The Subword Reversing Method

Patrick Dehornoy

Laboratoire de Mathématiques
Nicolas Oresme, Université de Caen

- A strategy for constructing van Kampen diagrams for semigroups, with an application to the combinatorial distance between the reduced expressions of a permutation.

Plan :

- The general case:
  - Subword reversing as a strategy for constructing van Kampen diagrams
  - Subword reversing as a syntactic transformation
  - A cancellativity criterion
- The case of permutations:
  - bounds for the combinatorial distance between reduced expressions of a permutation
  - recognizing the optimality of a van Kampen diagram

all relations of the form $\mathrm{u} = \mathrm{v}$ with u, v nonempty words on S

↓

- **Let (S, R) be a semigroup presentation. Then 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, ?): If (S, R) is 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 a van Kampen diagram for $(\mathrm{w}, \mathrm{w}')$.**

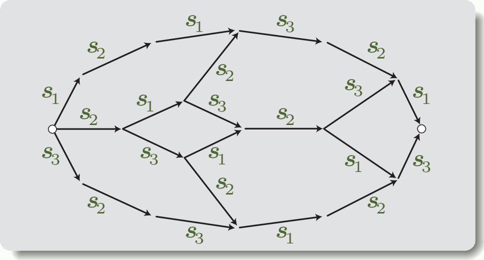
↑

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

- **Example:** Let $B_n^+ = \left\langle s_1, \ldots, s_{n-1} \;\middle|\; \begin{array}{ll} s_i s_j s_i = s_j s_i s_j & \text{for } |i-j| = 1 \\ s_i s_j = s_j s_i & \text{for } |i-j| \geqslant 2 \end{array} \right\rangle^+$

(the n-strand Artin braid monoid).

Then



is a van Kampen diagram for $(s_1 s_2 s_1 s_3 s_2 s_1, s_3 s_2 s_3 s_1 s_2 s_3)$.

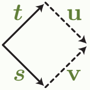
- **How to build a van Kampen diagram (when it exists)?**

  ↑

  $\cong$ solve the word problem: decide $\mathrm{w} \equiv_R^+ \mathrm{w}'$

- **Subword reversing = the left strategy: starting with two words w, w',**

  - look at the leftmost pending pattern 

  - choose a relation $s\mathrm{v} = t\mathrm{u}$ of R to close it into 

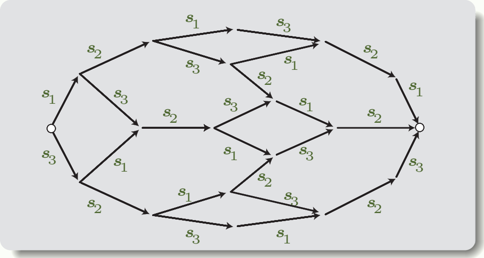
, and repeat.

- **Facts:** - May not be possible (no relation $s... = t...$);
  - May not be unique (several relations $s... = t...$);
  - May never terminate (when 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).

• At least: deterministic whenever R is a complemented presentation: for each pair of letters s, t in S, there is exactly one relation $s... = t...$ in R.

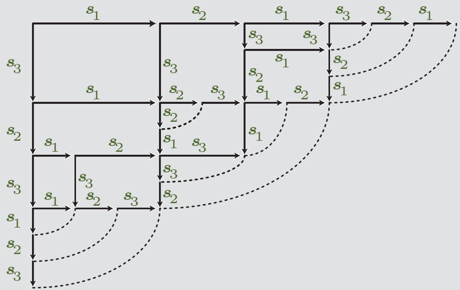
• Example: Let $B_n^+ = \left\langle s_1, ..., s_{n-1} \;\middle|\; \begin{array}{ll} s_i s_j s_i = s_j s_i s_j & \text{for } |i-j| = 1 \\ s_i s_j = s_j s_i & \text{for } |i-j| \geqslant 2 \end{array} \right\rangle^+$.

Applying the reversing strategy to $s_1 s_2 s_1 s_3 s_2 s_1$ and $s_3 s_2 s_3 s_1 s_2 s_3$:



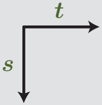
So, on this particular example, the reversing strategy works.

- **Another way of drawing the same diagram:**

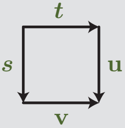


⇝ **only vertical and horizontal edges,**
plus dotted arcs connecting vertices that are to be identified
in order to get an actual van Kampen diagram.

- **In this way, a uniform pattern:**

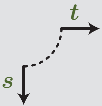


becomes

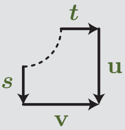


for $s\mathrm{v} = t\mathrm{u}$ **in** R

- **More exactly:**

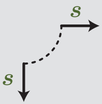


becomes

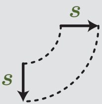


for $s\mathrm{v} = t\mathrm{u}$ **in** R

including



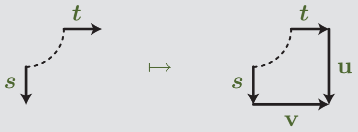
becomes



.

- Introduce two types of letters:
  - S for horizontal edges, S^{-1} for vertical edges;
  - read words the Mull of Kintyre to the Pentland Fifth (SW to NE).

- Basic step:



reads: $s^{-1}t \mapsto \mathrm{vu}^{-1}$,

including

reads: $s^{-1}s \mapsto \varepsilon$.

↑ the empty word

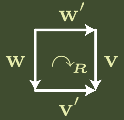
- Syntactically, "subword reversing": replacing $-+$ with $+-$.

- **Definition:** For w, w' words on $S \cup S^{-1}$, declare $\mathrm{w} \curvearrowright_R^{(1)} \mathrm{w}'$ if
  $\exists s, t, \mathrm{u}, \mathrm{v}$ ($s\mathrm{v} = t\mathrm{u}$ lies in R and $\mathrm{w} = \ldots s^{-1}t \ldots$ and $\mathrm{w}' = \ldots \mathrm{v}\mathrm{u}^{-1} \ldots$).

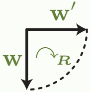
Declare $\mathrm{w} \curvearrowright_R \mathrm{w}'$ if there exist $\mathrm{w}_0, \ldots, \mathrm{w}_p$ s.t.
$\mathrm{w}_0 = \mathrm{w}$, $\mathrm{w}_p = \mathrm{w}'$, and $\mathrm{w}_i \curvearrowright_R^{(1)} \mathrm{w}_{i+1}$ for each i.

- Terminal words: $\mathrm{w}'\mathrm{w}^{-1}$ with w, w' words on S (no letter s^{-1}).

- **Lemma**: If $\mathrm{w}, \mathrm{w}', \mathrm{v}, \mathrm{v}'$ are words on S and $\mathrm{w}^{-1}\mathrm{w}' \curvearrowright_R \mathrm{v}'\mathrm{v}^{-1}$,

  i.e., 

, then $\mathrm{w}\mathrm{v}' \equiv_R^+ \mathrm{w}'\mathrm{v}$.

- In particular, if $\mathrm{w}^{-1}\mathrm{w}' \curvearrowright_R \varepsilon$, *i.e.*, if 

, then $\mathrm{w} \equiv_R^+ \mathrm{w}'$.

  ↑ the empty word

- Conversely, does $\mathrm{w} \equiv_R^+ \mathrm{w}'$ implies $\mathrm{w}^{-1}\mathrm{w}' \curvearrowright_R \varepsilon$?

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

↑

hence ... is equivalent to ...

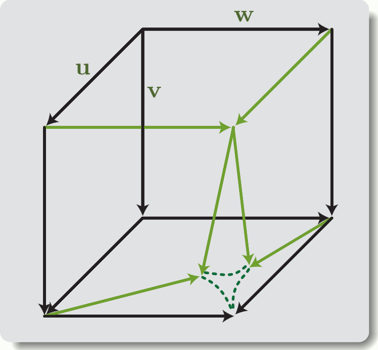
- Remark: Completeness implies the solvability of the word problem only if one knows that reversing always terminates.

- Two questions:
  - How to recognize completeness?
  - What to do with a complete presentation?

• **Theorem:** (D., '97) Assume that (S, R) is a homogeneous complemented 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 $\boldsymbol{\lambda} : S^* \to \mathbb{N}$ $(\boldsymbol{\lambda}(s\mathrm{w}) > \boldsymbol{\lambda}(\mathrm{w}))$.

• cube condition for a triple
of positive words $\mathrm{u}, \mathrm{v}, \mathrm{w}$:

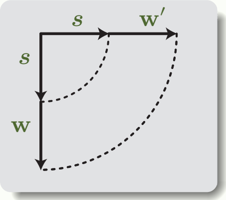


...hence checkable (for one triple)

• **Proposition:** Assume that (S, R) is a complete complemented presentation. Then the monoid $\langle S \mid R \rangle^+$ is left-cancellative.

↑ $sa = sa'$ implies $a = a'$

• **Proof:** Assume $s\mathrm{w} \equiv_R^+ s\mathrm{w}'$. Want to prove $\mathrm{w} \equiv_R^+ \mathrm{w}'$.
Completeness implies: $(s\mathrm{w})^{-1}(s\mathrm{w}') \curvearrowright_R \varepsilon$, *i.e.*, $\mathrm{w}^{-1}s^{-1}s\mathrm{w}' \curvearrowright_R \varepsilon$.



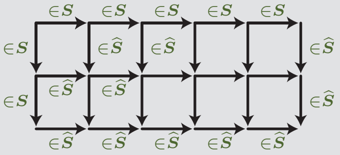
The first step must be $\mathrm{w}^{-1}s^{-1}s\mathrm{w}' \curvearrowright_R \mathrm{w}^{-1}\mathrm{w}'$,
so the sequel must be $\mathrm{w}^{-1}\mathrm{w}' \curvearrowright_R \varepsilon$, hence $\mathrm{w} \equiv_R^+ \mathrm{w}'$. □

• **Proposition:** Assume that (S, R) is a complete complemented presentation and there exists a finite set $\widehat{S}$ including S and closed under reversing. Then the word problem of $\langle S \mid R\rangle^+$ is solvable in quadratic time, and so is that of $\langle S \mid R\rangle$ if $\langle S \mid R\rangle^+$ is right-cancellative.

↑

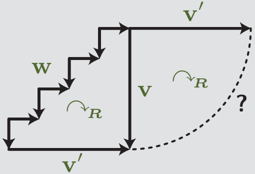
$\forall \mathrm{w},\mathrm{w}'\in\widehat{S}\ \exists \mathrm{v},\mathrm{v}'\in\widehat{S}\ (\mathrm{w}^{-1}\mathrm{w}' \curvearrowright_R \mathrm{v}'\mathrm{v}^{-1})$

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



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

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



Range

- For semigroups: in principle, all are eligible: completion procedure (when the cube condition fails).
- For groups: unknown; at least: classical and dual presentations of (generalized) braid groups (and all Garside groups) —but certainly more.

Uses

- Cancellativity criterion;
- Existence of least common multiples, identification of Garside structures;
- Computation of the greedy normal form;
- (with Y. Lafont) Construction of explicit resolutions (whence homology);
- (with B. Wiest) Solution to the word problem (complexity issues);
- (with M. Autord) Combinatorial distance between the reduced expressions of a permutation.

- Every permutation of $\{1, \ldots, n\}$ is a product of transpositions:

$$\mathfrak{S}_n = \left\langle s_1, \ldots, s_{n-1} \;\middle|\; \begin{array}{ll} s_i s_j s_i = s_j s_i s_j & \text{for } |i-j| = 1 \\ s_i s_j = s_j s_i & \text{for } |i-j| \geqslant 2 \end{array}, s_1^2 = \ldots = s_{n-1}^2 = 1 \right\rangle.$$

of minimal length
↓

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

- **Combinatorial distance**: $d(\mathrm{u}, \mathrm{v})$ = minimal number of braid relations needed to transform u into v.

- Question: Bounds on $d(\mathrm{u}, \mathrm{v})$? (The standard proof of the Exchange Lemma gives an exponential upper bound.)

- **Proposition** (folklore ?): There exist positive constants C, C' s.t.
  - $d(\mathrm{u}, \mathrm{v}) \leqslant C n^4$ holds for every permutation f of $\{1, \ldots, n\}$ and all reduced expressions u, v of f,
  - $d(\mathrm{u}, \mathrm{v}) \geqslant C' n^4$ holds for some permutation f of $\{1, \ldots, n\}$ and some reduced expressions u, v of f.

- Here: lower bounds; more specifically:

- **Aim**: Recognize whether a given Van Kampen diagram or reversing diagram is possibly optimal.

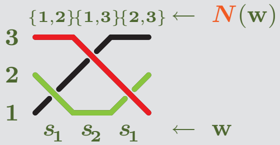
↑

\# faces = combinatorial distance between the bounding words

- Associate a braid diagram with every (reduced) s-word and use the names (or the colors) of the strands that cross

(*i.e.*, use a "position vs. name" duality):

$s_1 s_2 s_1 \quad \mapsto$



$\rightsquigarrow$ a sequence $N(\mathrm{w})$ of pairs of integers in $\{1, ..., n\}$.

- For S, S' sequences of pairs of integers in $\{1, ..., n\}$:
  - $I_3(S, S') = \#$ triples $\{p, q, r\}$ s.t. $\{p, q\}$, $\{p, r\}$ and $\{q, r\}$ appear in different orders in S, S'.
  - $I_{2,2}(S, S') = \#$ pairs of pairs $\{\{p, q\}, \{p', q'\}\}$ s.t. $\{p, q\}$ and $\{p', q'\}$ appear in different orders in S, S'.

- **Lemma**: If w, w' are two reduced expressions of some permutation, then
$$d(\mathrm{w}, \mathrm{w}') \geqslant I_3(N(\mathrm{w}), N(\mathrm{w}')) + I_{2,2}(N(\mathrm{w}), N(\mathrm{w}')).$$

- Proof: Each type I braid relation ("hexagon") contributes at most 1 to I_3, each type II braid relation ("square") contributes at most 1 to $I_{2,2}$. □

- Example: $\mathrm{w} = s_1 s_2 s_1 s_3 s_2 s_1$, $\mathrm{w}' = s_3 s_2 s_3 s_1 s_2 s_3$.

  Then $N(\mathrm{w}) = (\{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 4\}, \{2, 4\}, \{3, 4\})$,
  $N(\mathrm{w}') = (\{3, 4\}, \{2, 4\}, \{2, 3\}, \{1, 4\}, \{1, 3\}, \{1, 2\})$.

  Hence $d(\mathrm{w}, \mathrm{w}') \geqslant 4 + 2 = 6$.

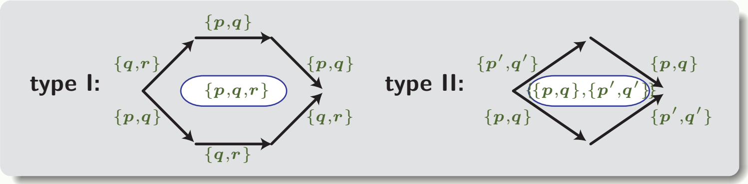
- Question (Conjecture?): Is the above inequality an equality?

- **Back to van Kampen diagrams with the aim of recognizing optimality.**

↑

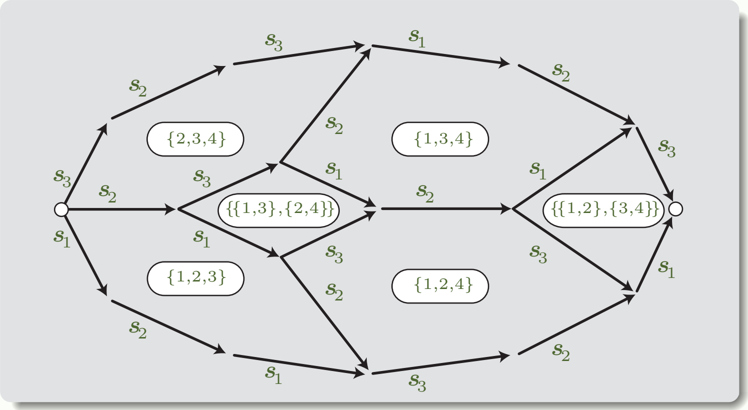
$\#$ faces $=$ combinatorial distance between bounding words

- **Having given names to the generators s_i (= the edges of the diagram), give names to the faces:**



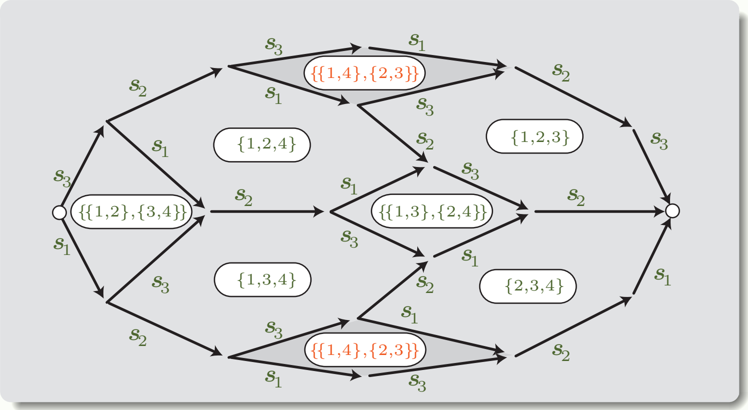
- **Criterion 1: A van Kampen diagram in which different faces have different names is optimal.**

- **Example:**

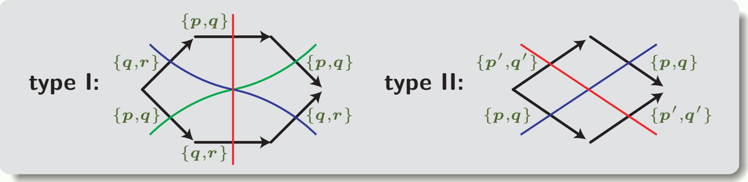


s3
s1
s2
s2
{2,3,4}
s2
{1,3,4}
s3
s3
s1
s1
s3
s2
s2
{{1,3},{2,4}}
{{1,2},{3,4}}
s1
s1
s3
s3
s1
{1,2,3}
s2
{1,2,4}
s2
s2
s1
s3

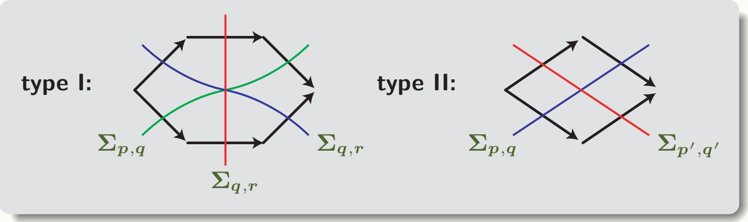
- **Example:**



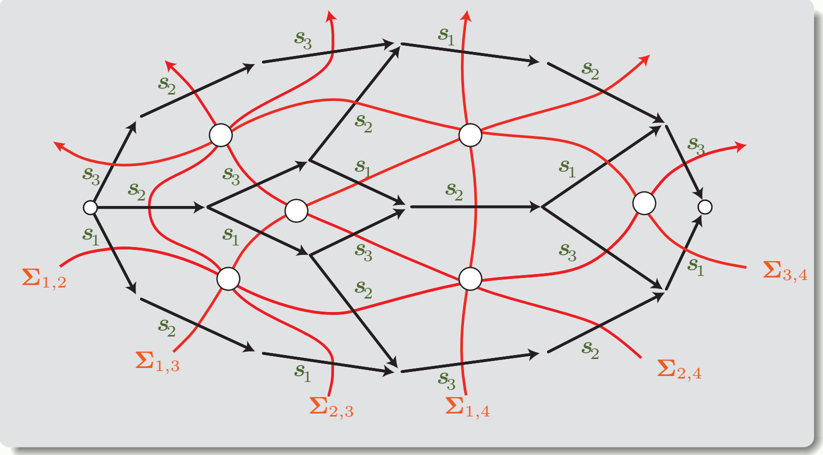
- (Again in a van Kampen diagram) connect the edges with the same name:



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

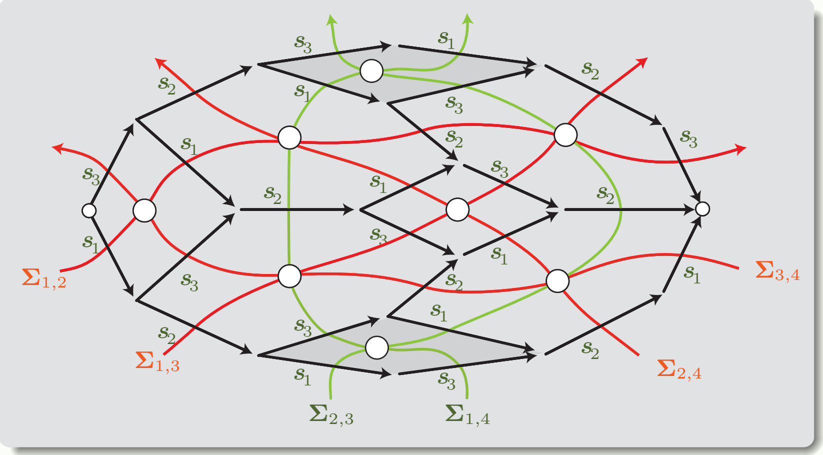


- **Example:**



s_3
s_1
s_2
s_2
s_2
s_3
s_3
s_1
s_1
s_3
s_2
s_2
s_1
s_3
s_1
s_1
s_3
s_3
s_1
s_2
s_2
s_2
s_1
s_3
s_2
$\Sigma_{1,2}$
$\Sigma_{1,3}$
$\Sigma_{2,3}$
$\Sigma_{1,4}$
$\Sigma_{2,4}$
$\Sigma_{3,4}$

- **Example:**



s_3
s_1
s_2
s_1
s_3
s_2
s_1
s_2
s_3
s_3
s_2
s_3
s_1
s_2
s_2
s_1
s_3
s_1
$\Sigma_{1,2}$
s_3
s_2
s_1
$\Sigma_{3,4}$
s_3
s_1
s_2
s_2
$\Sigma_{1,3}$
s_1
s_3
$\Sigma_{2,4}$
$\Sigma_{2,3}$
$\Sigma_{1,4}$

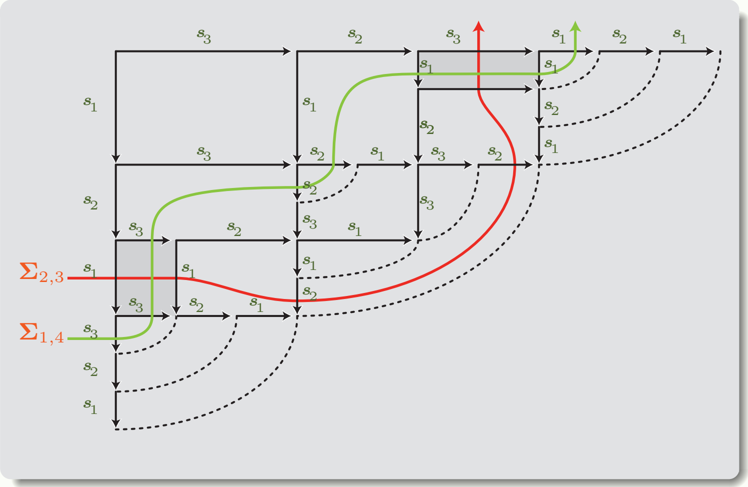
- **Criterion 2**: A van Kampen diagram in which any two separatrices cross at most once is optimal.

- Question: Is the condition necessary, *i.e.*, do any two separatrices cross at most once in an optimal van Kampen diagram?

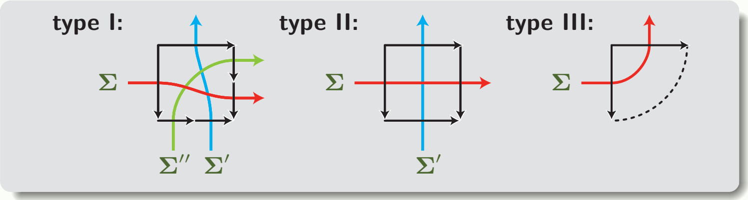
- Remark: Compare with "a s-word is reduced iff any two strands in the associated braid diagram cross at most one".

- **Applies in particular to reversing diagrams**

  (viewed as particular van Kampen diagrams):



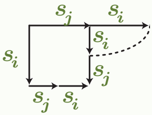
- How are separatrices in a reversing diagram? Three types of faces:

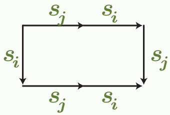


- **Criterion 3: A reversing diagram containing no type III face is optimal.**

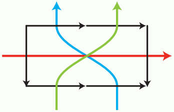
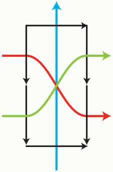
- Proof: In order that two separatrices cross twice, one has to go from horizontal to vertical. □

- **An improvement: Same argument when reversing steps are grouped:**

replace 

with 

for $|i-j|=1$,

corresponding to  and  .

- **An application:**

> • **Proposition**: For each ℓ, there exist length ℓ reduced s-words w, w' satisfying $\mathrm{w}^{-1}\mathrm{w}' \curvearrowright_R \mathrm{v}'\mathrm{v}^{-1}$ and $d(\mathrm{w}\mathrm{v}', \mathrm{w}'\mathrm{v}) \geqslant \ell^4/8$.

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

- Two conclusions:

- Even in the simple(?) case of braids and permutations, many open questions.
- Importance of having van Kampen diagrams included in a grid.

• 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.

• P. Dehornoy & M. Autord, On the combinatorial distance between expressions of a permutation
in preparation.

www.math.unicaen.fr/∼dehornoy