Garside germs for YBE structure groups, and an extension of Ore's theorem

Patrick Dehornoy

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen

Groups, Rings and the Yang-Baxter Equation
Spa, June 2017

- Advertizing for two (superficially unrelated) topics:
  - W. Rump's formalism of cycle sets for investigating YBE structure groups: revisit the Garside and the I-structures, and introduce a finite Coxeter-like quotient,
  - a new approach to the word problem of Artin-Tits groups, based on an extension of Ore's theorem from fractions to multifractions.

Plan:

- Structure groups of set-theoretic solutions of YBE
  - 1. RC-calculus
    - Solutions of YBE vs. biracks vs. cycle sets
    - Revisiting the Garside structure using RC-calculus
    - Revisiting the I-structure using RC-calculus
  - 2. A new application: Garside germs
    - The braid germ
    - The YBE germ
- A new approach to the word problem of Artin-Tits groups
  - 3. Multifraction reduction, an extension of Ore's theorem
    - Ore's classical theorem
    - Extending free reduction: (i) division, (ii) reduction
    - The case of Artin-Tits groups: theorems and conjectures

Plan:

- Structure groups of set-theoretic solutions of YBE
  - ▶ 1. RC-calculus
    - - Solutions of YBE vs. biracks vs. cycle sets
    - - Revisiting the Garside structure using RC-calculus
    - - Revisiting the I-structure using RC-calculus
  - ▶ 2. A new application: Garside germs
    - - The braid germ
    - - The YBE germ
- A new approach to the word problem of Artin-Tits groups
  - ▶ 3. Multifraction reduction, an extension of Ore's theorem
    - - Ore's classical theorem
    - - Extending free reduction: (i) division, (ii) reduction
    - - The case of Artin-Tits groups: theorems and conjectures

- Definition: A set-theoretic solution of YBE is a pair (S, r) where S is a set and r is a bijection from $S \times S$ to itself satisfying

$$r^{12}r^{23}r^{12} = r^{23}r^{12}r^{23}$$

where $r^{ij} : S^3 \to S^3$ means r acting on the i^{th} and j^{th} entries.

  - A solution $(S, r) = (S, (r_1, r_2))$ is nondegenerate if, for all s, t, the maps $y \mapsto r_1(s, y)$ and $x \mapsto r_2(x, t)$ are bijective.
  - A solution (S, r) is involutive if $r^2 = \mathrm{id}$.

- Changing framework 1 (folklore): view r as a pair of binary operations on S
  - "birack": $(S, \rceil, \lceil)$ where $\rceil$ and $\lceil$ are binary operations satisfying...

- Changing framework 2 (W. Rump): invert the operation(s):
  - If the left translations of a binary operation $\star$ are bijections, there exists $\overline{\star}$ s.t.

$$x \star y = z \iff x \,\overline{\star}\, z = y$$

(define $x \,\overline{\star}\, z :=$ the unique y satisfying $x \star y = z$)

  - Apply this to the operation(s) of a birack.

- A (small) miracle occurs: only one operation $*$ and one algebraic law are needed.

- Definition: A (right) cycle set (or RC-system), is a pair $(S, *)$ where $*$ obeys

$$(x * y) * (x * z) = (y * x) * (y * z). \qquad \text{(RC)}$$

  - An RC-quasigroup is a cycle set whose left-translations are bijective.
  - A cycle set is bijective if $(s, t) \mapsto (s * t, t * s)$ is a bijection of S^2.

- Theorem (Rump, 2005): (i) If (S, r) is an involutive nondegenerate solution, then $(S, *)$ is a bijective RC-quasigroup, where $s * t :=$ the unique r s.t. $r_1(s, r) = t$.

(ii) Conversely, is $(S, *)$ is a bijective RC-quasigroup, then (S, r) is an involutive nondegenerate solution, where $r(a, b) :=$ the unique pair (a', b') s.t. $a * a' = b$ and $a' * a = b'$.

- Claim: One can (easily) develop an "RC-calculus".

- Definition: For $n \geqslant 1$, define $\Omega_1(x_1) := x_1$ and

$$\Omega_n(x_1, ..., x_n) := \Omega_{n-1}(x_1, ..., x_{n-1}) * \Omega_{n-1}(x_1, ..., x_{n-2}, x_n).$$

Similarly, for $n \geqslant 1$, let (where $\cdot$ is another binary operation):

$$\Pi_n(x_1, ..., x_n) := \Omega_1(x_1) \cdot \Omega_2(x_1, x_2) \cdot \cdots \cdot \Omega_n(x_1, ..., x_n),$$

  - $\Omega_2(x, y) = x * y$, and the RC-law is $\Omega_3(x, y, z) = \Omega_3(y, x, z)$.
  - Think of the Ω_n as (counterparts of) iterated sums in the RC-world, and of the Π_n as (counterparts of) iterated products.

- Lemma: *If $(S, *)$ is a cycle set, then, for every π in $\mathfrak{S}_{n-1}$, one has*

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

  - In the language of braces, $\Omega_n(x_1, ..., x_n)$ corresponds to $(x_1 + \cdots + x_{n-1}) * x_n$.

- Lemma: If $(S, *)$ is a bijective RC-quasigroup, there exists $\tilde{*}$, unique, s.t.

$$(s, t) \mapsto (s \,\tilde{*}\, t, t \,\tilde{*}\, s) \text{ is the inverse of } (s, t) \mapsto (s * t, t * s).$$

Then $(S, \tilde{*})$ is a bijective LC-quasigroup and, for $\widetilde{s_i} := \Omega_n(s_1, ..., \widehat{s_i}, , ..., s_n, s_i)$, one has

$$\Omega_i(s_{\pi(1)}, ..., s_{\pi(i)}) = \widetilde{\Omega}_{n+1-i}(\widetilde{s}_{\pi(i)}, ..., \widetilde{s}_{\pi(n)}),$$
$$\Pi_n(s_1, ..., s_n) = \widetilde{\Pi}_n(\widetilde{s}_1, ..., \widetilde{s}_n).$$

  - "Inversion formulas"; etc. etc.

• Definition: The structure group (*resp.* monoid) associated with a (nondegenerate involutive) solution (S, r) of YBE is the group (*resp.* monoid)

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

The structure group (*resp.* monoid) associated with a cycle set $(S, *)$ is the group (*resp.* monoid) is

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

• Fact: *If* (S, r) *and* $(S, *)$ *correspond to one another, the structure monoids and groups are the same.*

• Claim: RC-calculus gives more simple proofs, and new results naturally occur.
- The relations of $(\#)$ are "RC-commutation relations" $\Pi_2(s, t) = \Pi_2(t, s)$.
- All rules of RC-calculus apply in the structure monoid.

• Theorem (Chouraqui, 2010): *The structure monoid of a solution* (S, r) *is a Garside monoid with atom set* S.

- What does this mean?
- «Definition»: A Garside monoid (group) is a monoid (group) that enjoys all good divisibility properties of Artin's braid monoids (groups).

• Divisibility relations of a monoid M:

$a \leqslant b$ means $\exists b' \in M\, (ab' = b)$, — a left-divides b, or b is a right-multiple of a

$a \,\widetilde{\leqslant}\, b$ means $\exists b' \in M\, (b'a = b)$. — a right-divides b, or b is a left-multiple of a

• Definition: A Garside monoid is a cancellative monoid M s.t.

- There exists $\lambda : M \to \mathbb{N}$ s.t. $\lambda(ab) \geqslant \lambda(a) + \lambda(b)$ and $a \neq 1 \Rightarrow \lambda(a) \neq 0$; ("a pseudo-length function")
- The left and right divisibility relations in M form lattices ("gcds and lcms exist")
- The closure of atoms under right-lcm and right-divisor is finite and it coincides with the closure of the atoms under left-lcm and left-divisor ("simple elements").

• If M is a Garside monoid, it embeds in its enveloping group, which is a group of left and right fractions for M.

• <u>Definition</u>: A Garside group is a group G that can be expressed, in at least one way, as the group of fractions of a Garside monoid (no uniqueness of the monoid in general).

• <u>Example</u>: Artin's n-strand braid group B_n admits (at least) two Garside structures:

- one associated with the braid monoid B_n^+, with $n-1$ atoms,
  $n!$ simples ($\cong$ permutations), the maximal one Δ_n of length $n(n-1)/2$,
- one associated with the dual braid monoid B_n^{+*}, with $n(n-1)/2$ atoms,
  $\mathrm{Catalan}_n$ simples ($\cong$ noncrossing partitions), the maximal one δ_n of length $n-1$.

• Why do we care about Garside structures?

- The word problem is solvable (in quadratic time).
- There is a canonical normal form for the elements ("greedy normal form").
- There is a (bi)-automatic structure.
- The (co)homology is efficiently computable.
- There is no torsion.

The whole structure is encoded in the (finite) family of simple elements.

- Assume M is the structure monoid of an RC-quasigroup $(S, *)$.
  - Step 1: *M is left-cancellative and admits right-lcms.*
    - ▶ Proof: The RC law directly gives the "right cube condition", implying left-cancellativity and right-lcms. □
  - Step 2: *M determines $(S, *)$.*
    - ▶ Proof: S is the atom set of M, and

      $s * t := s\backslash t$ for $s \neq t$, $s * s :=$ the unique element of S not in $\{s\backslash t \mid t{\neq}s \in S\}$. □

      ↑

      right-complement of s in t: the (unique) t' s.t. $st' =$ right-lcm(s, t).

- Assume moreover that $(S, *)$ is bijective.
  - Step 3: *M is cancellative, it admits lcms on both sides, and its group is a group of fractions.*
    - ▶ Proof: Bijectivity implies the existence of $\tilde{*}$ with symmetric properties. □
  - Step 4: *For $s_1, \ldots, s_n$ pairwise distinct, $\Pi_n(s_1, \ldots, s_n)$ is the right-lcm of $s_1, \ldots, s_n$, and the left-lcm of $\widetilde{s}_1, \ldots, \widetilde{s}_n$ defined by $\widetilde{s}_i = \Omega_n(s_1, \ldots, \widehat{s}_i, \ldots, s_n, s_i)$.*
    - ▶ Proof: Apply the "inversion formulas" of RC-calculus. □

- Revisiting the I-structure with the help of RC-calculus:

  "the Cayley graph of the structure group is a copy of the Euclidean lattice $\mathbb{Z}^{\#S}$".

- Theorem (Gateva-Ivanova, Van den Bergh, 1998): *If M is the monoid of a nondegenerate involutive solution (S, r), then there exists a bijection ν: $\mathbb{N}^{\#S} \to M$ satisfying $\nu(1) = 1$, $\nu(s) = s$ for s in S, and*

$$\{\nu(as) \mid s \in S\} = \{\nu(a)s \mid s \in S\} \qquad \text{for every } a \text{ in } \mathbb{N}^{\#S}.$$

Conversely, every monoid with an I-structure arises in this way.

Proof: If $(S, *)$ is an RC-quasigroup and M is the associated monoid, then defining

$$\nu(s_1 \cdots s_n) := \Pi_n(s_1, ..., s_n) \text{ for } n := \#S$$

provides a right I-structure on M.

Conversely, if ν is an I-structure, defining $*$ on S by

$$\nu(st) = \nu(s) \cdot (s * t)$$

provides a bijective RC-quasigroup on S. Then $\pi(s)$ belongs to $\mathfrak{S}_n$,
and one has $(r*s)*(r*t) = \pi(rs)(t)$, so $rs = sr$ in $\mathbb{N}^n$ implies the RC law for $*$.
More generally, one obtains $\pi(s_1 \cdots s_{p-1})(s_p) = \Omega_p(s_1, ..., s_p)$ for every p.
One concludes using Rump's result that every finite RC-quasigroup is bijective. □

- Once again, the proof seems easier and more explicit when stated in terms of $*$ and RC.

Plan:

- Structure groups of set-theoretic solutions of YBE
  - ▶ 1. Rump's RC-calculus
    - Solutions of YBE vs. biracks vs. cycle sets
    - Revisiting the Garside structure using RC-calculus
    - Revisiting the I-structure using RC-calculus
  - ▶ 2. A new application: Garside germs
    - The braid germ
    - The YBE germ
- A new approach to the word problem of Artin-Tits groups
  - ▶ 3. Multifraction reduction, an extension of Ore's theorem
    - Ore's classical theorem
    - Extending free reduction: (i) division, (ii) reduction
    - The case of Artin-Tits groups: theorems and conjectures

• The n-strand braid monoid B_n^+ and group B_n admit the presentation

$$\left\langle \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & \text{for } \; |i-j| \geqslant 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{for } \; |i-j| = 1 \end{array} \right\rangle.$$

Adding the torsion relations $\sigma_i^2 = 1$ gives the Coxeter presentation of $\mathfrak{S}_n$ in terms of the family Σ of adjacent transpositions, with

$$1 \longrightarrow PB_n \longrightarrow B_n \xrightarrow{\pi} \mathfrak{S}_n \longrightarrow 1.$$

• Claim: *The Garside structure of B_n based on B_n^+ "comes from" the group $\mathfrak{S}_n$: There exists a (set-theoretic) section $\sigma : \mathfrak{S}_n \hookrightarrow B_n^+$ of π s.t. $\mathrm{Im}(\sigma)$ is the set of simples of B_n^+ and, for all f, g in $\mathfrak{S}_n$,*

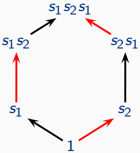
$(*) \quad \sigma(f)\sigma(g) = \sigma(fg)$ *holds in* B_n^+ *iff* $\ell_\Sigma(f) + \ell_\Sigma(g) = \ell_\Sigma(fg)$ *holds in* $\mathfrak{S}_n$,

where $\ell_\Sigma(f)$ is the Σ-length of f (:= # of inversions).

• Definition: A group W with generating family Σ is a germ for a monoid M if there exists a projection $\pi : M \to W$ and a section $\sigma : W \hookrightarrow M$ of π s.t. M is generated by $\mathrm{Im}(\sigma)$ and (the counterpart of) $(*)$ holds. It is a Garside germ if, in addition, M is a Garside monoid and $\mathrm{Im}(\sigma)$ is the set of simples of M.

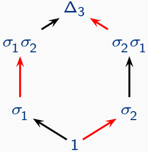
- Think of M as of an "unfolding" of W.

- So: the symmetric group $\mathfrak{S}_n$ is a Garside germ for the braid monoid B_n^+:



Cayley graph of $\mathfrak{S}_3$
w.r.t. adjacent transpositions

adding torsion $s_i^2 = 1$ $\longleftarrow$ $\simeq$ $\longrightarrow$ removing $h = fg$ for $\ell(h) < \ell(f) + \ell(g)$

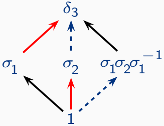


Hasse diagram of left division
for simple elements of B_3^+

- Works similarly for every finite Coxeter group with the associated Artin-Tits monoid.

- But: does not extend to arbitrary Garside monoids:

? $\quad$ adding ?? $\longleftarrow$ $\simeq$



Hasse diagram of left division
for simple elements of B_3^{+*}

- Finding a germ is difficult: partly open for braid groups of complex reflection groups: very recent (partial) positive results by Neaime building on Corran–Picantin.

- What for YBE monoids?
  - Partial positive result by Chouraqui and Godelle (= "RC-systems of class 2").
  - Complete positive result, once again based on RC-calculus.

- Definition: An RC-quasigroup $(S, *)$ is of class d if, for all s, t in S

$$\Omega_{d+1}(s, ..., s, t) = t.$$

  - class 1: $s * t = t$,
  - class 2: $(s * s) * (s * t) = t$, etc.
  - for ϕ an order d permutation, $s * t := \phi(t)$ is of class d.

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

  Proof: The map $(s, t) \mapsto (s * s, s * t)$ on $S \times S$ is bijective, hence of order $\leqslant (n^2)!$. □

• Notation: $x^{[d]}$ for $\Pi_d(x, ..., x)$.

• Theorem: *Let $(S, *)$ be an RC-quasigroup of cardinal n and class d, and let M and G be associated monoid and group. Then collapsing $s^{[d]}$ to 1 in G for every s in S gives a finite group $\overline{G}$ of order d^n that provides a Garside germ for M, with an exact sequence*

$$1 \longrightarrow \mathbb{Z}^n \longrightarrow G \longrightarrow \overline{G} \longrightarrow 1.$$

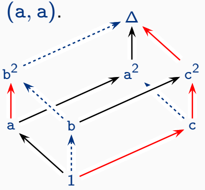
▶ Entirely similar to the ArtinTits/Coxeter case,
with the "RC-torsion" relations $s^{[d]} = 1$ replacing $s^2 = 1$.

▶ Proof: Use the I-structure to carry the results from the (trivial) case of $\mathbb{Z}^n$.
Express the I-structure ν in terms of the RC-polynomials Ω and Π, typically

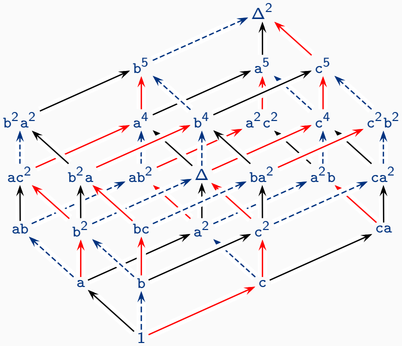
$$\begin{aligned}\nu(s^d a) &= \Pi_{d+q}(s, ..., s, t_1, ..., t_q)\\ &= \Pi_d(s, ..., s)\Pi_q(\Omega_{d+1}(s, ..., s, t_1), ..., \Omega_{d+1}(s, , ..., s, t_q))\\ &= \Pi_d(s, ..., s)\Pi_q(t_1, ..., t_q) = \nu(s^d)\nu(t_1 \cdots t_q) = s^{[d]}\,\nu(a).\end{aligned}$$

Then $\overline{G}$ is $G/\!\equiv$ where $g \equiv g'$ means $\forall s{\in}S\ (\#_s(\nu^{-1}(g)) = \#_s(\nu^{-1}(g')) \bmod d)$. □

- Example: Let $S := \{a, b, c\}$, with $s * t = \phi(t)$, $\phi : a \mapsto b \mapsto c \mapsto a$, of class 3.
  - Corresponds to $r(a, c) = (b, b)$, $r(b, a) = (c, c)$, $r(c, b) = (a, a)$.
  - Then $M = \langle a, b, c \mid ac = b^2, ba = c^2, cb = a^2 \rangle^+$,
    a Garside monoid with 2^3 simple elements:



  - Then $a^{[3]} = b^{[3]} = c^{[3]} = abc$, hence
    $\overline{G} := \langle a, b, c \mid ac = b^2, ba = c^2, cb = a^2, abc = 1 \rangle$.



• Question: Coxeter-like groups are in general larger than the "G_S^0"s of [Etingof et al., 98]. Which finite groups appear in this way?

- Those groups admitting a "pseudo-I-structure", with $(\mathbb{Z}/d\mathbb{Z})^n$ replacing $\mathbb{Z}^n$
- Those groups embedding in $\mathbb{Z}/d\mathbb{Z} \wr \mathfrak{S}_n$, like [Jespers-Okninski, 2005] with $(\mathbb{Z}/d\mathbb{Z})^n$.

• Question: To construct the Garside and I-structures, one uses Rump's result that finite RC-quasigroups are bijective. Can one instead prove this result using the Garside structure?

• Question: Does the brace approach make the cycle set approach obsolete?

- Can the RC-approach be used to address the left-orderability of the structure group?
- Could there exist a skew version of the RC-approach?

• References:

- W. Rump: *A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation*, Adv. Math. 193 (2005) 40–55
- P. Dehornoy, *Set-theoretic solutions of the Yang-Baxter equation, RC-calculus, and Garside germs* Adv. Math. 282 (2015) 93–127
- P. Dehornoy, with F. Digne, E. Godelle, D. Krammer, J. Michel, Chapter XIII of: Foundations of Garside Theory, EMS Tracts in Mathematics, vol. 22 (2015)

Plan:

- Structure groups of set-theoretic solutions of YBE
  - ▶ 1. Rump's RC-calculus
    - Solutions of YBE vs. biracks vs. cycle sets
    - Revisiting the Garside structure using RC-calculus
    - Revisiting the I-structure using RC-calculus
  - ▶ 2. A new application: Garside germs
    - The braid germ
    - The YBE germ
- A new approach to the word problem of Artin-Tits groups
  - ▶ 3. Multifraction reduction, an extension of Ore's theorem
    - Ore's classical theorem
    - Extending free reduction: (i) division, (ii) reduction
    - The case of Artin-Tits groups: theorems and conjectures

- Notation: $\mathcal{U}(M)$:= enveloping group of a monoid M.
  - $\exists\phi : M \to \mathcal{U}(M)$ s.t. every morphism from M to a group factors through ϕ.
  - If $M = \langle S \mid R\rangle^+$, then $\mathcal{U}(M) = \langle S \mid R\rangle$.

- Theorem (Ore, 1933): *If M is cancellative and satisfies the 2-Ore condition, then M embeds in $\mathcal{U}(M)$ and every element of $\mathcal{U}(M)$ is represented as ab^{-1} with a, b in M.*

"group of (right) fractions for M" (a/b)

  - 2-Ore condition: any two elements admit a common right-multiple.

- Definition: A gcd-monoid is a cancellative monoid, in which 1 is the only invertible element (so $\leqslant$ and $\widetilde{\leqslant}$ are partial orders) and any two elements admit a left and a right gcd (greatest lower bounds for $\leqslant$ and $\widetilde{\leqslant}$).

- Corollary: *If M is a gcd-monoid satisfying the 2-Ore condition, then M embeds in $\mathcal{U}(M)$ and every element of $\mathcal{U}(M)$ is represented by a unique irreducible fraction.*

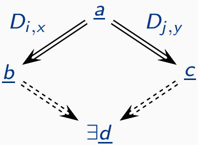
↑ ab^{-1} with $a, b \in M$ and right-gcd$(a, b) = 1$

- Example: every Garside monoid.

- When the 2-Ore condition fails (no common multiples), no fractional expression.

- <u>Example</u>: $M = F^+$, a free monoid; then M embeds in $\mathcal{U}(M)$, a free group;
  - No fractional expression for the elements of $\mathcal{U}(M)$,
  - But: unique expression $a_1 a_2^{-1} a_3 a_4^{-1} \cdots$ with $a_1, a_2, \dots$ in M and
    for i odd: a_i and a_{i+1} do not finish with the same letter,
    for i even: a_i and a_{i+1} do not begin with the same letter.
    - a "freely reduced word"

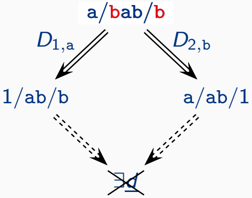
- <u>Proof</u>: (easy) Introduce rewrite rules on finite sequences of positive words:
  - rule $D_{i,x} := \begin{cases} \text{for } i \text{ odd, delete } x \text{ at the end of } a_i \text{ and } a_{i+1} \text{ (if possible...)}, \\ \text{for } i \text{ even, delete } x \text{ at the beginning of } a_i \text{ and } a_{i+1} \text{ (if possible...)}. \end{cases}$
  - Then the system of all rules $D_{i,x}$ is (locally) confluent:



  - Every sequence $\underline{a}$ rewrites into a unique irreducible sequence ("convergence"). □

- When M is not free, the rewrite rule $D_{i,x}$ can still be given a meaning:
  - no first or last letter,
  - but left- and right-divisors: $x \leqslant a$ means "x is a possible beginning of a".
  - rule $D_{i,x} := \begin{cases} \text{for } i \text{ odd, right-divide } a_i \text{ and } a_{i+1} \text{ by } x \text{ (if possible...),} \\ \text{for } i \text{ even, left-divide } a_i \text{ and } a_{i+1} \text{ by } x \text{ (if possible...).} \end{cases}$

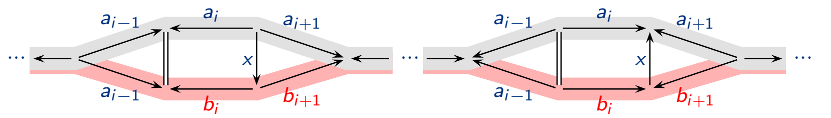
- <u>Example</u>: $M = B_3^+ = \langle \mathtt{a}, \mathtt{b} \mid \mathtt{aba} = \mathtt{bab} \rangle^+$;
  - start with the sequence $(\mathtt{a}, \mathtt{aba}, \mathtt{b})$, better written as a "multifraction" $\mathtt{a}/\mathtt{aba}/\mathtt{b}$:
    (think of $a_1/a_2/a_3/...$ as a sequence representing $a_1 a_2^{-1} a_3 a_4^{-1} ...$ in $\mathcal{U}(M)$)



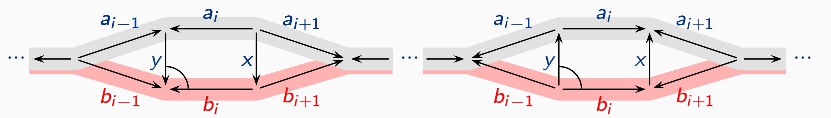
  - no hope of confluence... hence consider more general rewrite rules.

- Diagrammatic representation of elements of M: $\xrightarrow{a} \mapsto a$, and multifractions:
  $\xrightarrow{a_1}\xleftarrow{a_2}\xrightarrow{a_3}\cdots \mapsto a_1/a_2/a_3/\ldots \mapsto \phi(a_1)\phi(a_2)^{-1}\phi(a_3)\ldots$ in $\mathcal{U}(M)$.
  - Then: commutative diagram $\leftrightarrow$ equality in $\mathcal{U}(M)$.

- Diagram for $D_{i,x}$ (division by x at level i): declare $\underline{a} \bullet D_{i,x} = \underline{b}$ for



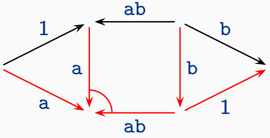
- Relax "x divides a_i" to "lcm(x, a_i) exists": declare $\underline{a} \bullet R_{i,x} = \underline{b}$ for



- Definition: "$\underline{b}$ obtained from $\underline{a}$ by reducing x at level i":
  divide a_{i+1} by **x**, push **x** through a_i using lcm, multiply a_{i-1} by the remainder **y**.

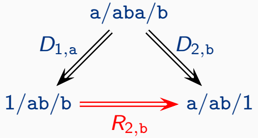
- Fact: $\underline{b} = \underline{a} \bullet R_{i,x}$ implies that $\underline{a}$ and $\underline{b}$ represent the same element in $\mathcal{U}(M)$.
  - Proof: We walk in the Cayley graph, replacing one path with an equivalent one. □

- Example: $M = B_3^+$ with $1/\mathtt{ab}/\mathtt{b}$:



b and ab admit a common multiple
  - we can push b through ab:
  - $\mathtt{a}/\mathtt{ab}/1 = 1/\mathtt{ab}/\mathtt{b} \bullet R_{2,\mathtt{b}}$

and now



  - possible confluence ?
  - In this way: for every gcd-monoid M, a rewrite system $\mathcal{R}_M$ ("reduction").

• <u>Theorem 1</u>: (i) *If M is a noetherian gcd-monoid satisfying the 3-Ore condition, then M embeds in $\mathcal{U}(M)$ and every element of $\mathcal{U}(M)$ is represented by a unique $\mathcal{R}_M$-irreducible multifraction; in particular, a multifraction $\underline{a}$ represents 1 in $\mathcal{U}(M)$ iff it reduces to $\underline{1}$.*

(ii) *If, moreover, M is strongly noetherian and has finitely many basic elements, the above method makes the word problem for $\mathcal{U}(M)$ decidable.*

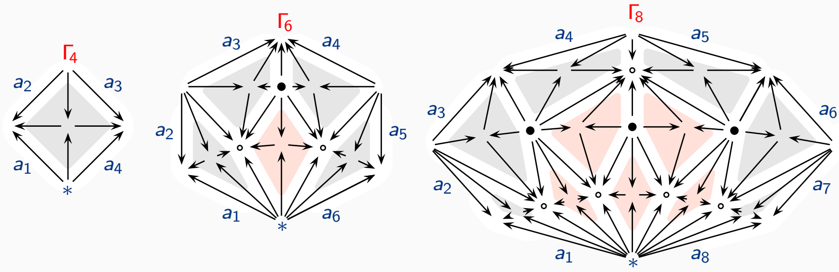
- M is noetherian: no infinite descending sequence for left- and right-divisibility.
- M is strongly noetherian: exists a pseudo-length function on M. ($\Rightarrow$ noetherian)
- M satisfies the 3-Ore condition: three elements that pairwise admit a common multiple admit a global one. (2-Ore $\Rightarrow$ 3-Ore)
- right-basic elements: obtained from atoms repeatedly using the right-complement operation: $(x, y) \mapsto x'$ s.t. $yx' = \text{right-lcm}(x, y)$.

• Fact: *If a noetherian gcd-monoid M satisfies the 3-Ore condition, then, for every multifraction $\underline{a}$ and every $i < \|\underline{a}\|$ (depth of $\underline{a}$:= # entries in $\underline{a}$), there exists a unique maximal level i reduction applying to $\underline{a}$.*

• Theorem 2: *For every n, there exists a universal sequence of integers $U(n)$ s.t., if M is any noetherian gcd-monoid satisfying the 3-Ore condition and $\underline{a}$ is any depth n multifraction representing 1 in $\mathcal{U}(M)$, then $\underline{a}$ reduces to $\underline{1}$ by maximal reductions at successive levels $U(n)$.*

- Example: $U(8) = (\underline{1, 2, 3, 4, 5, 6, 7}, \underline{1, 2, 3, 4, 5}, \underline{1, 2, 3}, \underline{1})$.

- Corollary: *For every n, there exists a universal diagram Γ_n s.t.,*
  if M is any noetherian gcd-monoid satisfying the 3-Ore condition
  and $\underline{a}$ is any depth n multifraction representing 1 in $\mathcal{U}(M)$,
  then some M-labelling of Γ_n is a van Kampen diagram with boundary $\underline{a}$.



- An Artin-Tits monoid: $\langle S \mid R\rangle^+$ such that, for all s, t in S,
  there is at most one relation $s... = t...$ in R and, if so, the relation has the form
  $stst... = tsts...$, both terms of same length (a "braid relation").

- Theorem (Brieskorn–Saito, 1971): *An Artin-Tits monoid satisfies the 2-Ore condition iff it is of spherical type (= the associated Coxeter group is finite).*
  - "Garside theory": group of fractions of the monoid

- Theorem: *An Artin-Tits monoid satisfies the 3-Ore condition iff it is of FC type (= parabolic subgroups with no ∞-relation are spherical).*
  - Reduction is convergent: group of multifractions of the monoid

- Conjecture: *Say that reduction is semi-convergent for M if every multifraction representing 1 in $\mathcal{U}(M)$ reduces to $\underline{1}$. Then reduction is semi-convergent for every Artin-Tits monoid.*
  - Sufficient for solving the word problem (in the case of an Artin-Tits group).

- Question: How to prove the conjecture for general Artin-Tits groups?
  - Partial results known (all Artin-Tits groups of "sufficiently large type").
  - Most probably relies on the theory of the underlying Coxeter groups.

- Question: Does the convergence of reduction imply torsion-freeness?

- Question: Does this extension of Ore's theorem in the "monoid/group" context make sense in a "ring/skew field" context?

- References:

  - P. Dehornoy, *Multifraction reduction I: The 3-Ore case and Artin-Tits groups of type FC*, J. Comb. Algebra 1 (2017) 185–228
  - P. Dehornoy, *Multifraction reduction II: Conjectures for Artin-Tits groups* J. Comb. Algebra, to appear, arXiv:1606.08995
  - P. Dehornoy & F. Wehrung, *Multifraction reduction III: The case of interval monoids* J. Comb. Algebra, to appear, arXiv:1606.09018
  - P. Dehornoy, D. Holt, & S. Rees, *Multifraction reduction IV: Padding and Artin-Tits groups of sufficiently large type*, arXiv:1701.06413

www.math.unicaen.fr/∼dehornoy/