Multifraction reduction and the Word Problem for Artin-Tits groups

Patrick Dehornoy

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen

AAA92, Prague, May 2016

- A new approach to the Word Problem for Artin-Tits groups (and other groups),
  - based on a rewrite system extending free reduction,
  - reminiscent of the Dehn algorithm for hyperbolic groups,
  - proved in particular cases, conjectured in the general case.

Plan:

- 1. The enveloping group of a monoid
  - Mal'cev theorem
  - Ore theorem
- 2. Reduction of multifractions
  - Free reduction
  - Division
  - Reduction
- 3. Artin–Tits monoids
  - The FC case
  - The general case
- 4. Interval monoids (joint with F. Wehrung)
  - The interval monoid of a poset
  - A criterion for near-convergence
  - Examples and counter-examples

Plan:

- 1. The enveloping group of a monoid
  - Mal'cev theorem
  - Ore theorem
- 2. Reduction of multifractions
  - Free reduction
  - Division
  - Reduction
- 3. Artin–Tits monoids
  - The FC case
  - The general case
- 4. Interval monoids (joint with F. Wehrung)
  - The interval monoid of a poset
  - A criterion for near-convergence
  - Examples and counter-examples

• <u>Proposition</u>: *For every monoid M, there exists a unique group $\mathcal{U}(M)$ and a morphism $\phi : M \to \mathcal{U}(M)$ s.t. every morphism from M to a group factors through ϕ.*
If $M = \langle S \mid R\rangle^+$, then $\mathcal{U}(M) = \langle S \mid R\rangle$.

• If M is not cancellative, ϕ is not injective: $ab = ac \Rightarrow \phi(ab) = \phi(ac) \Rightarrow \phi(b) = \phi(c)$.

• Even if M is cancellative, ϕ need not be injective:
for $M = \langle \mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}, \mathtt{a}', \mathtt{b}', \mathtt{c}', \mathtt{d}' \mid \mathtt{ac} = \mathtt{bd}, \mathtt{ac}' = \mathtt{bd}', \mathtt{a}'\mathtt{c} = \mathtt{b}'\mathtt{d}\rangle^+$,
$\phi(\mathtt{a}'\mathtt{c}') = \phi(\mathtt{a}'\mathtt{c})\phi(\mathtt{ac})^{-1}\phi(\mathtt{ac}') = \phi(\mathtt{b}'\mathtt{d})\phi(\mathtt{bd})^{-1}\phi(\mathtt{bd}') = \phi(\mathtt{b}'\mathtt{d}')$.

• <u>Theorem</u> (Mal'cev, 1937): *There exists an explicit infinite list of conditions $C_1, C_2, \ldots$ such that M embeds in $\mathcal{U}(M)$ iff M is cancellative and satisfies $C_1, C_2, \ldots$.*

(C_1): $\forall a, b, c, d, a', b', c', d'$ $((ac = bd$ and $ac' = bd'$ and $a'c = b'd) \Rightarrow a'c' = b'd')$.

- An easy case:

- 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.*

  ▸ " $\mathcal{U}(M)$ is a group of (right) fractions for M "

- Definition: a left-divides b, or b is a right-multiple of a, if $\exists x\,(ax = b)$. $\leftarrow a \leqslant b$
  - ▸ 2-Ore condition: Any two elements admits a common right-multiple.

- Examples: $\mathbb{N}$ *vs.* $\mathbb{Z}$, $\mathbb{Z}^+$ *vs.* $\mathbb{Q}^+$, $K[X]$ *vs.* $K(X)$, etc.

- Whenever 1 is the only invertible element, $\leqslant$ (left-divisibility) is a partial ordering;
  left-gcd:= greatest lower bound, right-lcm:= least upper bound (when they exist).

- Definition: A gcd-monoid is a cancellative monoid, in which 1 is the only invertible element and any two elements admit a left- and a right-gcd.

- 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$(a, b) = 1$

- Examples:
  - $M = B_n^+$, braid monoid on n strands, with $\mathcal{U}(M) = B_n$.
  - more generally: all Garside monoids and the associated Garside groups.

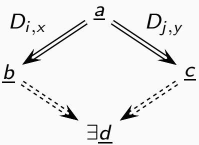
Plan:

- 1. The enveloping group of a monoid
  - Mal'cev theorem
  - Ore theorem
- 2. Reduction of multifractions
  - Free reduction
  - Division
  - Reduction
- 3. Artin–Tits monoids
  - The FC case
  - The general case
- 4. Interval monoids (joint with F. Wehrung)
  - The interval monoid of a poset
  - A criterion for near-convergence
  - Examples and counter-examples

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

- Example: $M = F^+$, 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 $a_1, a_2, \ldots$ 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"

- Proof: (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:

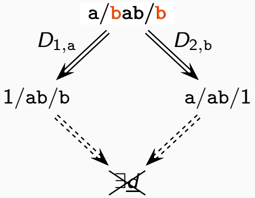


  - Every sequence $\underline{a}$ rewrites into a unique irreducible sequence ("convergence"). □

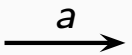
- When M is not free, the rewrite rule $D_{i,x}$ can still be given a meaning:
  - no first or last letter,
  - but left- and right-divisors: $x \leqslant a$ means "x is a possible beginning of a".
  - rule $D_{i,x} := \begin{cases} \text{for } i \text{ odd, right-divide } a_i \text{ and } a_{i+1} \text{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

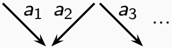
- Useful???

- Example: $M = B_3^+ = \langle \mathtt{a}, \mathtt{b} \mid \mathtt{aba} = \mathtt{bab} \rangle^+$;
  - start with the sequence $(\mathtt{a}, \mathtt{aba}, \mathtt{b})$, better written $\mathtt{a}/\mathtt{aba}/\mathtt{b}$ ("multifraction")

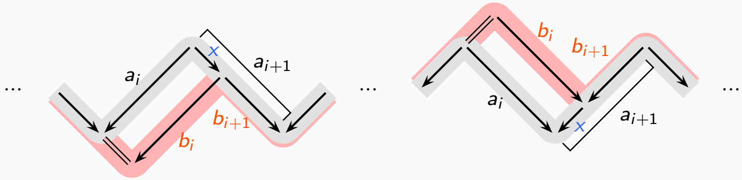


  - no hope of confluence...

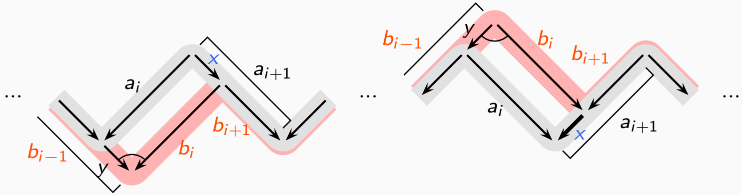
- Consider more general rewrite rules.
- Diagrammatic representation of elements of the monoid: $a \mapsto$ 

,
  ...and of multifractions ($=$ finite sequences): $a_1/a_2/a_3/\ldots \mapsto$ 

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



- Relax the condition "x divides a_i": declare $\underline{a} \bullet R_{i,x} = \underline{b}$ (even i) for

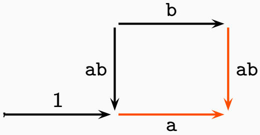


  - ▶ divide a_{i+1} by x, push x through a_i using lcm, multiply a_{i-1} by the reminder y.

- Definition: For i even, $\underline{b} = \underline{a} \bullet R_{i,x}$ ("$\underline{b}$ obtained from $\underline{a}$ by reducing x at level i") if
$$b_{i-1} = a_{i-1}y, \quad xb_i = a_iy = \text{right-lcm}(x, a_i), \quad xb_{i+1} = a_{i+1},$$
and $b_k = a_k$ for $k \neq i-1, i, i+1$, and symmetrically for i odd.

  - ▶ $\underline{a} \bullet D_{i,x}$ is defined if x divides both a_i and a_{i+1};
  - ▶ $\underline{a} \bullet R_{i,x}$ is defined if x divides a_{i+1}, and x and a_i have a common multiple.

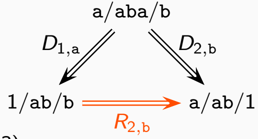
- Example: $M = B_3^+$ with $1/\mathtt{ab}/\mathtt{b}$.



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: a rewrite system $\mathcal{R}(M)$ ("reduction") for every gcd-monoid M.

• <u>Theorem</u>: (i) *If M is a noetherian gcd-monoid satisfying the 3-Ore condition, then M embeds in $\mathcal{U}(M)$ and $\mathcal{R}(M)$ is convergent: every element of $\mathcal{U}(G)$ is represented by a unique $\mathcal{R}(M)$-irreducible multifraction.*

(ii) *If, moreover, M is strongly noetherian and has finitely many primitive elements, then the Word Problem for $\mathcal{U}(M)$ is 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-primitive elements: obtained from atoms repeatedly using the right-complement operation: $(x, y) \mapsto x'$ s.t. $yx' = \text{right-lcm}(x, y)$.

• <u>Proof</u>: (i) The rewrite system $\mathcal{R}(M)$ is convergent:
- noetherianity of M ensures termination;
- the 3-Ore condition ensures confluence.

(ii) Finitely many primitive elements provides an upper bound for possible common multiples, ensuring that $\Rightarrow$ is decidable. □

Plan:

- 1. The enveloping group of a monoid
  - Mal'cev theorem
  - Ore theorem
- 2. Reduction of multifractions
  - Free reduction
  - Division
  - Reduction
- 3. Artin–Tits monoids
  - The FC case
  - The general case
- 4. Interval monoids (joint with F. Wehrung)
  - The interval monoid of a poset
  - A criterion for near-convergence
  - Examples and counter-examples

- 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.

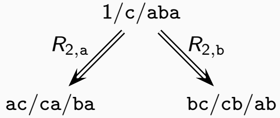
- Proposition (Brieskorn–Saito, 1971): *An Artin-Tits monoid satisfies the* 2*-Ore condition iff it of spherical type.*
  ↑
  adding $s^2 = 1$ for every s in S yields a finite Coxeter group
  - "Garside theory"

- Proposition: *An Artin-Tits monoid satisfies the* 3*-Ore condition iff it of FC ("flag complex") type.*
  ↑
  if $\forall s, t \in S' \subseteq S\ \exists s... = t...$ in R, then $\langle S' \rangle$ is spherical
  - a new (?) normal form for AT-monoids of FC type
    ↑
    (L. Paris) connection with the Niblo–Reeves action on a CAT(0)-complex?

- Good news: Every AT-monoid satisfies the assumptions:
  - strongly noetherian (relations preserve the length of words);
  - finitely many primitive elements (D.-Dyer-Hohlweg, 2015).

- Bad news: Every AT-monoid is not of FC-type...

- Example: type $\widetilde{A}_2$: $\langle \mathtt{a}, \mathtt{b}, \mathtt{c} \mid \mathtt{aba} = \mathtt{bab}, \mathtt{bcb} = \mathtt{cbc}, \mathtt{cac} = \mathtt{aca} \rangle^+$
  - the elements a, b, c pairwise admit common multiples, but no global multiple
  - the rewrite system $\mathcal{R}(M)$ is not confluent:

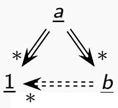


  - ???

- <u>Definition</u>: The system $\mathcal{R}(M)$ is near-convergent if

$$\underline{a} \text{ represents } 1 \text{ in } \mathcal{U}(M) \quad \text{iff} \quad \underline{a} \Rightarrow^* \underline{1}.$$

  - Equivalently: conjunction of $\underline{a} \Rightarrow^* \underline{1}$ and $\underline{a} \Rightarrow^* \underline{b}$ implies $\underline{b} \Rightarrow^* \underline{1}$:



- <u>Lemma</u>: *If $\mathcal{R}(M)$ is convergent, then it is near-convergent.*

- <u>Proposition</u>: *If M is a strongly noetherian gcd-monoid with finitely many primitive elements and $\mathcal{R}(M)$ is near-convergent, the Word Problem for $\mathcal{U}(M)$ is decidable.*

- <u>Conjecture</u>: *For <u>every</u> Artin-Tits monoid M, the system $\mathcal{R}(M)$ is near-convergent.*

  - Would imply the decidability of the Word Problem for AT groups.
  - Similarity with the Dehn algorithm: no introduction of pairs ss^{-1} or $s^{-1}s$.

- <u>Example</u>: type $\widetilde{\mathrm{A}}_2$: $\langle \mathtt{a}, \mathtt{b}, \mathtt{c} \mid \mathtt{aba} = \mathtt{bab}, \mathtt{bcb} = \mathtt{cbc}, \mathtt{cac} = \mathtt{aca} \rangle^+$

$$\begin{array}{ccc} & \mathtt{1/c/aba} & \\ {\scriptstyle R_{2,\mathtt{a}}} \swarrow & & \searrow {\scriptstyle R_{2,\mathtt{b}}} \\ \mathtt{ca/ac/ba} & & \mathtt{cb/bc/ab} \end{array}$$

  - ▶ The quotient ca/ac/ba/ab/bc/cb represents 1 in the group...

... and, indeed, it reduces to <u>1</u>:

$$\begin{array}{rcll} \mathtt{ac/ca/ba/ab/cb/bc} & \Rightarrow & \mathtt{ac/cac/b/1/cb/bc} & \text{via } R_{3,\mathtt{ab}} \\ & \Rightarrow & \mathtt{ac/cac/bcb/1/1/bc} & \text{via } R_{4,\mathtt{cb}} \\ & \Rightarrow & \mathtt{ac/cac/bcb/bc/1/1} & \text{via } R_{5,\mathtt{bc}} \\ & \Rightarrow & \mathtt{1/c/bcb/bc/1/1} & \text{via } R_{1,\mathtt{ac}} \\ & \Rightarrow & \mathtt{bc/1/1/bc/1/1} & \text{via } R_{2,\mathtt{cbc}} \\ & \Rightarrow & \mathtt{bc/bc/1/1/1/1} & \text{via } R_{3,\mathtt{bc}} \\ & \Rightarrow & \mathtt{1/1/1/1/1/1} & \text{via } R_{1,\mathtt{bc}} \end{array}$$

- Conjecture supported by massive computer experiments.

- Finite approximation $(\mathcal{NC}_n)$: Near-convergence for depth n;
  - ▶ Then $(\mathcal{NC}_2)$ equivalent to $M \hookrightarrow \mathcal{U}(M)$, which is true (L. Paris, 2001).

Plan:

- 1. The enveloping group of a monoid
    - Mal'cev theorem
    - Ore theorem
- 2. Reduction of multifractions
    - Free reduction
    - Division
    - Reduction
- 3. Artin–Tits monoids
    - The FC case
    - The general case
- 4. Interval monoids (joint with F. Wehrung)
    - The interval monoid of a poset
    - A criterion for near-convergence
    - Examples and counter-examples

- Definition (F.Wehrung): For $(P, \leqslant)$ a poset, the interval monoid of P is

$$\mathrm{Int}(P) := \langle \{[x,y] \mid x < y \in P\} \mid \{[x,y][y,z] = [x,z] \mid x < y < z \in P\}\rangle^+.$$

↑ the intervals of P

- Lemma: *A monoid* $\mathrm{Int}(P)$ *embeds in its group; it is a gcd-monoid iff, for every* $x \in P$, $P^{\geqslant x}$ *is a* $\wedge$*-semilattice and* $P^{\leqslant x}$ *is a* $\vee$*-semilattice.*

- Proposition (D.–Wehrung) *Assume that* M *is the interval monoid of a finite poset* P*, and* M *is a gcd-monoid. Define a simple circuit in* P *to be a finite sequence* $(x_0, ..., x_n)$ *in* P *satisfying*
  - $x_i < x_{i-1}$ *and* $x_i < x_{i+1}$ *for* i *even,*
  - $x_0 = x_n$ *and* $x_i \neq x_j$ *for* $1 \leqslant i < j \leqslant n$.

  Say that a circuit is reducible if ... (an effectively checkable combinatorial property).
  - *If every simple circuit of* P *is reducible, then* $\mathcal{R}(M)$ *is near-convergent;*
  - *If every length* $\leqslant n$ *simple circuit of* P *is reducible, then* M *satisfies* $(\mathcal{NC}_n)$.

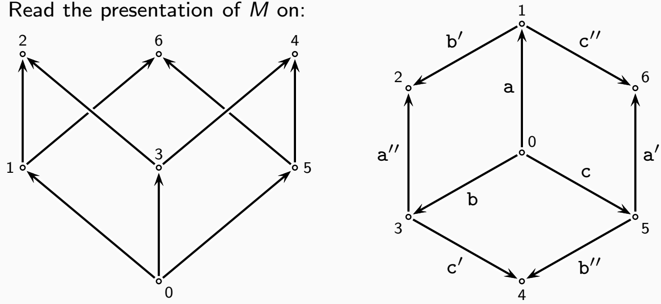
- A checkable condition when P is finite:

  a finite poset admits finitely many simple circuits.

- Is near-convergence weaker than convergence?

- Proposition (D.-Wehrung): *There exists a noetherian gcd-monoid M such that $\mathcal{R}(M)$ is near-convergent but not convergent.*

- Proof: Read the presentation of M on:



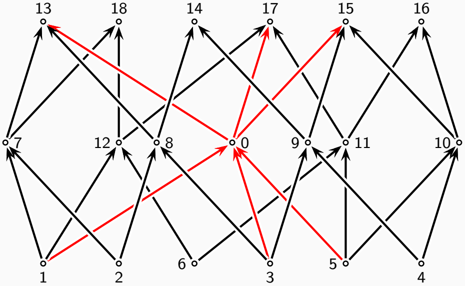
$$M = \langle \mathtt{a}, \mathtt{a}', \mathtt{a}'', \mathtt{b}, \mathtt{b}', \mathtt{b}'', \mathtt{c}, \mathtt{c}', \mathtt{c}'' \mid \mathtt{ab}' = \mathtt{ba}'', \mathtt{bc}' = \mathtt{cb}'', \mathtt{ca}' = \mathtt{ac}'' \rangle^+$$

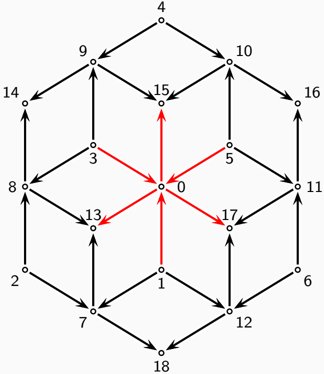
▸ $\mathcal{R}(M)$ is not convergent because M does not satisfy the 3-Ore condition. □

- Are the properties $(\mathcal{NC}_n)$ stronger and stronger?

- <u>Proposition</u> (D.–Wehrung): *For every even $n \geqslant 4$, there exists a noetherian gcd-monoid M satisfying $(\mathcal{NC}_{n'})$ for $n' < n$ but not $(\mathcal{NC}_n)$.*

- Proof: Read the presentation on (here $n = 6$):





  ▸ a necklace of n connected diamonds,
  plus a central cross connecting each other extremal vertex. ☐

- The monoids $\mathrm{Int}(P)$ are (very) far from Artin-Tits monoids
  ▸ A proof of the conjecture will require specific "non-Garside" arguments.