The Subword Reversing Method

Patrick Dehornoy

Laboratoire de Mathématiques
Nicolas Oresme, Université de Caen

- A strategy for constructing van Kampen diagrams for semigroups, with various applications: cancellativity, embedding in a group, recognizing Garsideness, determining combinatorial distance...

Plan :

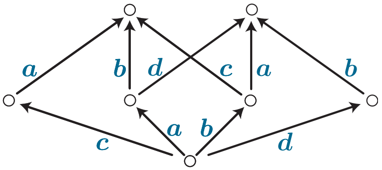
- 1. Subword Reversing : Description
- 2. Subword Reversing : Range
- 3. Subword Reversing : Uses
- 4. Subword Reversing : Efficiency

1. Subword Reversing : Description

- A motivating example
- Van Kampen diagrams
- Reversing : geometric description
- Reversing : syntactic description

- Our red line in the sequel:

$$M = \langle a, b, c, d \,|\, ab = bc = ca, ba = db = ad \rangle^+.$$



- Typical questions:
  - Is M cancellative?
  - Does M embed in a group?
  - Does the universal group of M admit an automatic structure connected with this presentation?

- Note: M is **not** eligible for Adjan's cancellativity criterion.

all relations of the form $u = v$ with u, v nonempty words on S

↓

- Let (S, R) be a semigroup presentation.
  Two words w, w' on S represent the same element of the monoid $\langle S \mid R\rangle^+$
  if and only if there exists an R-derivation from w to w'.

- **Proposition** (van Kampen, ?): Two words w, w' on S represent the same element of $\langle S \mid R\rangle^+$ if and only if there exists a van Kampen diagram for (w, w').

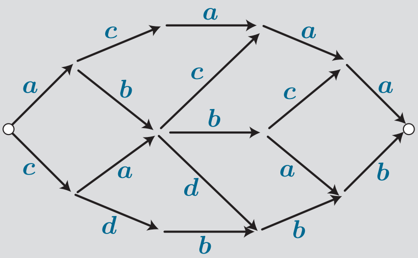
↑

a tesselated disk with (oriented) edges labeled by elements of S and faces labeled by relations of R, with boundary paths labelled w and w'.

- **Example:**

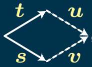
  Let $M = \langle a, b, c, d \mid ab = bc = ca, ba = db = ad\rangle^+$ (our preferred example).

  Then a van Kampen diagram for $(acaaa, cdbbb)$ is



- **How to build a van Kampen diagram for (w, w')—when it exists?**
  (includes solving the word problem, i.e., deciding whether w, w' are R-equivalent)

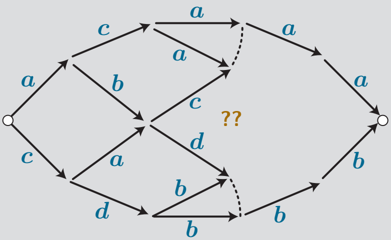
- **Definition : Subword reversing** = the "left strategy", i.e.,
  - look at the (a) leftmost pending pattern 

  ,
  - choose a relation $sv = tu$ of R to close this pattern into 

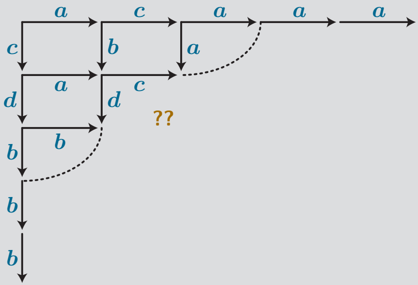
  , and repeat.

- **Facts** : - May not be possible
  (no relation $s... = t...$);
  - May not be unique
  (several relations $s... = t...$);
  - May never terminate
  (if u, v have length more than 1);
  - May terminate but boundary words are longer than w, w'
  (certainly happens if w, w' are not R-equivalent).

- **Example:** (same hypotheses)

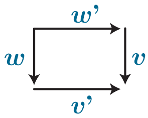


- Another way of drawing the same diagram: "reversing diagram"

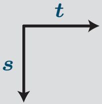


⇝ only vertical and horizontal edges,
plus dotted arcs connecting vertices that are to be identified
in order to (possibly) get an actual van Kampen diagram.

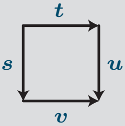
- Can be applied with arbitrary (= equivalent or not) initial words
and then possibly gives a common right-multiple
of (the elements represented by) these words:



- In this way, a uniform pattern:

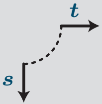


becomes

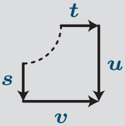


with $sv = tu$ in R.

- More exactly:

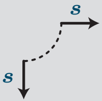


becomes

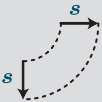


with $sv = tu$ in R,

including



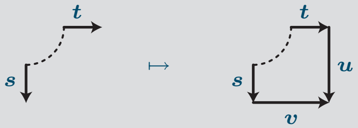
becomes



.

- Syntactic description of the reversing process:
  - introduce a formal copy S^{-1} of the alphabet S;
  - read words from SW to NE, using s^{-1} when a vertical s-edge is crossed (in the wrong direction).

- Basic step:



reads: $s^{-1}t \curvearrowright vu^{-1}$,
↑
reverses to

including

reads: $s^{-1}s \curvearrowright \varepsilon$.
↑
the empty word

- In this setting, "subword reversing" means replacing $-+$ with $+-$, whence the terminology.

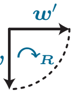
- **Definition** : For w, w' words on $S \cup S^{-1}$, declare $w \curvearrowright_R^1 w'$ if
  $\exists s, t, u, v$ ($sv = tu$ belongs to R and $w = \dots s^{-1}t \dots$ and $w' = \dots vu^{-1} \dots$).

  Declare $w \curvearrowright_R w'$ if there exist $w_0, \dots, w_p$ s.t.
  $w_0 = w$, $w_p = w'$, and $w_i \curvearrowright_R^1 w_{i+1}$ for each i.

- Terminal words: $v'v^{-1}$ with v, v' words on S
  (no $-+$ pattern $s^{-1}t$ to possibly reverse).

- **Lemma** : If w, w', v, v' are words on S,
  then $w^{-1}w' \curvearrowright_R v'v^{-1}$, i.e., w  v , implies $wv' \equiv_R^+ w'v$.

(obvious, since one gets a witnessing van Kampen diagram)

- In particular, $w^{-1}w' \curvearrowright_R \varepsilon$, i.e., w  , implies $w \equiv_R^+ w'$.

  ↑ the empty word

2. Subword Reversing : Range

- Completeness
- The cube condition

- When is reversing useful ?

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

- **Definition** : A presentation (S, R) is called **complete** (w.r.t. subword reversing) if $w \equiv_R^+ w'$ implies $w^{-1}w' \curvearrowright_R \varepsilon$.

↑ hence ... is equivalent to ...

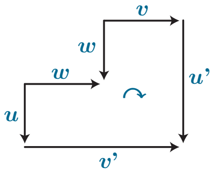
- **Two remarks** :
  - Completeness implies the solvability of the word problem **only if** reversing is proved to always terminate.
  - Our favourite presentation $(a, b, c, d \mid \ldots)$ is not complete: $acaaa$ and $cdbbb$ are equivalent, but $(acaaa)^{-1}(cdbbb) \curvearrowright \varepsilon$ fails —and so does $(acaaa)^{-1}(cdbbb) \curvearrowright v'v^{-1}$ for all positive words v, v'.

- **Three problems** :
  - How to recognize completeness?
  - What to do with a non-complete presentation? (Make it complete...)
  - What to do with a complete presentation? (Prove properties of the monoid.)

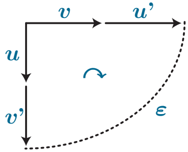
- **Theorem** (D., ’97 and ’02): Assume that (S, R) is a homogeneous presentation. Then (S, R) is complete if, and only if,
  for each triple r, s, t in S, the cube condition for r, s, t is satisfied.

- homogeneous: exists R-invariant function $\lambda : S^* \to \mathbb{N}$ s.t. $\lambda(sw) > \lambda(w)$.

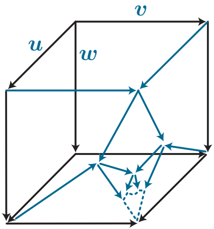
- cube condition for
  a triple u, v, w:



implies

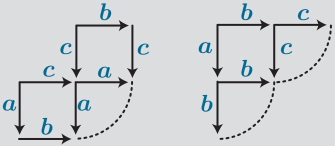


- called “cube condition” because it means
  that every reversing (u, v, w)-cube closes:

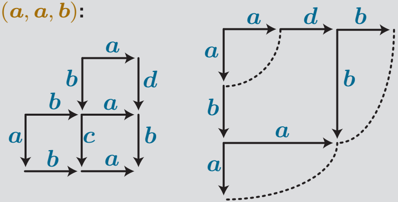


- **Example:** $M = \langle a, b, c, d \mid ab = bc = ca,\ ba = db = ad \rangle^+$.
  - Homogeneous: take $\lambda =$ length.
  - Cube condition?

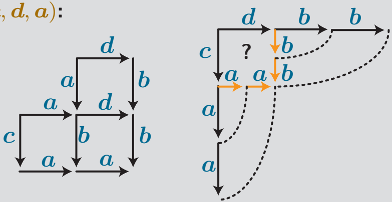
(a, b, c):



(a, a, b):

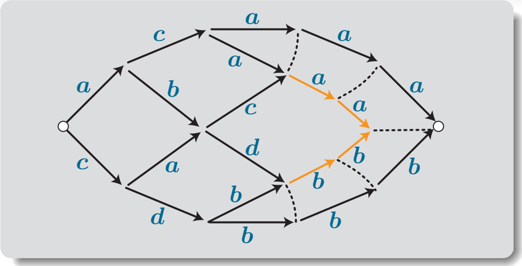


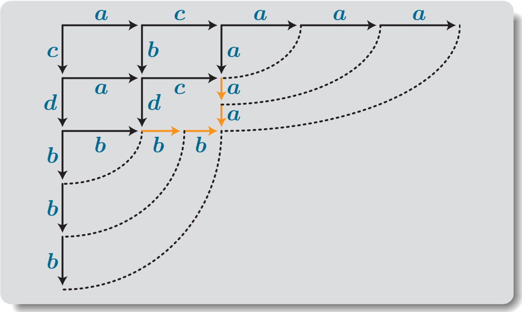
(c, d, a):



$\rightsquigarrow$ A completion procedure: if the cube fails, add the (redundant) missing relation.

here: add $caa = dbb$.


a
c
a
a
a
a
b
a
c
a
c
d
a
b
b
b
d
b
b
b

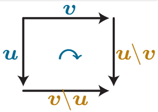

a
c
a
a
a
c
b
a
a
c
a
d
d
a
b
b
b
b
b
b

- Three possible cases:
  - Originally complete presentations (the optimal case);
  - Presentations that become complete after finitely many completion steps
    = the case of our current example: becomes complete
    after adding the single (redundant) relation $caa = dbb$;
  - Presentations that require infinitely many completion steps (the bad case).

- A particular framework:

- **Definition** : A semigroup presentation (S, R) is called **complemented** if, for all s, t in S, there is at most one relation $s \ldots = t \ldots$ in R.

- For a complemented presentation, reversing is deterministic:
  (= only one reversing diagram for all initial words u, v)



- **Proposition** : If (S, R) is complemented, the cube condition for u, v, w holds iff
$$(u\backslash v)\backslash(u\backslash w) \equiv_R^+ (v\backslash u)\backslash(v\backslash w).$$

(the cube law)

3. Subword Reversing : Uses

- Cancellativity
- Word problems
- Recognizing Garside structures
- Computing in Garside structures

- **Proposition :** Assume that (S, R) is a complete presentation and R contains no relation $s\ldots = s\ldots$. Then the monoid $\langle S \mid R\rangle^+$ is left-cancellative.

$\uparrow$ $sx = sx'$ implies $x = x'$

- **Proof:** Assume $sw \equiv_R^+ sw'$. (Want to prove $w \equiv_R^+ w'$.)

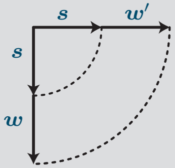
Completeness implies: $(sw)^{-1}(sw') \curvearrowright_R \varepsilon$, *i.e.*,

exists a sequence $w^{-1}s^{-1}sw' \curvearrowright_R^1 \ldots \curvearrowright_R^1 \ldots \curvearrowright_R^1 \varepsilon$.

The first step must be $w^{-1}s^{-1}sw' \curvearrowright_R w^{-1}w'$,

so the sequel must be $w^{-1}w' \curvearrowright_R \varepsilon$,

which implies $w \equiv_R^+ w'$. $\square$



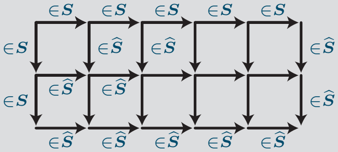
- **Example :** M is left-cancellative —and right-cancellative too by symmetry.

(not visible on the initial presentation; becomes visible after completion only)

- Remark: Applies in particular to every complete complemented presentation.

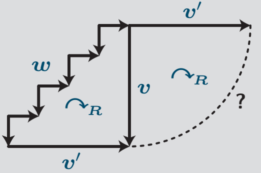
• **Proposition** : Assume that (S, R) is a complete (complemented) presentation and there exists a finite set $\widehat{S} \supseteq S$ satisfying $\forall w, w' \in \widehat{S}\ \exists v, v' \in \widehat{S}\ (w^{-1}w' \curvearrowright_R v'v^{-1})$.
Then the word problem of $\langle S \mid R \rangle^+$ is solvable in exponential (quadratic) time,
and so is that of $\langle S \mid R \rangle$ whenever $\langle S \mid R \rangle^+$ is right-cancellative.

• Proof: Reversing terminates
in exponential (quadratic) time:
construct an $\widehat{S}$-labeled grid



• For w, w' words on S:
$w \equiv_R^+ w'$ iff $w^{-1}w' \curvearrowright_R \varepsilon$.

• For w a word on $S \cup S^{-1}$:
assume $w \curvearrowright_R v'v^{-1}$;
then $w \equiv_R \varepsilon$ iff $v \equiv_R v'$ iff $v \equiv_R^+ v'$
assuming right-cancellativity, hence
iff $v^{-1}v' \curvearrowright_R \varepsilon$ (double reversing). □



• **Example** : Applies to M with $\widehat{S} = \{\varepsilon, a, b, c, d, a^2, ab, ba, b^2\}$.
So M satisfies Ore's conditions, hence embeds in a group of fractions (here B_3).

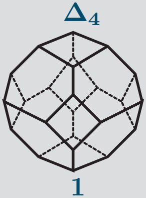
- Definition : A Garside monoid is a pair (M, Δ) such that
  - M is a cancellative monoid admitting lcm's and gcd's, and no nontrivial unit,
  - Δ is a Garside element in M:
    $\mathrm{Div}_L(\Delta) = \mathrm{Div}_R(\Delta)$, this set is finite, and generates M.

- By Ore's conditions, a Garside monoid embeds in a group of fractions.

- Definition : A Garside group is a group that is the group of fractions of (at least one) Garside monoid.

- Principle : A Garside group is controlled by the finite lattice $\mathrm{Div}(\Delta)$.
  (Many generalizations: categories, remove existence of Δ, etc.)

- Example : Artin's braid group B_n (the original example):
  - $B_n = \langle \sigma_1, ..., \sigma_{n-1} \mid \sigma_i\sigma_j = \sigma_j\sigma_i$ for $|i-j| \geqslant 2$,
    $\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$ for $|i-j| = 1\rangle$;
  - Garside structure:
    - monoid: $B_n^+ = \langle ... \rangle^+$,
    - Garside half-turn braid: $\Delta_n = \sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1 ...$;
  - lattice $\mathrm{Div}(\Delta_n) \approx$ (symmetric group $\mathfrak{S}_n$, weak order).



• **Proposition** : Every Garside monoid admits a finite complete complemented presentation.

⇝ Hence: natural to start from such presentations.

• **Question 1** : Starting from a complete complemented presentation (S, R), how to use reversing to recognize whether $\langle S \mid R\rangle^+$ is a Garside monoid?

⇝ Typically: recognize whether least common multiples exist.

• **Proposition** : Assume that (S, R) is a complete complemented presentation. Then two elements of $\langle S \mid R\rangle^+$ that admit a common right-multiple admit a right-lcm.

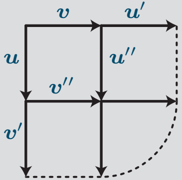
• **Proof** : Assume $uv' \equiv_R^+ vu'$. By completeness, $(uv')^{-1}(vu') \curvearrowright_R \varepsilon$, i.e., $v'^{-1}u^{-1}vu \curvearrowright_R \varepsilon$.

The reversing diagram splits as

This means that $[uv']$ is a right-multiple of $[uv'']$.

The latter only depends on $[u]$ and $[v]$.

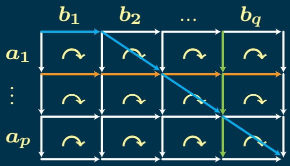
Hence it is a right-lcm of $[u]$ and $[v]$. □



- **Question 2** : Assuming that (S, R) is a complete presentation for a Garside monoid, how to use reversing to investigate that monoid?

- Word problems: one/two reversings.
- Least common multiple: one reversing; Greatest common divisor: three reversings.
- **Greedy normal form**: Every non-trivial element in a Garside monoid admits a unique decomposition $a = a_1 ... a_p$ such that, for each i,
  - a_i belongs to $\mathrm{Div}(\Delta)$, with $a_1 \neq 1$;
  - a_i is the maximal right-divisor of $a_1 ... a_i$ lying in $\mathrm{Div}(\Delta)$.

- **Theorem** : Assume that $(a_1, ..., a_p)$, $(b_1, ..., b_q)$ are normal. Then so is every horizontal-then-diagonal and vertical-then-diagonal sequence in



- Leads to the so-called grid property in Garside groups (≈ CAT(0) geometry).

4. Subword Reversing : Efficiency

- Upper bounds
- Optimality criteria

- Preliminary remark: Subword reversing (viewed as a method for finding derivations between equivalent words) need not be optimal.

  ↑ provide shortest derivation

- **Definition** : For (S, R) (complete), and w, w' (equivalent) words on S,
  - $\mathrm{dist}(w, w') :=$ minimal # of relations needed to go from w to w';
  - $\mathrm{dist}_{\curvearrowright}(w, w') :=$ (minimal) # of non-trivial steps needed to reverse $w^{-1}w'$ into ε.

- **Proposition** : Assume that (S, R) is complete, and there exists a finite set $\widehat{S} \supseteq S$ that is closed under reversing. Then there exists C s.t., for all equivalent w, w',

$$\mathrm{dist}(w, w') \leqslant \mathrm{dist}_{\curvearrowright}(w, w') \leqslant C \cdot |w| \cdot |w'|.$$

- Easy...

  contrary to the next result, which does **not** assume that reversing terminates:

- **Theorem** (D., 2003) : Assume that (S, R) is finite, complemented, complete, and the relations of R preserve the length. Then there exists C—effectively computable from (S, R)—such that, for all equivalent w, w',

$$\mathrm{dist}(w, w') \leqslant \mathrm{dist}_{\curvearrowright}(w, w') \leqslant \mathrm{dist}(w, w') \cdot 2^{2^{C|w|}}.$$

- **Definition** : Artin's **braid monoid** vs. symmetric group:

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

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

- **Proposition** ("Exchange Lemma") : Any two reduced (= of minimal length) expressions of a permutation are connected by braid relations (no need of using $\sigma_i^2 = 1$).

- Combinatorial distance makes sense both for B_n^+ and $\mathfrak{S}_n$:
  dist(w, w') = minimal # of braid relations needed to transform w into w'
  both for w, w' positive braid words and for w, w' reduced expressions.

- **Proposition** : There exist positive constants C, C' s.t.
  - dist$(u, v) \leqslant Cn^4$ for all f in $\mathfrak{S}_n$ and all reduced expressions u, v of f,
  - dist$(u, v) \geqslant C'n^4$ for some f in $\mathfrak{S}_n$ and some reduced expressions u, v of f.

- **Aim** : Recognize whether a given reversing diagram (= reversing sequence) (or, more generally, a Van Kampen diagram) is possibly optimal.

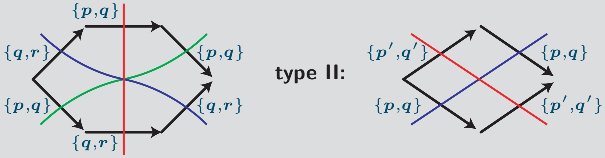
↑

non-trivial faces = combinatorial distance between the bounding words

- Use the names of the elements (or braid strands) that cross (*i.e.*, use a "position vs. name" duality), then connect the edges with the same name:

type I:

type II:

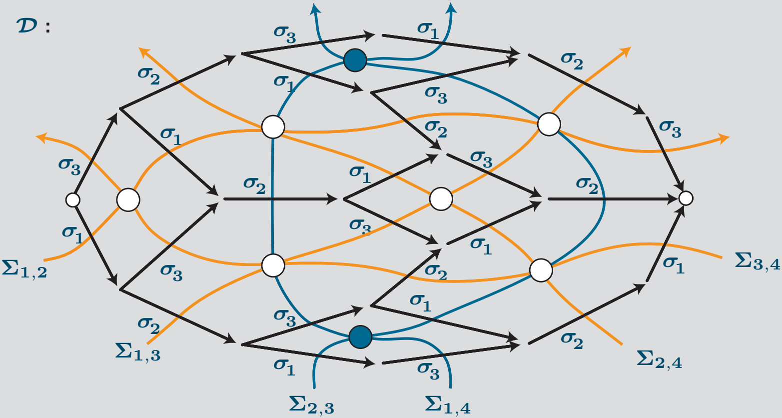


⇝ for each pair $\{p, q\}$, an (oriented) curve that connect all $\{p, q\}$-edges: the $\{p, q\}$-separatrix $\Sigma_{p,q}$.

- **Lemma** : A sufficient condition for a van Kampen diagram $\mathcal{D}$ to be optimal is that any two separatrices cross at most once in $\mathcal{D}$.

- **Example** : $w = \sigma_3\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3$, $w' = \sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$.

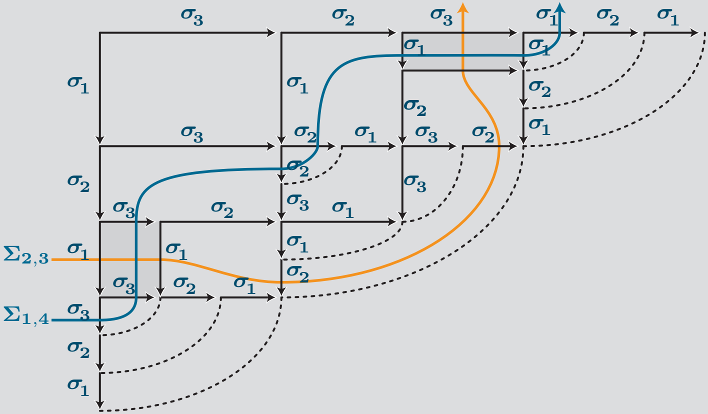
$\mathcal{D}$:



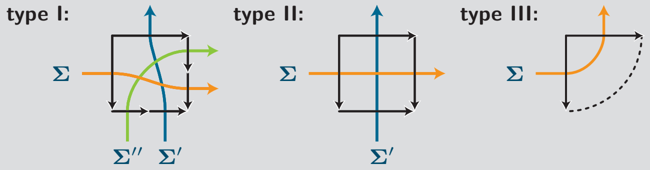
⇝ The separatrices $\Sigma_{2,3}$ and $\Sigma_{1,4}$ cross twice, hence $\mathcal{D}$ is not optimal.

- **Applies in particular to reversing diagrams**

  (viewed as particular van Kampen diagrams):



- How are separatrices in a reversing diagram? Three types of faces:



- **Proposition** : A reversing diagram containing no type III face is optimal.

- Proof: For two separatrices to cross twice, must go from horizontal to vertical. □

⇝ Note the importance of metric vs. topological features here.

- **Corollary** (Autord, D.): For each ℓ, there exist length ℓ braid words w, w' satisfying $w^{-1}w' \curvearrowright_R v'v^{-1}$ and $\mathrm{dist}(wv', w'v) \geqslant \ell^4/8$.

- By contrast: for fixed n, Garside's theory gives an upper bound in $O(\ell^2)$.

- **Conclusion** : In good cases (= when it is complete), subword reversing is useful
  - for proving cancellativity,
  - for solving word problems (both for monoids and for groups),
  - for recognizing Garside structures,
  - for computing in Garside structures (normal form, homology, ...),
  - for getting optimal derivations,
  - hopefully more...

- **Attention** ! Once completeness is granted, using words and reversing is essentially equivalent to using elements of the monoid and common multiples,

  but, before completeness is established, it is crucial to distinguish between words and the elements they represent: reversing equivalent words need not lead to equivalent results.

Reversing is really an operation on **words**.

- P. Dehornoy, Deux propriétés des groupes de tresses
C. R. Acad. Sci. Paris 315 (1992) 633–638.
- F.A. Garside, The braid group and other groups
Quart. J. Math. Oxford 20-78 (1969) 235–254.
- K. Tatsuoka, An isoperimetric inequality for Artin groups of finite type
Trans. Amer. Math. Soc. 339–2 (1993) 537–551.
- R. Corran, A normal form for a class of monoids including the singular braid monoids J. Algebra 223 (2000) 256–282.
- P. Dehornoy, Complete positive group presentations;
J. Algebra 268 (2003) 156–197.
- P. Dehornoy & Y. Lafont, Homology of Gaussian groups
Ann. Inst. Fourier 53-2 (2003) 1001–1052.
- P. Dehornoy & B. Wiest, On word reversing in braid groups
Int. J. for Algebra and Comput. 16-5 (2006) 941–957.
- M. Autord & P. Dehornoy, On the combinatorial distance between expressions of a permutation arXiv: math.CO/0902.3074

www.math.unicaen.fr/∼dehornoy