Subword Reversing and Ordered Groups

Patrick Dehornoy
Laboratoire de Mathématiques Nicolas Oresme
Université de Caen

- Use subword reversing to constructing examples of ordered groups.

- Subword Reversing is a combinatorial method (≈ rewrite rule on words) for investigating (certain) concrete positive group presentations.

↑ all relations of the form $w = w'$ with no s^{-1} in w, w'

- Here, case of triangular presentations: construct monoids in which the left-divisibility relation is a linear ordering.

↑ all relations of the form $s_i r_i = s_{i+1}$, with r_i a positive word

- (Modest) output: a very simple (self-contained) proof of

- Proposition (Navas, Ito).— For $n, m \geqslant 1$, the group $\langle x, y \mid x^m = y^n \rangle$ is left-orderable with isolated points in the LO space.

(and a new proof of the orderability of the braid group B_3)

– Plan –

I. What is subword reversing?

II. Subword reversing in a triangular context

Appendix. The μ function on positive braids

– Part I –

What is subword reversing?

- A strategy for constructing Kampen diagrams

all relations of the form $w = w'$ with w, w' nonempty words in S (no s^{-1})
↓
- Let (S, R) be a positive group presentation.
  Then two words u, v in S represent the same element in the monoid $\langle S \mid R \rangle^+$
  iff there exists an R-derivation from u to v: $u \equiv_R^+ v$.

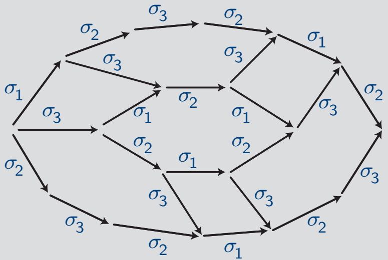
- **Proposition** (van Kampen?).— The relation $u \equiv_R^+ v$ holds iff
  there exists a van Kampen diagram for (u, v).

↑
a tesselated disk with (oriented) edges labeled by elements of S and faces labeled by relations of R, with boundary paths labeled u and v.

- Example:

  $B_4^+ = \langle \sigma_1, \sigma_2, \sigma_3 \mid \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$
  $\sigma_2\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_3, \sigma_1\sigma_3 = \sigma_3\sigma_2 \rangle^+$

  A van Kampen diagram
  for $(\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_2, \sigma_2\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3)$ is



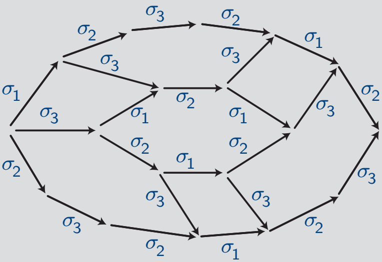
- How to build a van Kampen diagram for (u, v)—when it exists?

- **Definition.**— Subword reversing = the "left strategy", i.e.,
  - look at the (a) leftmost pending pattern 

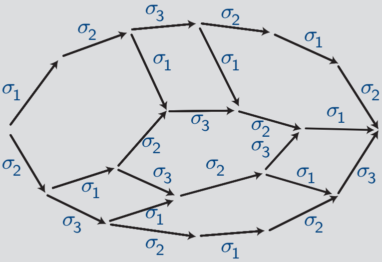
,
  - choose a relation $s\ldots = t\ldots$ of R to close this pattern into 

, and repeat.

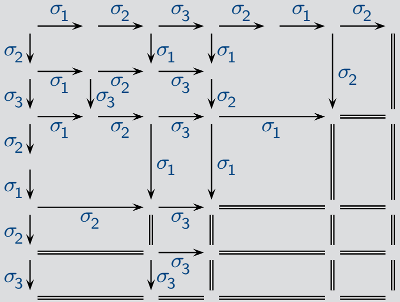
- Example: same as before



- Example: using subword reversing

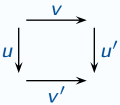


- Another way of drawing the same diagram: "reversing diagram"

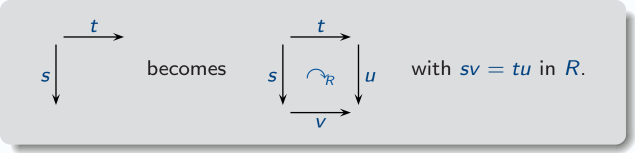


⇝ only vertical and horizontal arrows,
plus equality signs connecting vertices that are to be identified
in order to (possibly) get an actual van Kampen diagram.

- Can be applied with arbitrary (= not necessarily equivalent) initial words and then (possibly) leads to a diagram of the form



• In this way, a uniform pattern:

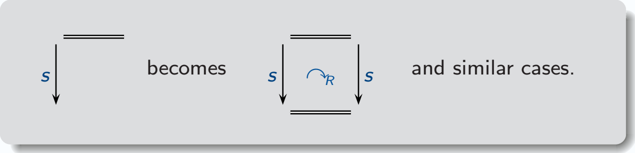


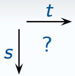
• Encoding by signed words: read labels from SW to NE and put a negative sign when one crosses in the wrong direction (words in $S \cup S^{-1}$). The basic step reads

$$s^{-1}t \curvearrowright_R vu^{-1} \text{ ("} s^{-1}t \text{ reverses to } vu^{-1}\text{")}.$$

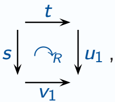
Then subword reversing means replacing $-+$ with $+-$, whence the terminology.

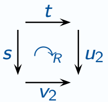
• Degenerated cases:



- Reversing may be stuck: 

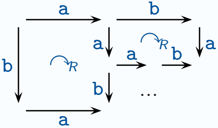
if no relation $s\ldots = t\ldots$;

- Result may not be unique: 

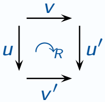
, 

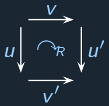
, if several relations $s\ldots = t\ldots$;

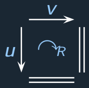
- Reversing may never terminate (unless relations involve words of length $\leqslant 2$): assume $\mathtt{a}^2\mathtt{b} = \mathtt{ba}$:



- Reversing may terminate with nonempty output words: (certainly happens if input words u, v are not equivalent)



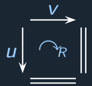
- **Lemma.**— 

implies $uv' \equiv_R^+ vu'$. In particular, 

implies $u \equiv_R^+ v$.

- When is reversing useful ?

  ...When it succeeds in building a van Kampen diagram whenever one exists.

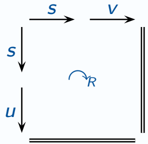
- **Definition.**— A presentation (S, R) is called complete for $\curvearrowright$ if $u \equiv_R^+ v$ implies 

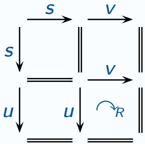
.

- Remark.— Completeness for $\curvearrowright$ does **not** imply the solvability of the word problem unless reversing has been proved to always terminate.

- **Proposition.**— Assume (S, R) is complete for $\curvearrowright$ and contains no relation $s... = s...$. Then the monoid $\langle S \mid R \rangle^+$ is left-cancellative ($fg = fh$ implies $g = h$).

- Proof. Assume $su \equiv_R^+ sv$.

By completeness, 

. Must be 

. Hence $u \equiv_R^+ v$ □

- How to recognize completeness?

- Proposition.— If (S, R) is homogeneous, then (S, R) is complete for $\curvearrowright$ iff, for all r, s, t in S, the cube condition for r, s, t is satisfied.

  - homogeneous: there exists an R-invariant function $\lambda : S^* \to \mathbb{N}$ s.t. $\lambda(sw) > \lambda(w)$.
    typically : $\lambda(w) =$ length of w if preserved by the relations of R
    for instance : braid relations $\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$
  - cube condition for three words u, v, w: some effective transitivity condition involving the reversings of $u^{-1}v$, $v^{-1}w$, and $u^{-1}w$.

- Summary.— In good cases (= complete presentations), subword reversing is useful
  - for proving cancellativity,
  - for solving word problems (both for monoids and for groups),
  - for recognizing Garside structures and computing with them, etc.

- What for a non-complete presentation? Make it complete : completion procedure...

– Part II –

Subword reversing in a triangular context

- Construct monoids in which the left-divibility relation is a linear ordering, thus leading to ordered groups of fractions.

- Definition.— For M a monoid and f, g in M, say that f is a left-divisor of g, or g is a right-multiple of f, denoted $f \preccurlyeq g$, if we have $fg' = g$ for some g' (of M).

- Recall: (S, R) triangular if $S = \{s_1, s_2, ...\}$ and $R = \{s_i r_i = s_{i+1} \mid i = 1, 2, ...\}$,
with r_i word in S (no letter s^{-1}).

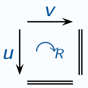
  Typically: $(\mathtt{a}, \mathtt{b} \mid \mathtt{aba} = \mathtt{b}, \mathtt{b}^2\mathtt{cac}^2 = \mathtt{c})$, ...

- Bad news: a triangular presentation is (almost) never homogeneous:
e.g., $\mathtt{aba} = \mathtt{b}$ makes $\lambda(\mathtt{b}) < \lambda(\mathtt{ab}) \leqslant \lambda(\mathtt{aba}) = \lambda(\mathtt{b})$ impossible

- Good news:

- **Main lemma.**— Every triangular presentation is complete for $\curvearrowright$.

- Proof. Show using induction on k that

  $u \equiv_R^{+(k)} v$ ($\exists$ a length k derivation from u to v) implies .

Claim: Let $\widetilde{u}$ be obtained from u by replacing the first letter, say s_i, with $s_1 r_1 ... r_{i-1}$.
Then $u \equiv_R^{+(k)} v$ implies $\widetilde{u} \equiv_R^{+(k)} \widetilde{v}$, and, if the first letter changes at least once in $u \equiv_R^{+(k)} v$, one even has $\widetilde{u} \equiv_R^{+(<k)} \widetilde{v}$.

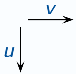
↑ makes the induction possible

□

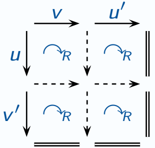
• Recall: Interested in the case when the left-divisibility relation $\preccurlyeq$ — which in general is a partial (pre)-order — is a linear order: any two elements are comparable.

• **Lemma.**— Assume (S, R) is a triangular presentation. Then any two elements f, g of $\langle S \mid R \rangle^+$ that admit a common right-multiple are comparable for $\preccurlyeq$.

• Proof. Choose words u, v in S^* that represent f and g. The assumption is that $uv' \equiv_R^+ vu'$ holds for some u', v'.

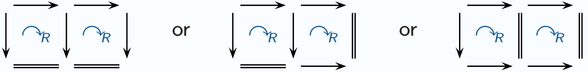
Step 1: Reversing 

must terminate in finitely many steps.

Indeed: by completeness, we must have 

.

Step 2: A terminating reversing finishes with at least one empty word. Indeed, use induction on the number n of reversing steps. For $n = 1$, follows from triangularity of (S, R). For $n > 1$, three possible ways of concatenating two reversing diagrams:



□

• The aim is to prove that the left-divisibility relation $\preccurlyeq$ is (possibly) a linear ordering. By the lemma, it is enough to prove that any two elements admit a common right-multiple. How to prove that property?

• Lemma.— Assume that M is a monoid generated by S and δ is a central element of M that is a right-multiple of every element of S. Then every element of M left-divides δ^r for r large enough.

• Proof. Show using induction on r that $h \in S^r$ implies $h \preccurlyeq \delta^r$. By assumption, true for $r = 1$. Assume $h \in S^r$ with $r > 1$. Write $h = fg$, $f \in S^p$, $g \in S^q$ and $p + q = r$. By IH, there exists f', g' s.t. $ff' = \delta^p$, $gg' = \delta^q$. Then

$$h \cdot g'f' = fgg'f' = f\delta^q f' = ff'\delta^q = \delta^p\delta^q = \delta^r. \qquad \square$$

• ...(under the same hypotheses) any two elements of M admit a common right-multiple.

• **Proposition.**— For $p, q \geqslant 1$, let $G_{p,q} = \langle \mathtt{a}, \mathtt{b} \mid (\mathtt{ab}^p)^q\mathtt{a} = \mathtt{b} \rangle$. Then $G_{p,q}$ is left-orderable, and $LO(G_{p,q})$ has isolated points.

• Proof. Let $G^+_{p,q} = \langle \mathtt{a}, \mathtt{b} \mid (\mathtt{ab}^p)^q\mathtt{a} = \mathtt{b} \rangle^+$. The presentation $(\mathtt{a}, \mathtt{b} \mid (\mathtt{ab}^p)^q\mathtt{a} = \mathtt{b})$ is triangular. Hence the monoid $G^+_{p,q}$ is left-cancellative. Let $\delta = \mathtt{b}^{p+1}$. Then

$$\mathtt{a}\delta = \mathtt{ab}^p\mathtt{b} = \mathtt{ab}^p(\mathtt{ab}^p)^q\mathtt{a} = (\mathtt{ab}^p)^q\mathtt{ab}^p\mathtt{a} = \mathtt{bb}^p\mathtt{a} = \delta\mathtt{a}.$$

So δ lies in the center of $G^+_{p,q}$. Hence any two elements of $G^+_{p,q}$ have a common right-multiple, and the left-divisibility relation $\preccurlyeq$ is a linear order on $G^+_{p,q}$.
By symmetry, $G^+_{p,q}$ is right-cancellative. By Ores's theorem, $G_{p,q}$ is a group of fractions for $G^+_{p,q}$, and $G^+_{p,q}$ is the positive cone of a left-invariant ordering on $G_{p,q}$. □

• Remark.— Put $x = \mathtt{ab}^p$ and $y = \mathtt{b}$. Then $(\mathtt{ab}^p)^q\mathtt{a} = \mathtt{b}$ (iff) $x^{q+1} = y^{p+1}$.

• Particular cases:
- $p = q = 1$: $\mathtt{aba} = \mathtt{b}$ (or $x^2 = y^2$), the Klein bottle group K;
- $p = 2, q = 1$: $\mathtt{ab}^2\mathtt{a} = \mathtt{b}$ (or $x^2 = y^3$), the 3-strand braid group B_3;
- $p = 1, q = 2$: $\mathtt{ababa} = \mathtt{b}$ (or $x^3 = y^2$), the 3-strand braid group B_3 again.

– Appendix –

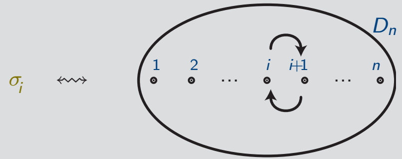
The μ function on positive braids

…The orderability of braid groups is 20 years old this week.

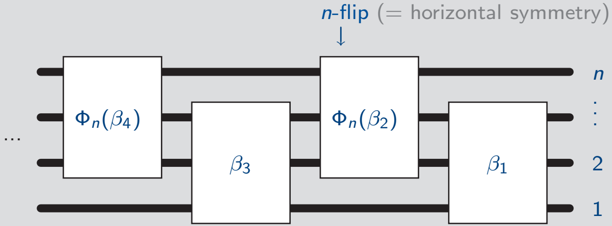
- Artin's braid group B_n: $\left\langle \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{rl} \sigma_i\sigma_j = \sigma_j\sigma_i & \text{for } |i-j| \geqslant 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{for } |i-j| = 1 \end{array} \right\rangle$.

$\simeq$ { braid diagrams }/ isotopy:

$\simeq$ mapping class group of D_n (disk with n punctures):



- Associate with every braid β in B_n^+
  a finite sequence $(\ldots, \beta_3, \beta_2, \beta_1)$ of braids in B_{n-1}^+: the *n*-splitting of β.



- Iterating the splitting operation gives for every β in B_n^+ a finite tree $T_n(\beta)$.

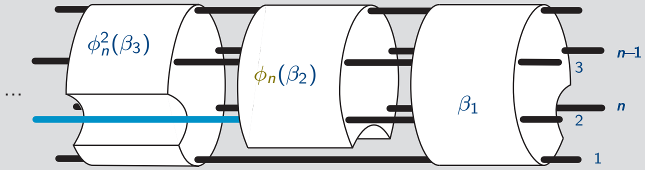
- **Theorem** (D., 2007, building on Burckel, 1997): For β, β' in B_n^+,
  $\beta <_D \beta'$ is equivalent to $T_n(\beta) <^{\text{ShortLex}} T_n(\beta')$.

- **Corollary**.— The D-ordering on B_n^+ is a well-ordering of type $\omega^{\omega^{n-2}}$.

• Definition (Birman-Ko-Lee, 1997).— The dual braid monoid B_n^{+*} is the submonoid of B_n generated by $(a_{i,j})_{1 \leqslant i < j \leqslant n}$ with $a_{i,j} = \sigma_{j-1}^{-1} \ldots \sigma_{i+1}^{-1} \sigma_i \sigma_{i+1} \ldots \sigma_{j-1}$.

• Dual Garside structure for B_n, with Cat_n non-crossing partitions vs. $n!$ permutations.

• Then similar splitting of braids in B_n^{+*} into sequences of braids in B_{n-1}^{+*}.



• Iterating the dual splitting operation gives for every β in B_n^{+*} a finite tree $T_n^*(\beta)$.

• Theorem (Fromentin, 2008): For β, β' in B_n^{+*},

$\beta <_D \beta'$ is equivalent to $T_n^*(\beta) <^{\mathrm{ShortLex}} T_n^*(\beta')$.

• Corollary.— The D-ordering on B_n^{+*} is a well-ordering of type $\omega^{\omega^{n-2}}$.

- **Definition.**— For β in B_∞^+ (resp. in B_∞^{+*}), put

$$\mu(\beta) = \min_{<_D}\{\, \beta' \in B_\infty^+ \mid \beta' \text{ conjugate to } \beta \,\}$$
$$(\text{resp. } \mu^*(\beta) = \min_{<_D}\{\, \beta' \in B_\infty^{+*} \mid \beta' \text{ conjugate to } \beta \,\}).$$

- Makes sense because $<_D$ is a well-ordering on B_∞^+ and B_∞^{+*}.
- Example: $\mu(\sigma_1) = \mu(\sigma_2) = ... = \sigma_1$, $\mu(\Delta_3) = \Delta_3$, ...

- **The problem** : Compute μ and/or μ^* effectively (at least for 3 or 4 strands).

- Computing μ or μ^* would give a solution (of a totally new type) for the Conjugacy Problem of B_n.
- Remark (good news): The (alternating and) rotating normal forms now give realistic ways of investigating the order $<_D$.

- **Conjecture** (D., Fromentin, Gebhardt, 2009).— For β in B_3^+,

$$\mu(\beta\Delta_3^2) = \sigma_1\sigma_2^2\sigma_1 \cdot \mu(\beta) \cdot \sigma_2^2.$$

- A. Navas, *A remarkable family of left-ordered groups: central extensions of Hecke groups*, J. Algebra, 328 (2011) 31-42.

- T. Ito, *Dehornoy-like left-orderings and isolated left-orderings*, arXiv:1103.4669.

- T. Ito, *Construction of isolated left-orderings via partially central cyclic amalgamation* arXiv:1107.0545.

- P. Dehornoy, *The subword reversing method*, Intern. J. Alg. and Comput. 21 (2011) 71–118

- P. Dehornoy, I. Dynnikov, D. Rolfsen, B. Wiest, Ordering Braids, Mathematical Surveys and Monographs vol. 148, Amer. Math. Soc. (2008).

- J. Fromentin, *Every braid admits a short sigma-definite expression*, J. Europ. Math. Soc. 13 (2011) 1591–1631.

www.math.unicaen.fr/∼dehornoy