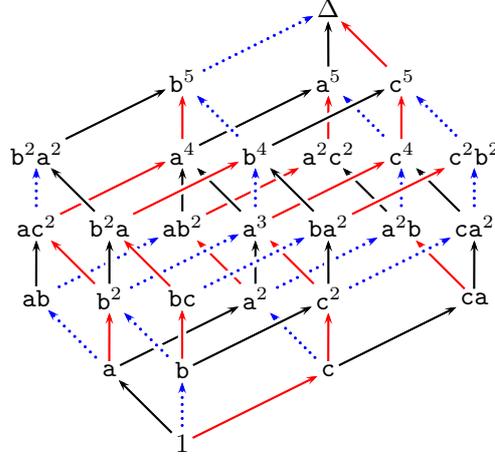


FIGURE 3. The Coxeter-like group associated with the RC-quasigroup of Example 3.8; the 27-vertex cube shown above is the lattice of divisors of a^6 in the associated monoid M , the Hasse diagram of the weak order on the finite group \overline{G} with respect to the generators a, b, c , and the Cayley graph of the germ derived from \overline{G} with respect to the previous generators.

quotients are those finite groups that admit the counterpart of an I -structure where some cyclic group $\mathbb{Z}/d\mathbb{Z}$ replaces \mathbb{Z} , that is, what was called an I -structure of shape $(\mathbb{Z}/d\mathbb{Z})^S$ in Definition 5.1.

Proposition 6.12. *For every finite group W , the following are equivalent:*

- (i) *There exists a finite RC-quasigroup $(S, *)$ of class d such that W is the associated Coxeter-like group.*
- (ii) *The group W admits a right- I -structure of shape $(\mathbb{Z}/d\mathbb{Z})^S$.*

Proof. Assume that $(S, *)$ is a finite RC-quasigroup and G and M are the associated group and monoid. Then M admits an I -structure ν . With the notation of the proof of Proposition 6.2, the congruences \equiv_\bullet on \mathbb{Z}^S and \equiv on G are compatible and ν induces a well-defined map $\overline{\nu}$ of $(\mathbb{Z}/d\mathbb{Z})^S$ to G/\equiv that makes the diagram of (6.6) commutative. Then $\overline{\nu}$ is bijective by construction, and projecting the relation (5.2) for ν gives its counterpart for $\overline{\nu}$. So $\overline{\nu}$ is a right- I -structure of shape $(\mathbb{Z}/d\mathbb{Z})^S$, and (i) implies (ii).

Conversely, assume that W admits a right- I -structure of shape $(\mathbb{Z}/d\mathbb{Z})^S$. As $(\mathbb{Z}/d\mathbb{Z})^S$ satisfies (5.3), Lemmas 5.4 and 5.5 apply. Thus putting $s * t = \psi(s)(t)$ yields an RC-quasigroup and the formulas (5.6) are valid. Let s and t belong to S . In $(\mathbb{Z}/d\mathbb{Z})^S$, we have $s^d = 1$, whence $\psi(s^d) = \psi(1) = \text{id}_S$. Applying (5.6) (left), we deduce $\Omega_{d+1}(s, \dots, s, t) = \psi(s^d)(t) = t$. Hence the RC-quasigroup $(S, *)$ is of class d .

Now, let G be the group associated with $(S, *)$, and let \overline{G} be the associated finite quotient as provided by Proposition 6.2. The group G is generated by S and it admits a presentation consisting of all relations $s(s * t) = t(t * s)$ with s, t in S . By assumption, the group W is generated by S , and we observed that the relations $s(s * t) = t(t * s)$ with s, t in S are satisfied in W since, by definition, they are equivalent to $\nu(st) = \nu(ts)$ and $(\mathbb{Z}/d\mathbb{Z})^S$ is Abelian. Hence there exists a surjective homomorphism θ from G to W that is the identity on S .

$$\begin{array}{ccc}
\mathbb{Z}^S & \xrightarrow{\widehat{\nu}} & G \\
\pi \cdot \downarrow & & \downarrow \pi \\
(\mathbb{Z}/d\mathbb{Z})^S & \xrightarrow{\quad} & \overline{G}
\end{array}
\begin{array}{c}
\begin{array}{ccc}
& & \theta \\
& \searrow & \\
& & W
\end{array} \\
\begin{array}{ccc}
& \xrightarrow{\overline{\theta}} & \\
& & \\
& \xrightarrow{\nu} &
\end{array}
\end{array}$$

Next, \overline{G} is the quotient of G obtained by adding the relations $s^{[d]} = 1$, that is, $\Pi_d(s, \dots, s) = 1$ for s in S . Now, in W , we have $\Pi_d(s, \dots, s) = \nu(s^d)$ by (5.6); but $s^d = 1$ holds in $(\mathbb{Z}/d\mathbb{Z})^S$, so we deduce that, in W , we have $\Pi_d(s, \dots, s) = 1$ for every s in S . Thus the surjective homomorphism θ factorizes through \overline{G} , yielding a surjective homomorphism $\overline{\theta}$ from \overline{G} to W . As both \overline{G} and W have cardinality d^n , the homomorphism $\overline{\theta}$ must be an isomorphism. Hence W is the Coxeter-like quotient of the group associated with $(S, *)$. So (ii) implies (i). \square

Using Proposition 5.7, we deduce

Corollary 6.13. *Assume that $(S, *)$ is an RC-quasigroup of cardinal n and class d . Then there exists an injective homomorphism of the associated Coxeter-like group into the wreath product $\mathbb{Z}/d\mathbb{Z} \wr \mathfrak{S}_n$ whose first component is a bijection.*

Example 6.14. For the last group \overline{G} of Example 6.10, owing to the fact that the permutations of $\{1, 2, 3\}$ associated with $\mathbf{a}, \mathbf{b}, \mathbf{c}$ all are the cycle $f : 1 \mapsto 2 \mapsto 3 \mapsto 1$, one obtains a description as the family of the 27 tuples $(p, q, r; f^{p+q+r})$ with p, q, r in $\mathbb{Z}/3\mathbb{Z}$, the product of triples being twisted by the action of f^{p+q+r} on positions.

We conclude with a few observations about linear representations of the groups G and \overline{G} associated with finite RC-quasigroups are linear groups, which both turn out to be linear. Here again, we start from the trivial case of a free Abelian group and use the I -structure to carry the results to the group of an arbitrary RC-quasigroup.

Proposition 6.15. *Assume that $(S, *)$ is an RC-quasigroup of cardinal n and class d . Let G be the associated group. For s the i th element of S (in some fixed enumeration), define*

$$(6.7) \quad \Theta(s) = \Theta_{\bullet}(s)P_{\psi(s)},$$

where $\Theta_{\bullet}(s)$ is the diagonal $n \times n$ -matrix with diagonal entries $(1, \dots, 1, q, 1, \dots, 1)$, q at position i and P_f is the permutation matrix associated with a permutation f of $\{1, \dots, n\}$. Then Θ provides a faithful representation of G into $\mathrm{GL}(n, \mathbb{Q}[q, q^{-1}])$; specializing at $q = \exp(2i\pi/d)$ gives a faithful representation of the associated Coxeter-like group \overline{G} .

Proof. First, Θ_{\bullet} defines a faithful representation of \mathbb{Z}^S into $\mathrm{GL}(n, \mathbb{Q}[q, q^{-1}])$ since $\Theta_{\bullet}(\prod \mathbf{s}_i^{e_i})$ is the diagonal matrix with diagonal $(q^{e_1}, \dots, q^{e_n})$, and specializing at $q = \exp(2i\pi/d)$ gives a faithful representation of $(\mathbb{Z}/d\mathbb{Z})^S$.

In order to carry the results to G and \overline{G} , we now show that (6.7) extends into

$$(6.8) \quad \Theta(\nu(a)) = \Theta_{\bullet}(a)P_{\psi(a)}$$

for every a in \mathbb{Z}^S . As we are working with invertible matrices, it is enough to consider multiplication by one element of S (division automatically follows) and, therefore, the point for an induction is to go from a to as . Now we find

$$\Theta(\nu(as)) = \Theta(\nu(a))\psi(a)(s) \quad \text{by (5.2)}$$

$$\begin{aligned}
 &= \Theta(\nu(a)) \Theta(\psi(a)(s)) && \text{by definition} \\
 &= \Theta_{\bullet}(a) P_{\psi(a)} \Theta_{\bullet}(\psi(a)(s)) P_{\psi(\psi(a)(s))} \\
 & && \text{by induction hypothesis and definition} \\
 &= \Theta_{\bullet}(a) \Theta_{\bullet}(s) P_{\psi(a)} P_{\psi(\psi(a)(s))} \\
 & && \text{by conjugating a diagonal matrix by a permutation matrix} \\
 &= \Theta_{\bullet}(as) P_{\psi(\psi(a)(s) \circ \psi(a))} && \text{by definition} \\
 &= \Theta_{\bullet}(as) P_{\psi(as)}. && \text{by (5.7)}
 \end{aligned}$$

So (6.8) is established. It is then clear that Θ is well-defined on the monoid associated with $(S, *)$, hence on its group of fractions, which is G . For faithfulness, $\Theta_{\bullet}(\nu^{-1}(g))$ is the unique diagonal matrix obtained from $\Theta(g)$ by right-multiplication by a permutation matrix, so $\Theta(g)$ determines $\nu^{-1}(g)$, hence g .

Finally, specializing at a d th root of unity induces a well-defined faithful representation of the finite group \overline{G} since, by definition, g and g' represent the same element of \overline{G} if and only if $\nu^{-1}(g)$ and $\nu^{-1}(g')$ are \equiv_{\bullet} -equivalent, hence if and only if $\Theta_{\bullet}(\nu^{-1}(g))_{q=\exp(2i\pi/d)}$ and $\Theta_{\bullet}(\nu^{-1}(g'))_{q=\exp(2i\pi/d)}$ are equal. \square

Example 6.16. Coming back to the last case in Example 6.10 with the enumeration $(\mathbf{a}, \mathbf{b}, \mathbf{c})$, the permutations $\psi(\mathbf{a})$, $\psi(\mathbf{b})$, and $\psi(\mathbf{c})$ all are the 3-cycle $(1, 2, 3)$, and we find the explicit representation

$$\Theta(\mathbf{a}) = \begin{pmatrix} 0 & q & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \Theta(\mathbf{b}) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & q \\ 1 & 0 & 0 \end{pmatrix}, \quad \Theta(\mathbf{c}) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ q & 0 & 0 \end{pmatrix}.$$

Specializing at $q = \exp(2i\pi/3)$ gives a faithful unitary representation of the associated 27-element group \overline{G} . Using the latter, it is easy to check for instance that \overline{G} has exponent 9: $\mathbf{a}, \mathbf{b}, \mathbf{c}$ have order 9, and all elements have order 1, 3, or 9.

Corollary 6.17. *Assume that $(S, *)$ is an RC-quasigroup of cardinal n and class d and G is the associated group. Then the associated Coxeter-like group can be realized as a group of isometries in an n -dimensional Hermitian space.*

Proof. The matrices $\Theta_{\bullet}(s)_{q=\exp(2i\pi/d)}$ correspond to order d complex reflections, whereas permutation matrices are finite products of hyperplane symmetries. \square

We shall not go farther in the description of the Coxeter-like groups \overline{G} . As \overline{G} characterizes the RC-quasigroup it comes from, classifying all finite groups that occur in this way is *a priori* not easier than classifying all solutions of YBE, hence presumably (very) difficult. On the other hand, the analogy with Coxeter groups suggests to investigate geometric characterizations further.

Let us conclude with another speculative idea. So far, Proposition 4.1 is the only known global characterization of a relatively large family of Garside groups: owing to the results of Section 5, it identifies Garside groups that admit a presentation of a certain form with those that admit an I -structure, hence resemble a free Abelian group \mathbb{Z}^n . One might think of replacing free Abelian groups with other groups Γ and consider those groups G that admit a “ I -structure of shape Γ ” in the sense that their Cayley graph is that of Γ up to relabeling the edges. Should the above approach make sense, a natural problem would be to characterize those Garside groups that admit an I -structure of shape Γ for various reference (Garside) groups Γ

and, from there, maybe approach a global classification of Garside groups which, so far, remains out of reach.

REFERENCES

- [1] N. Bourbaki, *Groupes et algèbres de Lie*, chapitres I–III, Masson, Paris (1972).
- [2] M.R. Bridson and S.M. Gersten, *The optimal isoperimetric inequality for torus bundles over the circle*, *Quart. J. Math. Oxford* **47** (1996) 1–23.
- [3] F. Cedó, E. Jespers, and J. Okniński, *Braces and the Yang–Baxter equation*, *Comm. Math. Physics* **327** (2014) 101–116; arXiv:1205.3587.
- [4] F. Chouraqui, *Garside groups and Yang–Baxter equations*, *Comm. Algebra* **38-12** (2010) 4441–4460.
- [5] F. Chouraqui and E. Godelle, *Finite quotients of groups of I-type*, *Adv. in Math.*, to appear; arXiv:1301.3707.
- [6] A.H. Clifford and G.B. Preston, *The algebraic Theory of Semigroups*, vol. 1, *Amer. Math. Soc. Surveys* **7**, (1961).
- [7] P. Dehornoy and L. Paris, *Gaussian groups and Garside groups, two generalizations of Artin groups*, *Proc. London Math. Soc.* **79-3** (1999) 569–604.
- [8] P. Dehornoy, *Groupes de Garside*, *Ann. Scient. Ec. Norm. Sup.* **35** (2002) 267–306.
- [9] P. Dehornoy, *Complete positive group presentations*, *J. of Algebra* **268** (2003) 156–197.
- [10] P. Dehornoy, *The group of fractions of a torsion free lcm monoid is torsion free*, *J. Algebra* **281** (2004) 303–305.
- [11] P. Dehornoy, with F. Digne, E. Godelle, D. Krammer, J. Michel, *Foundations of Garside Theory*, EMS Tracts in Mathematics, to appear; www.math.unicaen.fr/~garside/Garside.pdf.
- [12] P. Dehornoy, F. Digne, and J. Michel, *Garside families and Garside germs*, *J. of Algebra* **380** (2013) 109145.
- [13] F. Digne and J. Michel, *Garside and locally Garside categories*, Preprint; math.GR/0612652.
- [14] P. Etingof, T. Schedler, and A. Soloviev, *Set-theoretical solutions to the quantum Yang–Baxter equation*, *Duke Math. J.* **100** (1999) 169–209.
- [15] R. Fenn, M. Jordan-Santana, and L. Kauffman, *Biquandles and virtual links*, *Topology and its Applic.* **145** (2004) 157–175.
- [16] R. Fenn and C.P. Rourke, *Racks and links in codimension 2*, *J. Knot Theory and its Ramifications* **1-4** (1992) 343–406;
- [17] T. Gateva-Ivanova, *Garside structures on monoids with quadratic square-free relations*, *Algebr. Represent. Theory* **14** (2011) 779–802.
- [18] T. Gateva-Ivanova and M. Van den Bergh, *Semigroups of I-type*, *J. Algebra* **206** (1998) 97–112.
- [19] T. Gateva-Ivanova and S. Majid, *Set theoretic solutions of the Yang–Baxter equation, graphs and computations*, *J. Symbolic Comput.* **42** (2007) 1079–1112.
- [20] T. Gateva-Ivanova and S. Majid, *Matched pairs approach to set theoretic solutions of the Yang–Baxter equation*, *J. Algebra* **319** (2008) 1462–1529.
- [21] E. Jespers and J. Okniński, *Monoids and groups of I-type*, *Algebr. Represent. Theory*; 8; 2005; 709–729.
- [22] E. Jespers and J. Okniński, *Noetherian semigroup algebras*, *Algebra and Applications* vol. 7, Springer-Verlag (2007).
- [23] M. Jimbo, *Introduction to the Yang–Baxter equation*, *Int. J. Modern Physics A* **4-15** (1989) 3759–3777.
- [24] W. Rump, *A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation*, *Adv. in Math.* **193** (2005) 40–55.

LABORATOIRE DE MATHÉMATIQUES NICOLAS ORESME, UMR 6139 CNRS, UNIVERSITÉ DE CAEN
BP 5186, 14032 CAEN CEDEX, FRANCE

Current address: LABORATOIRE PREUVES, PROGRAMMES, SYSTÈMES, UMR 7126 CNRS, UNI-
VERSITÉ PARIS-DIDEROT CASE 7014, 75205 PARIS CEDEX 13, FRANCE

E-mail address: dehornoy@math.unicaen.fr

URL: [//www.math.unicaen.fr/~dehornoy](http://www.math.unicaen.fr/~dehornoy)