Course notes on Braids

The purpose of these notes is to provide an example (braids) of an orthogonal rewrite system which is completely distinct from orthogonal term rewriting systems.

We study an equational system for *braids* [Art26]. Firstly, we present in Section 1, an informal specification which is subsequently formalised in Section 2 by means of an equational specification $\langle \Sigma, E \rangle$. Whether two braids $\mathbf{U}$ and $\mathbf{V}$ are equivalent, is an instance of the *uniform word problem* for this equational specification:

$$\mathbf{U} =_E \mathbf{V} \quad ?$$

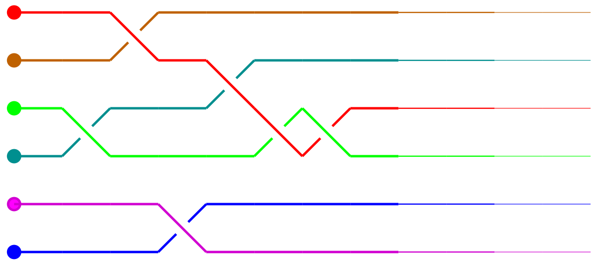
This problem is dealt with in Section 5. The problem whether two braids $\mathbf{U}$, $\mathbf{V}$ can be 'extended' by braids $\mathbf{U}'$, $\mathbf{V}'$ such that they become equivalent:

$$\exists \mathbf{U}', \mathbf{V}' \quad \mathbf{U}\mathbf{U}' =_E \mathbf{V}\mathbf{V}' \quad ?$$

is an instance of the *unification* problem up to an equational theory. This latter problem and its solution by means of rewriting techniques are extensively discussed in Section 3.

1 Informal Specification[1]

This is a braid:[2]



The braid consists of 6 *strands* which are braided. The strands start on the left and extend to the right (infinitely long and straight). If two strands cross ($\times$), then the top one crosses over the bottom one. This we call a *crossing*. Doing this with real strands makes clear that some braids can be transformed into one another. That is, keeping the (eventual) end-point of the strands fixed, one can be obtained from the other by manipulating the strands.[3] Two simple cases are presented in Figure 1, where the arrows indicate how to manipulate the strands to transform the left-hand braid into the right-hand braid and vice versa.

[1]This section is based on [KV].

[2]Like for knots, we will concentrate on a two-dimensional representation for three-dimensional braids [Art47].

[3]Such braids are said to be *isotopic* [Art47].

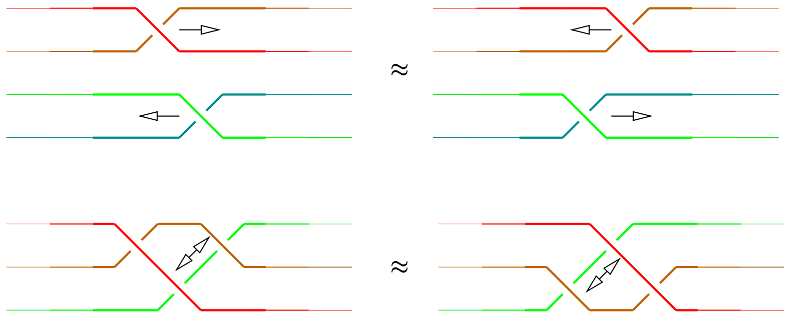
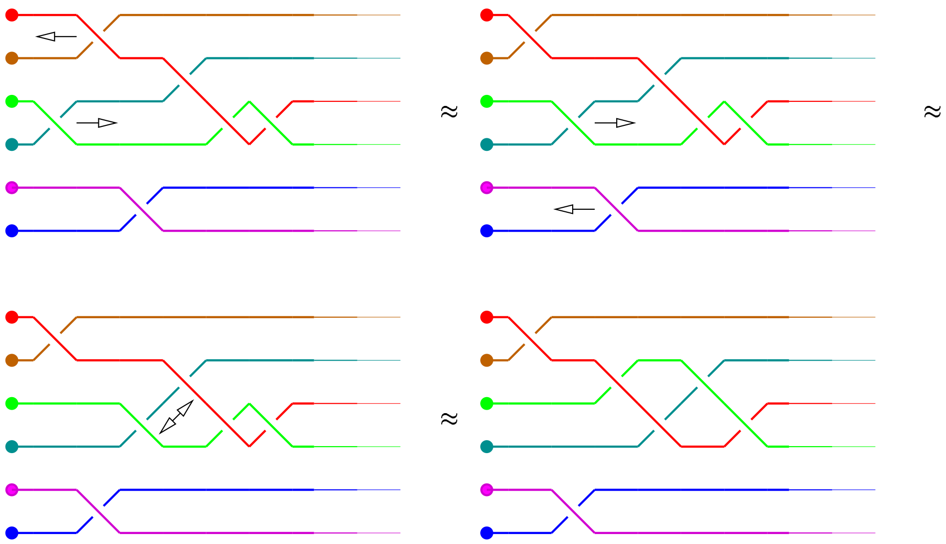


Figure 1: Transformaties op vlechten

Exercise 1 *Execute the transformations in Figure 1 on real strands (e.g. strands of hair). For the first equivalence at least four and for the second equivalence at least three strands are required.*

Two braids are said to be *equivalent* if they can be transformed into each other.

Example 2 *Using the transformations in Figure 1, which of course can be applied anywhere in a braid, we can transform our example braid as follows (into an equivalent one):*

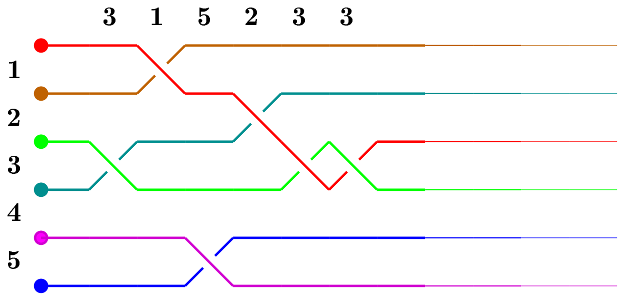


The arrows indicate how a braid is transformed into its successor.

How can we determine whether two braids are equivalent?[4] The first step to be taken is to formalise the intuitive notions of braid and equivalence. In the most natural formalisation strands are represented as certain (continuous) curves in $\mathbb{R}^3$ [Art47]. However, as shown in [Art26, Boh47], it suffices to find a suitable (discrete) representation of sequences of crossings and transformations on those, as shown in Figure 1. This will be the topic of the next section.

2 Equational Specification

Consider a braid consisting of $n+1$ strands. The gaps between successive strands can be numbered from 1 to n, like in the braid:



Then, the braid itself can be represented by listing the (numbers of the gaps of the) crossings from left to right. The braid in the example is represented by 315233. Representing the transformations in Figure 1 in this way gives rise to the transformations in Figure 2.

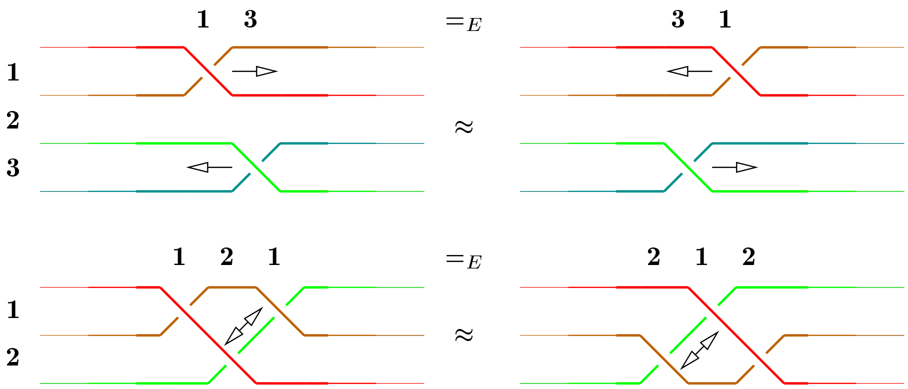
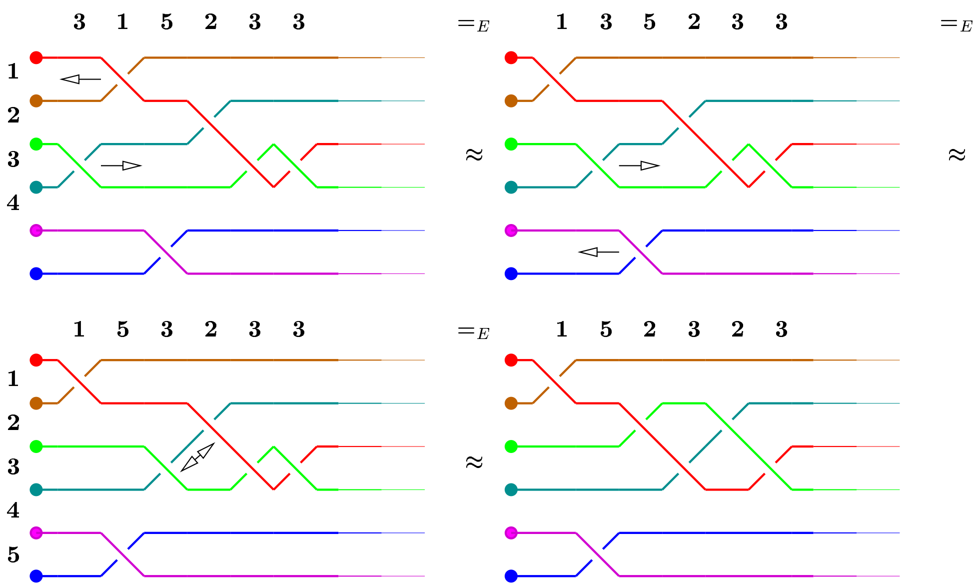


Figure 2: Transformations on braidrepresentations

[4] Cf. the same questions for knots.

Example 3 *Providing the transformations in Example 2 with their representations results in*



Forgetting about the two-dimensional representation, we get:

$$\mathbf{\underline{31}5233} =_E \mathbf{1\underline{35}233} =_E \mathbf{15\underline{3233}} =_E \mathbf{152323}$$

where the underlinings indicate how a braid is transformed into its successor.

Hopefully the above is clear enough to make the following definition understandable.

Definition 4 *For every natural number $n \in \mathbb{N}$, $\langle \Sigma, E \rangle$ is the equational specification (cf. [DII, Completion of equational specifications]) of* braids with n strands.

- Σ *is an alphabet consisting of unary symbols* $\mathbf{i}$*, the* crossings*, for every* $1 \le i < n$*, and a constant (nullary function symbol)* o*.* Braids *are closed* Σ*-terms. We use* $\mathbf{U}$, $\mathbf{V}$, $\mathbf{W}$, $\ldots$ *to range over braids.*
- E *is a set of schemata consisting of*

  1.

  $$\mathbf{i}(\mathbf{j}(\mathbf{i}(x))) = \mathbf{j}(\mathbf{i}(\mathbf{j}(x)))$$

  for every $1 \le i, j < n$ *such that* $|i - j| = 1$ *(the crossings apply to three successive strands in the braid), and*

2.

$$\mathbf{i}(\mathbf{j}(x)) = \mathbf{j}(\mathbf{i}(x))$$

for all $1 \leq i, j < n$ *such that* $|i - j| \geq 2$ *(the crossings apply to four pairwise distinct strands).*[5]

Note that we have presented an equational specification for 'strings' (cf. [DI, Sectie 2.7]. In the sequel we will employ the standardnotation for these (we've already done so in Example 3). In particular, instead of $\mathbf{1}(\mathbf{2}(\mathbf{3}(o)))$ we just write **123**. A braid which doesn't contain any crossings is denoted by the empty string o. The *concatenation* $\mathbf{UV}$ of braids $\mathbf{U} = \mathbf{i}_1(\ldots(\mathbf{i}_k(o))\ldots)$ and $\mathbf{V}$ is defined by $\mathbf{i}_1(\ldots(\mathbf{i}_k(\mathbf{V}))\ldots)$.

Exercise 5 *1. Show that equivalent braids have the same depth (cf. [DI, Definition 2.1.5]).*

2. Show that the concatenation of two braids is a braid.

3. Demonstrate: $\mathbf{U} =_E \mathbf{V}$ *en* $\mathbf{U}' =_E \mathbf{V}'$ *implies* $\mathbf{UU}' =_E \mathbf{VV}'$.

After formalising we will now try to solve the problems mentioned in the introduction.

3 Unification

The unification problem for braids is described in an antropomorphical way in [SS91, pp. 132-134]. A girl has two braids, each consisting of six strands (see Figure 3). Her father starts braiding the left braid, and her mother starts braiding the right braid. After some crossings they arrive at the situation in the figure and notice that the left and right braid are different. Of course, they want their daughter to have identical braids[6], but how to achieve this?[7] Using the formalisation of braids the parents' question can be rephrased as

$$\exists \mathbf{U}, \mathbf{V} \quad \mathbf{315233U} = \mathbf{42531V} \quad ?$$

We will use some variations on well-known rewriting techniques to solve this problem. First we define a TRS such that performing a rewrite step corresponds to the application of a crossing.

Definition 6 *1. Consider the TRS* $\langle \Sigma, R \rangle$*, where* R *consists of the rules:*

$$o \to \mathbf{i}(o)$$

for every $1 \leq i < n$.

[5] This schema is called *syntactic isotopy* in [Laf].

[6] Symmetric braids would be nice as well, but wouldn't change the problem. (Why?)

[7] Note that only one way of crossing strands is allowed, hence the parents cannot 'undo' what they have done. (Undoing corresponds to an equivalence on knots. Which one?

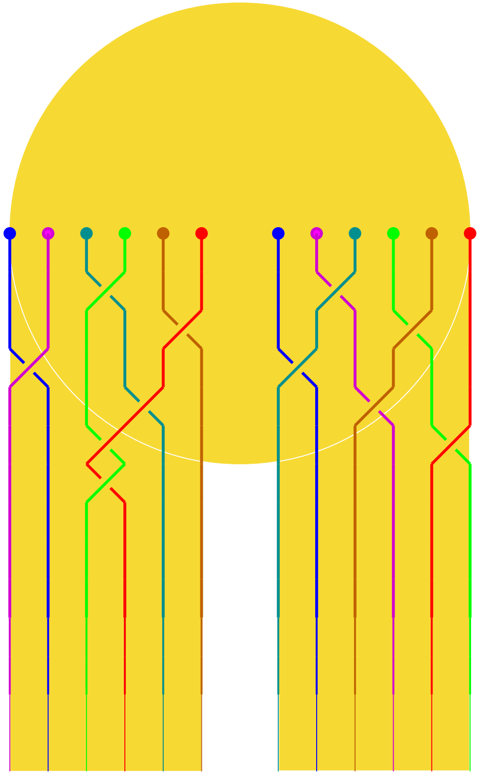


Figure 3: Girl (m/f) with two braids

2. *The rewrite relation of the ARS* $\langle \mathrm{Ter}(\Sigma)/E, \to\rangle$ *is defined by*

$$\mathbf{U} \to \mathbf{V} \iff \exists \mathbf{U}', \mathbf{V}' \quad \mathbf{U} =_E \mathbf{U}' \to_R \mathbf{V}' =_E \mathbf{V}$$

The objects of the ARS are equivalenceclasses of braids which can be transformed into each other. The question of the parents can now be rephrased again as: Is $\to$ confluent?

Exercise 7 1. *Show that* $\mathbf{U} \twoheadrightarrow_R \mathbf{UV}$ *for arbitrary braids* $\mathbf{U}$ *and* $\mathbf{V}$*.*

2. *Show that if* $\mathbf{U}' =_E \mathbf{U}$*,* $\mathbf{U} \to \mathbf{V}$*, and* $\mathbf{V} =_E \mathbf{V}'$*, then* $\mathbf{U}' \to \mathbf{V}'$*.*

3. *Check that the parents' problem is indeed equivalent to the confluence problem for* $\to$*.*

Local confluence (WCR) is a necessary condition for confluence of ARSs. Figure 4 shows that braiding is indeed locally confluent. We call the corresponding diagrams as shown in Figure 4 *elementary diagrams*. (In a diagram a dashed line indicates an empty rewrite sequence.)

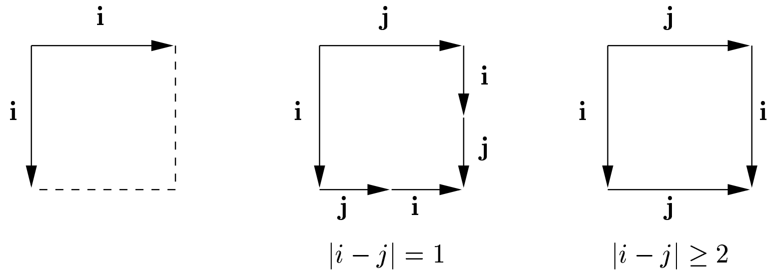


Figure 4: Elementary diagrams ($1 \leq i, j < n$)

Note that in the elementary diagram in the middle, several rewrite steps (both on the right and on the bottom 2 steps) are required to reach a common reduct (**iji** $=_E$ **jij**). Because of this confluence does *not* follow directly from local confluence; one could imagine that tiling the plane with elementary diagrams can go on forever (cf. [DII, Figures 4.3,4,4]). Hence, it is a priori not clear whether the ARS $\rightarrow$ is confluent or not,[8] and a more detailed analysis is called for.

Exercise 8 *1. Check that the elementary diagrams in Figure 4 are indeed confluent. (What do you have to check?)*

2. Show that $\rightarrow$ *is confluent for* $0 \leq n \leq 2$.

3.1 Confluence by Completion (a few strands)[9]

Consider a braid consisting of a few (three or four) strands.

Example 9 *For the braids* **1112** *and* **2221** *a common reduct can be found by tiling with the the elementary diagrams in Figure 4, as is shown in Figure 5. The top side of that figure is formed by the rewrite sequence* **1112** *and the left side by* **2221**.

We observe that although the elementary diagrams in Figure 4 could in principle give rise to an 'infinite descend', it doesn't in reality, at least not in the reality of Figure 5. Looking for example at the 3^{th} column, the diagrams become smaller toward the bottom but this is 'compensated for' by a growing number of empty steps. In preparation for the general proof of confluence for braiding, we first show this for braids having three strands.

Lemma 10 $\rightarrow$ *is confluent for braids consisting of three strands.*

[8]None of the standard confluence techniques (decreasing diagrams fails, why?) for ARSs seems to apply.

[9]This subsection is based on [Zan95].

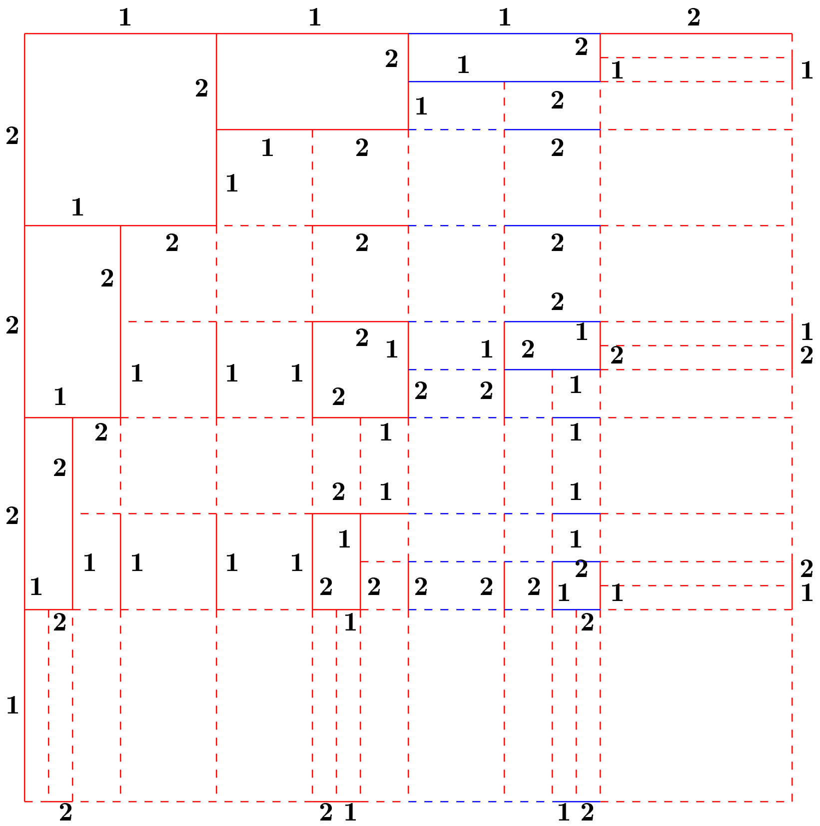


Figure 5: Canonical tiling for the braids **1112** and **2221**

Proof Extend R by the rules:

$$
\begin{array}{lcl}
o & \to & \mathbf{1}(\mathbf{2}(o)) \\
o & \to & \mathbf{2}(\mathbf{1}(o))
\end{array}
$$

The rewrite relation of the ARS corresponding to these rules (obtained in the same way $\to$ was obtained) is denoted by $\multimap\!\!\to$.

1. Since we have $o \to_R \mathbf{1}(o) \to_R \mathbf{1}(\mathbf{2}(o))$ and $o \to_R \mathbf{2}(o) \to_R \mathbf{2}(\mathbf{1}(o))$, confluence of $\to$ is equivalent to confluence of $\multimap\!\!\to$.

2. It is easily checked that all 'critical pairs' of $\multimap\!\!\to$ are convergent *in at most one step*. Stated differently, $\multimap\!\!\to$ is subcommutative ($\mathrm{CR}^{\leq 1}$) hence confluent [DI, Theorem 1.1.8.(iv)].

Confluence of $\to$ follows by combining both parts. □

The general proof idea is starting from R to adjoin rules to the ARS, until all 'critical pairs' converge in *in at most one step*, and confluence follows. With an ugly word one could call this a 'subcommufication', since like in Knuth-Bendix completion rules are adjoined to the original rewrite system (without changing the equational theory) until the rewrite system satisfies some property. Subcommutativity in case of subcommufication and completeness in case of completion. Like completion, commufication may fail to terminate (can it also fail?).

Exercise 11 *1. Does it make sense to try Knuth-Bendix completion here?*

2. Explain what happens if a locally confluent and terminating TRS is completed.

3. Explain how the standard proof of confluence for orthogonal TRSs can be viewed upon as being obtained by subcommufication.

In case $n = 3$ subcommufication stops after having adjoined two rules, as shown in the proof of Lemma 10. For small n it is easy to check by computer that subcommufication stops.[10] In the following (extended) example subcommufication is carried out for braids having four strands.

Example 12 *The TRS for braids with four strands, initially has three rules:*

$$\begin{array}{lcl} o & \to & \mathbf{1}(o) \\ o & \to & \mathbf{2}(o) \\ o & \to & \mathbf{3}(o) \end{array}$$

Since all left-hand sides of the (generated) rules have form o, rules can be denoted just by the string representation of their right-hand sides:

$$\mathbf{1}, \mathbf{2}, \mathbf{3}$$

1. *In the first iteration of the subcommufication process three critical pairs are generated (up to symmetry and trivial critical pairs): $\langle \mathbf{1}, \mathbf{2} \rangle, \langle \mathbf{2}, \mathbf{3} \rangle, \langle \mathbf{3}, \mathbf{1} \rangle$. The pair $\langle \mathbf{1}, \mathbf{2} \rangle$ can be turned into an elementary diagram via* **21** *and* **12** *(the middle diagram in Figure 4). According to the process described above, we adjoin* **21** *and* **12** *to the set of rules. Similarly, the critical pair $\langle \mathbf{2}, \mathbf{3} \rangle$ entails adjunction of the rules: $\mathbf{32}, \mathbf{23}$. The critical pair $\langle \mathbf{3}, \mathbf{1} \rangle$ can be completed via* **1** *and* **3** *(the diagram on the right in Figure 4), not entailing an extension of the set of rules. To conclude, in this iteration we have adjoined the rules:*

$$\mathbf{21}, \mathbf{12}, \mathbf{32}, \mathbf{23}$$

[10] This solves the parents' problem in a practical sense.

2. *In the next iteration three times four critical pairs are obtained between 'old' and 'new' (adjoined in the previous iteration) rules:* $\langle \mathbf{i}, \mathbf{12}\rangle, \langle \mathbf{i}, \mathbf{21}\rangle, \langle \mathbf{i}, \mathbf{23}\rangle, \langle \mathbf{i}, \mathbf{32}\rangle$, *for* $1 \leq i \leq 3$. *Tiling with the elementary diagrams in Figure 4 yields for* $i = 1$ *the new rules:*

   $$\mathbf{2132}, \mathbf{123}, \mathbf{321}$$

   $i = 2$ *doesn't yield any new rules.* $i = 3$ *yields (modulo E!) exactly the same rules as* $i = 1$. *There are six more critical pairs between the 'new' rules themselves (up to symmetry and trivial critical pairs). Noticing moreover that the confluence problem is symmetrical in* **1** *and* **3** *(i.e. exchanging* **1** *and* **3** *everywhere preserves correctness of diagrams), we only need to consider four critical pairs:* $\langle \mathbf{12}, \mathbf{21}\rangle, \langle \mathbf{12}, \mathbf{23}\rangle, \langle \mathbf{12}, \mathbf{32}\rangle, \langle \mathbf{21}, \mathbf{23}\rangle$. *Only the second pair entails adjunction of a new rule* **132**. *So, in this iteration we have adjoined the rules:*

   $$\mathbf{2132}, \mathbf{123}, \mathbf{321}, \mathbf{132}$$

3. *The third iteration leads to adjunction of the rules:*

   $$\mathbf{13}, \mathbf{12321}, \mathbf{2321}, \mathbf{1213}$$

4. *The fourth iteration to adjunction of:*

   $$\mathbf{213}, \mathbf{1321}, \mathbf{1232}, \mathbf{121}, \mathbf{232}$$

5. *The fifth iteration:*

   $$\mathbf{12132}, \mathbf{21321}$$

   after which the set of rules remains stable, i.e. all critical pairs are subcommutative.

The final set of (right-hand sides of) rules is:

$$\mathbf{1}, \mathbf{12}, \mathbf{123}, \mathbf{1232}, \mathbf{12321}, \mathbf{121}, \mathbf{1213}, \mathbf{12132}, \mathbf{13}, \mathbf{132}, \mathbf{1321}$$

$$\mathbf{2}, \mathbf{23}, \mathbf{232}, \mathbf{2321}, \mathbf{21}, \mathbf{213}, \mathbf{2132}, \mathbf{21321}, \mathbf{3}, \mathbf{32}, \mathbf{321}$$

Exercise 13 *Check that all critical pairs in the final set of rules in both Lemma 10 and the preceding example are subcommutative (this is a lot of work in case of the example).*

To prove that subcommufication always terminates, it is convenient to develop some theory first.

3.2 Confluence by Complete Developments[11]

Is there any regularity in the generated sets of rules in Subsection 3.1? Staring at the rules, we notice after some time that all have shape $\mathbf{u}_1\mathbf{u}_2$ or $\mathbf{u}_1\mathbf{u}_2\mathbf{u}_3$, where $\mathbf{u}_i$ is a (possibly empty) prefix of $\mathbf{i}\dots\mathbf{1}$, e.g. $\mathbf{32}$ is a possible instantiation of $\mathbf{u}_3$.

Example 14 *1. The rules in Lemma 10 all have shape* $\mathbf{u}_1\mathbf{u}_2$*:*

$$\widehat{\mathbf{1}}\widehat{\ }, \widehat{\mathbf{1}}\widehat{\mathbf{2}}, \widehat{\ }\widehat{\mathbf{2}}, \widehat{\ }\widehat{\mathbf{21}}$$

where each time the hat ($\widehat{.}$) *covers crossings in the same descending sequence.*

2. The rules in the preceding example all have shape $\mathbf{u}_1\mathbf{u}_2\mathbf{u}_3$ *(where we've omitted steps* $\mathbf{u}_i$*):*

$$\widehat{\mathbf{1}}, \widehat{\mathbf{1}}\widehat{\mathbf{2}}, \widehat{\mathbf{1}}\widehat{\mathbf{2}}\widehat{\mathbf{3}}, \widehat{\mathbf{1}}\widehat{\mathbf{2}}\widehat{\mathbf{32}}, \widehat{\mathbf{1}}\widehat{\mathbf{2}}\widehat{\mathbf{321}}, \widehat{\mathbf{1}}\widehat{\mathbf{21}}, \widehat{\mathbf{1}}\widehat{\mathbf{21}}\widehat{\mathbf{3}},$$

$$\widehat{\mathbf{1}}\widehat{\mathbf{21}}\widehat{\mathbf{32}}, \widehat{\mathbf{1}}\widehat{\mathbf{3}}, \widehat{\mathbf{1}}\widehat{\mathbf{32}}, \widehat{\mathbf{1}}\widehat{\mathbf{321}}, \widehat{\mathbf{2}}, \widehat{\mathbf{2}}\widehat{\mathbf{3}}, \widehat{\mathbf{2}}\widehat{\mathbf{32}},$$

$$\widehat{\mathbf{2}}\widehat{\mathbf{321}}, \widehat{\mathbf{21}}, \widehat{\mathbf{21}}\widehat{\mathbf{3}}, \widehat{\mathbf{21}}\widehat{\mathbf{32}}, \widehat{\mathbf{21}}\widehat{\mathbf{321}}, \widehat{\mathbf{3}}, \widehat{\mathbf{32}}, \widehat{\mathbf{321}}$$

Since this regularity is not a coincidence, we present an inductive definition of such sequences.

Definition 15 *Consider the ARS* $\langle \mathrm{Ter}(\Sigma)/E, \mathrel{\circ\!\!\!\!\longrightarrow} \rangle$ *of* developments*, where* $\mathrel{\circ\!\!\!\!\longrightarrow}$ *is generated (cf. Definition 6) by the rules:*

$$o \mathrel{\circ\!\!\!\!\longrightarrow} \mathbf{u}_1 \dots \mathbf{u}_n$$

where for every $1 \leq i \leq n$*,* $\mathbf{u}_i$ *is a (possibly empty) prefix of* $\mathbf{i}\dots\mathbf{1}$*. Denoting a* descending sequence from i to j *by* $[i,j\rangle$*,* $\mathbf{u}_i$ *has shape* $[i,j\rangle$*, for some* $0 \leq j \leq i$*. We call a development having shape* $[1,0\rangle[2,0\rangle[3,0\rangle\dots[n,0\rangle = \widehat{\mathbf{1}}\widehat{\mathbf{21}}\widehat{\mathbf{321}}\dots\widehat{\mathbf{n}\dots\mathbf{1}}$ complete *and it is denoted by* n^* *(see Figure 8).*

The notion complete development was dubbed *fundamental word* in [Gar69]. Complete developments in braids play the same rôle as Gross-Knuth-steps in λ-calculus and orthogonal term rewriting.

All this seems pretty complicated, but this is mainly caused by the (1-dimensional) representation (of braids by words). Looking at the 2-dimensional representation, a sequence having shape $[i,j\rangle$ represents a braid where the $(i+1)^{th}$ strand crosses its $i-j$ neighbouring strands. For example, the sequence $[4,1\rangle = \mathbf{432}$ can be interpreted as: cross the fifth strand over its three neighbouring strands (to the left, see Figure 6). A development expresses that all of the strands *simultaneously* cross a number of strands to their left. The

[11] This subsection is based on [Gar69].

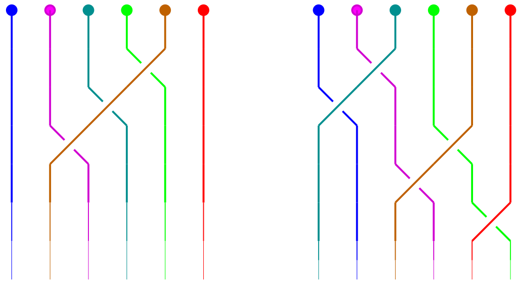


Figure 6: Two developments: **432** and **21435** in 2D

right braid **42531** of the girl in Figure 3 is equivalent to **21435**. This sequence has the shape required for a development $\widehat{\mathbf{21}}\widehat{\mathbf{43}}\widehat{\mathbf{5}}$ (see Figure 6). On the contrary, the left braid of the girl is not (equivalent to) a development (why not? can strands cross twice in a development?).

In the most natural representation of braids as curves in $\mathbb{R}^3$ we can flesh out the intuition that the strands in a development cross simultaneously. A *simultaneous* crossing is constructed as follows:

- Lead the strands straight from their starting points to points on a central vertical axis, such that a strand to the left of another one ends up lower on the axis.
- From these points on the central axis, the strands are led straight to an arbitrary ending point.

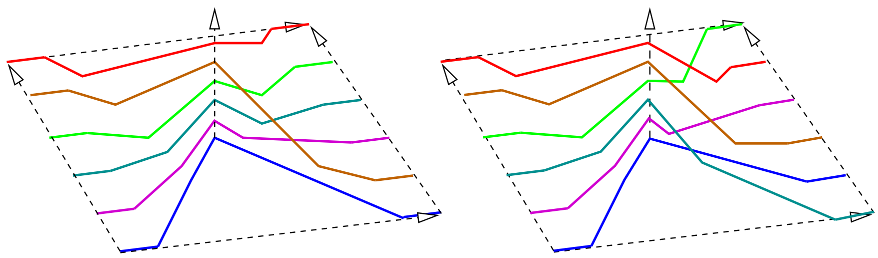


Figure 7: Two developments: **432** and **21435** in 3D

Viewing the horizontal axis as representing time, progressing to the right, we observe that all crossings really take place simultaneously. From this it is easy to see (literally) why the left braid of the girl is not a development: the successive crossings **33** can not be applied simultaneously (there will be some ϵ time between them).

[12] Note that the figure is transformed into itself by a 180 degree rotation. In general: developments are closed w.r.t 180 degree rotations.

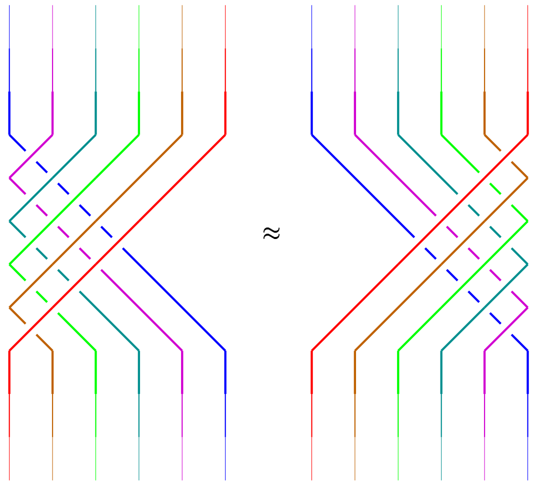


Figure 8: A complete development (in two 2D representations)[12]

We will prove that an arbitrary development can always be extended by *another development* to a complete development, This implies confluence by the so-called *triangle lemma* [Tak95].

Lemma 16 (Triangle) *An ARS $\langle A, \to\rangle$ has the* triangle property, *if there exists a map $.^* : A \to A$ such that for every $a, b \in A$ we have:*

1. *$a \to a^*$, and*
2. *if $a \to b$, then $b \to a^*$.*

An ARS having the triangle property is confluent. □

Exercise 17

1. *Prove the triangle lemma.*
2. *Show that the second condition of the triangle property implies the first if $\to$ is reflexive.*
3. *How many non-equivalent developments can be constructed for braids with n strands?*

The following lemma is the key to confluence and shows that if a development can be completed, then the same holds after 'insertion' of some strand (see Figure 9).

Definition 18 *The* insertion $[i,j\rangle\!\rangle\mathbf{u}$ *of* $[i,j\rangle$ *in the development* $\mathbf{u} = \mathbf{u}_1 \dots \mathbf{u}_n$ *is defined by:* $\mathbf{u}_1 \dots \mathbf{u}_{i-1}[i,j\rangle\tilde{\mathbf{u}}_i \dots \tilde{\mathbf{u}}_n$. *Here* $\widetilde{[k,m\rangle}$ *is defined by* $[k+1,\tilde{m}\rangle$, *where* $\tilde{m} = m$ *if* $m < j$, *and* $\tilde{m} = m + 1$ *otherwise.*

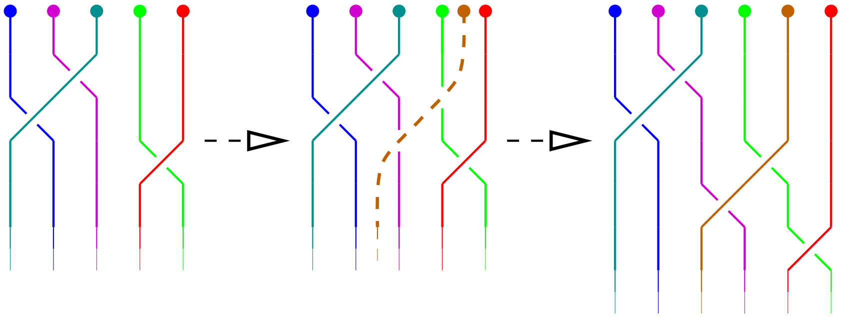


Figure 9: Insertion of a strand $[\mathbf{4{,}2}\rangle\!\rangle\mathbf{214} = \mathbf{21435}$

By definition, inserting a strand in a development yields a development again.

Lemma 19 (Key) *Let* $\mathbf{u} = \mathbf{u}_1 \dots \mathbf{u}_n$ *and* $\mathbf{v} = \mathbf{v}_1 \dots \mathbf{v}_n$ *be developments. Then*

$$\mathbf{uv} =_E n^* \implies ([n+1{,}i\rangle\!\rangle\mathbf{u})([i{,}0\rangle\!\rangle\mathbf{v}) =_E (n+1)^*$$

for all $0 \le i \le n+1$.

Proof

$$\begin{array}{rcl}
([n+1{,}i\rangle\!\rangle\mathbf{u})([i{,}0\rangle\!\rangle\mathbf{v}) & = & ([n+1{,}i\rangle\!\rangle\mathbf{u})\mathbf{v}_1 \dots \mathbf{v}_{i-1}[i{,}0\rangle\tilde{\mathbf{v}}_i \dots \tilde{\mathbf{v}_n} \\
& = & \mathbf{u}_1 \dots \mathbf{u}_n[n+1{,}i\rangle\mathbf{v}_1 \dots \mathbf{v}_{i-1}[i{,}0\rangle\tilde{\mathbf{v}}_i \dots \tilde{\mathbf{v}_n} \\
& =_E & \mathbf{uv}_1 \dots \mathbf{v}_{i-1}[n+1{,}i\rangle[i{,}0\rangle\tilde{\mathbf{v}}_i \dots \tilde{\mathbf{v}}_n \\
& = & \mathbf{uv}_1 \dots \mathbf{v}_{i-1}[n+1{,}0\rangle\tilde{\mathbf{v}}_i \dots \tilde{\mathbf{v}}_n \\
& =_E & \mathbf{uv}_1 \dots \mathbf{v}_{i-1}\mathbf{v}_i \dots \mathbf{v}_n[n+1{,}0\rangle \\
& = & \mathbf{uv}[n+1{,}0\rangle \\
& =_E & n^*[n+1{,}0\rangle \\
& = & (n+1)^*
\end{array}$$

□

Theorem 20 *Braiding is confluent.*

Proof From the triangle lemma it suffices to show that $\twoheadrightarrow$ has the triangle property (why?). We show by induction on n, that if $o \twoheadrightarrow \mathbf{u}$, then $\mathbf{u} \twoheadrightarrow n^*$.

(0) In the base case (one strand) $\mathbf{u} = 0^* = o$.

$(n+1)$ In the induction case, the development can be written as $[n+1{,}i\rangle\!\rangle\mathbf{u}$ for some $0 \le i \le n+1$. By the induction hypothesis it is known that there exists a $\mathbf{v}$ such that $\mathbf{uv} =_E n^*$. We conclude using the key lemma that $[i{,}0\rangle\!\rangle\mathbf{v}$ is the development we are looking for. □

Exercise 21 *1. Show that inserting a development in a development yields a development.*

2. Demonstrate the three equivalences of braids in the proof of the key lemma.

Example 22 *The construction in the proof of Theorem 20 is illustrated in Figure 10 by means of the right braid of the girl in Figure 3. The figure shows how each time the insertion of a (dashed) strand in the top braid is compensated for by the insertion of a (dashed) strand in the bottom braid, such that their concatenation is a complete development.*

Although Theorem 20 solves the parents' problem in general, the solution it yields is usually far from optimal; the extensions contain many more crossings than would have been necessary to find a common one.

Example 23 *Consider the braids* **1** *and* **3***, both consisting of four strands. They can be extended by* **21321** *and* **12132** *respectively, to complete developments. It is more efficient to do so via* **3** *and* **1** *respectively.*

In the sequel, we show that tiling with elementary diagrams always yields a solution and (among others) that the solution found in this way is minimal with respect to the number of crossings. The former follows from *orthogonality* of the braiding ARS. The latter follows from the fact that braiding does not have *syntactical accidents*.

3.3 Orthogonality of Parallel Moves[13]

We introduce an alternative representation of developments as certain relations, called *parallel moves*, and show these relations to be orthogonal.

The representation is based on the following observations. At any moment the strands in a braid are linearly ordered (from left to right). Such an order we call a *state*. A *parallel move* is a relation on strands. Parallel moves induce transformations on states, by viewing them as specifications of which strands should cross (just like the usual representation of permutations in mathematics).

A *union* ($\sqcup$) and a *residual* ($\setminus$) operation are defined on parallel moves. The union of two parallel moves is the minimal common extension of the parallel moves. The residual of a parallel move after another parallel move, is that 'what is left to be done' to reach the common extension, after 'doing' the former. Orthogonality expresses that these operations satisfy the following laws (see Figure 14)

$$
\begin{array}{rcll}
(u \sqcup v) \setminus w & = & (u \setminus w) \sqcup (v \setminus w) & \text{(Arrow)} \\
w \setminus (u \sqcup v) & = & (w \setminus u) \setminus (v \setminus u) & \text{(Prism)}
\end{array}
$$

[13]This subsection is based on [Mel].

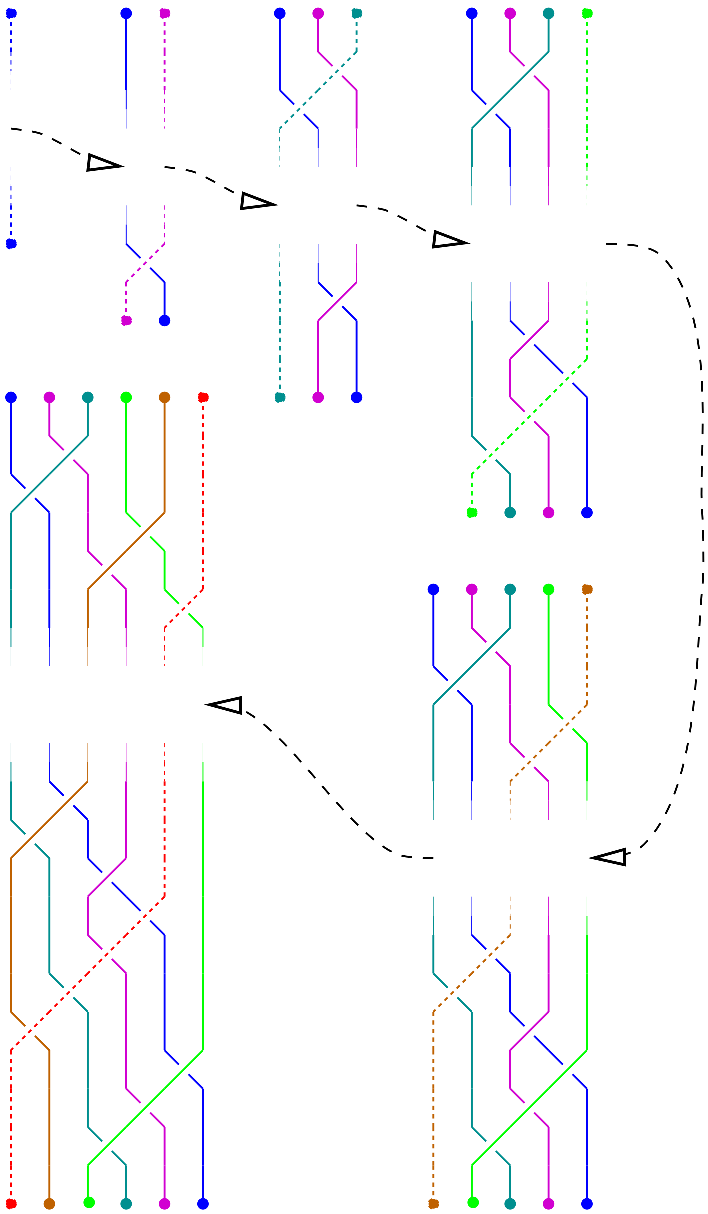


Figure 10: Inductive completion of developments

for arbitrary parallel moves u, v, and w. This will be the main theorem proven in this subsection.

Throughout this subsection braids will consist of n *strands and the (names* *of the) strands are* $\{1,\ldots,n\}$.

Orderings of $\{1,\ldots,n\}$ will sometimes be represented by enumerating the strands in increasing (according to the ordering) order.

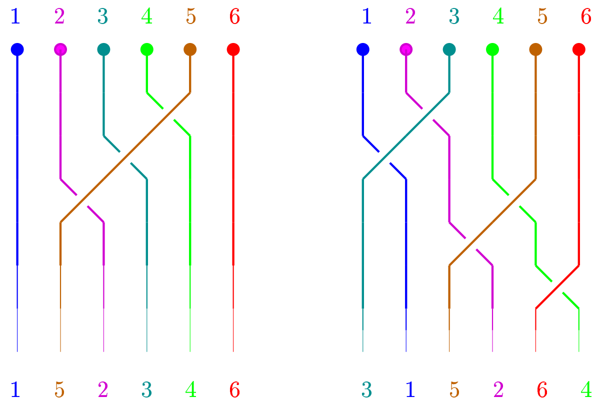


Figure 11: Parallel moves as transformations on orderings

Example 24 *The orderings* $< = 123456$ *and* $\ll = 315264$ *represent the initial and final state of the right braid in Figure 11. Note that the (relational) difference* $v = < - \ll$ *between* $<$ *and* $\ll$ *consists of the pairs* $(1,3),(2,3),(2,5),(4,5),(4,6)$. *These are exactly the pairs of crossing strands. This is no coincidence; for example the difference* u *between the initial and final state of the left braid consists of the pairs* $(2,5),(3,5),(4,5)$ *of crossing strands.*

Definition 25 *A* state *is an irreflexive, transitive, total relation on* $\{1,\ldots,n\}$. *We use* $<, \ll, \lll$ *to range over states. The* parallel move from $<$ to $\ll$ *is* $\complement\ll$, *where* $\complement R = < - R$ *is the* (relative) complement *of* R *with respect to* $<$. *We employ* u, v, *and* w *to range over parallel moves. The* effect $[R]$ *of* R *on* $<$ *is defined by* $\complement R \cup R^\top$, *where* $R^\top$ *is the inverse of* R.[14]

Relative complements will always be relative to the order $<$, *unless stated otherwise. We also assume that if a complement of a relation with respect to some other relation is taken, the former is a subrelation of the latter.*

Parallel moves are by definition completely determined by their initial and final state. This doesn't hold the other way around; for example, the empty relation is a parallel move from any state to itself. We do have that a parallel move together with either its initial or its final state, completely determines the other state. In particular, the final state is determined by the effect $[u]$ of a parallel move u on the initial state $<$ (as we will shortly see).

Exercise 26 *What is the effect of the parallel move* $<$ *on* $<$*?*

[14]Representing a relation by its incidence-matrix, inverting a relation coincides with $\top$ransposition of the matrix.

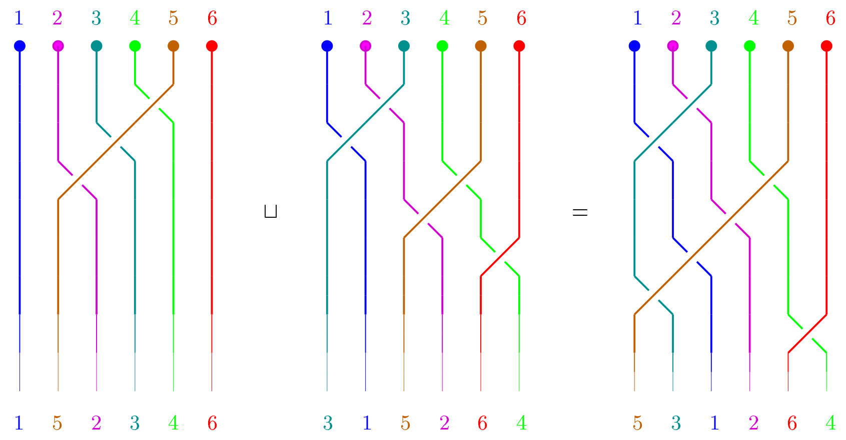


Figure 12: Union of parallel moves

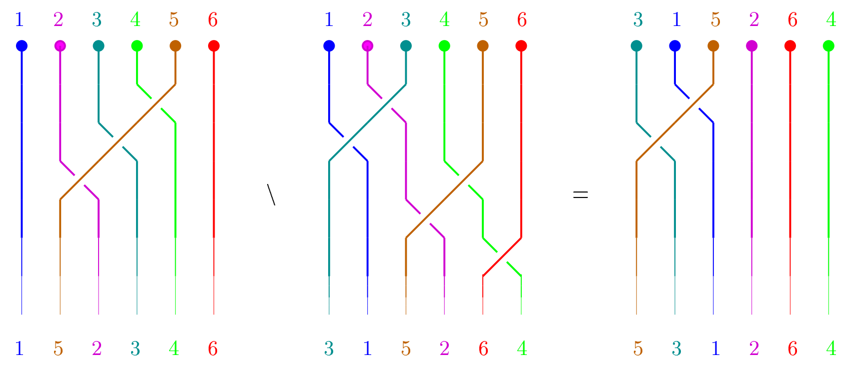


Figure 13: Residual of parallel moves

Example 27 *Consider the parallel moves u and v in Example 24. Their relational union $u \cup v$ consists of the pairs $(1,3),(2,3),(2,5),(3,5),(4,5),(4,6)$. This relation is not transitive (the pair $(1,5)$ is 'missing') hence doesn't represent a parallel move. Only after adjoining the missing pair the parallel move shown in Figure 12 is obtained. The reason for initial failure is intuitively clear: if 1 crosses 3 and 3 crosses 5, then 1 has to cross 5. The other way around, 1 does not cross 6 since 1 crosses 2 nor 2 crosses 6 (see Proposition 32).*

The residual $v \setminus u$ of v after u consists of the pairs $(1,5),(3,5)$ (see Figure 13). Notice that concatenating the parallel moves u and $v \setminus u$ is possible and yields a braid which is equivalent to the parallel move $u \sqcup v$.

Definition 28 *Let R and S be relations.*

1. *The* union *$R \sqcup S$ of R and S is defined by $(R \cup S)^+$.*

2. *The* residual $S \setminus R$ *of* S *after* R *is defined by* $(R \sqcup S) - R$.

3. S *is* contained in R, *if* $S \setminus R = \varnothing$. *This is denoted by* $S \sqsubseteq R$. *If moreover* $R \sqsubseteq S$, *then* R *and* S *are said to be* permutation equivalent, *denoted by* $R \equiv S$.

The definition of the union operation $\sqcup$ on moves can be understood in the following way. In a minimal extension of two parallel moves u and v, at least those strands have to cross which cross in either of them. This explains the relational union $\cup$ in $(u \cup v)^+$. The only remaining problem is that the relational union need not be transitive, hence need not represent a parallel move. Taking the transitive closure is the minimal way to obtain a transitive relation, explaining the $\cdot^+$ in $(u \cup v)^+$. As it turns out (after some interesting calculations) this suffices to yield a parallel move.

The definition of the residual $v \setminus u$ of v after u by means of the expression $(u \sqcup v) - u$ can be seen as a literal translation of the sentence 'that what is left to be done to reach the common extension $(u \sqcup v)$, after doing the former (u).

Proposition 29 (Semilattice)

$$
\begin{array}{rcl@{\qquad\qquad}rcl}
R \sqcup R & = & R & R \setminus R & = & \varnothing \\
R \sqcup \varnothing & = & R & R \setminus \varnothing & = & R \\
R \sqcup S & = & S \sqcup R & \varnothing \setminus R & = & \varnothing \\
R \sqcup (S \sqcup T) & = & (R \sqcup S) \sqcup T & & &
\end{array}
$$

for relations R, S, *and* T *(*R *needs to be transitive for idempotence and the equations containing* $\varnothing$ *to hold).*

Proof The properties of $\sqcup$ follow easily from the corresponding properties of $\cup$ and monotonicity of $\cdot^+$. The properties of $\setminus$ follow from the corresponding properties of $-$ and the properties of $\sqcup$. $\square$

We have to show well-definedness of the union and residual operations, i.e. that applying them to parallel moves yields a parallel move, not just a relation. To that end, we first present a more intrinsic characterisation of parallel moves. Note that $\complement\!\ll\, = \,< \cap \ll^\top$, because of totality of $\ll$ and irreflexivity of $<$. This immediately implies irreflexivity and transitivity of parallel moves. This does not completely characterise parallel moves: the pair $(1, 3)$ is irreflexive and transitive, but does not represent a move from 123. The problem is that 1 cannot cross 3 without 2 crossing either strand (cf. Example 27). To make the latter intuition formal, the *duals* of some standard operations on relations are required.

Definition 30 (Dual) *The* dual $\complement f$ *of an* m*-ary function* f *on relations is defined by* $(\complement f)(R_1, \ldots, R_m) = \complement(f(\complement R_1, \ldots, \complement R_m))$. *The dual of closure and transitive are called* interior *and* scopic *[Mel], respectively. The scopic interior of a relation* R *is denoted by* R^-.

Note that these notions (implicitly) depend on the relation with respect to which the complement is taken. The scopic interior of the complement of a relation is the complement of the transitive closure of the relation.

Exercise 31 *1. Show that identity, inverse, subrelation and intersection are the duals of complement, inverse, superrelation and union respectively.*

*2. Describe the duals of relation composition (*decomposition*) and union (of moves).*

3. Show that a relation R is scopic iff for all $a < c < b$:

$$a \; R \; b \;\Rightarrow\; a \; R \; c \text{ or } c \; R \; b.$$

(I.e. it formalises what we intended to formalise.)

The next proposition provides the alternative characterisation of parallel moves as well as two properties which are essential for well-definedness of union and residual and for the proof that braiding is orthogonal.

Proposition 32 *Let R, S, and T be transitive relations.*

1. If R is a subrelation of state $<$, then

$$R \text{ is a parallel move} \;\Leftrightarrow\; R \text{ is scopic.}$$

2. $(R^-)^+ = R^-$.

3. If $\complement R \subseteq S \cap T$, then $(R \cap (S \cup T))^+ = R \cap (S \cup T)^+$.

Proof

1. ($\Rightarrow$) Suppose $R = \complement\!\ll$ for some state $\ll$. Then $\complement R = \ll$ is transitive because of transitivity of $\ll$. Scopicness then follows from the definition.

   ($\Leftarrow$) We first show that $[R] = \complement R \cup R^\top$ is a state.

   - If $<$ is total, then $\complement Q \cup Q^\top$ as well, for arbitrary Q.
   - $R^\top$ is a subrelation of the irreflexive relation $>$.
   - To show transitivity, it suffices to show that all for compositions of $\complement R$ and $R^\top$ are contained in $[R]$. The components $\complement R$ and $R^\top$ are both transitive by scopicness and transitivity of R respectively. It remains to show that both 'cross-compositions' $\complement R \,;\, R^\top$ and $R^\top \,;\, \complement R$ are contained in $[R]$. W.l.o.g. we only demonstrate the former. Let $a \; (\complement R) \; c \; R^\top \; b$.

     $(a = b)$ cannot occur.

     $(a < b)$ then $a \; \complement R \; b$ because of transitivity of R,

     $(b < a)$ then $b \; R \; a$ because of scopicness of R.

It easily follows that R is the parallel move from $<$ to $[R]$.

2. Since the transitive closure of a relation contains the relation itself the inclusion $(R^-)^+ \subseteq R^-$ remains to be shown. $(\complement R)^+$ is the complement of R^-, hence if the inclusion wouldn't hold then there would exist a minimal m, and a, b, and c such that $a\ R^-\ c\ R^-\ b$ and $a\ (\complement R)^m\ b$.

   (1) Suppose $a \complement R\ b$. Because $R^- \subseteq R$ holds, we have $a\ R\ c\ R\ b$ from the hypothesis hence $a\ R\ b$ by transitivity of R. Contradiction.

   (>1) Suppose $a\ (\complement R)^{m_1}\ c'\ (\complement R)^{m_2}\ b$ for some c', with $1 \leq m_1, m_2 < m$. By totality of $<$ we may w.l.o.g. assume that $c < c'$.

   - If $c\ (\complement R)^+\ c'$, then from $c'\ (\complement R)^{m_2}\ b$ also $c\ (\complement R)^+\ b$. Contradiction.
   - If $c\ R^-\ c'$, then $a\ R^-\ c\ R^-\ c'$. From $a\ (\complement R)^{m_1}\ c'$ a contradiction with the induction hypothesis is obtained since $m_1 < m$.

3. ($\subseteq$) $(R \cap (S \cup T))^+ \subseteq R^+ \cap (S \cup T)^+ = R \cap (S \cup T)^+$.

   ($\supseteq$) Choose a minimal m, and a and b such that $a\ R\ b$ and $a\ (S \cup T)^m\ b$, but not $a\ (R \cap (S \cup T))^+\ b$.

   (1) $a\ (S \cup T)\ b$ leads linea directa to a contradiction.

   (>1) Let $a\ (S \cup T)^{m_1}\ c\ (S \cup T)^{m_2}\ b$ for some c, with $1 \leq m_1, m_2 < m$. It suffices to show $a\ R\ c$ and $c\ R\ b$, since then the induction hypothesis is applicable to both components. Suppose e.g. $a \complement R\ c$. Then $a\ (S \cap T)\ c$ (using the condition) and $c\ (S \cup T)^{m_2}\ b$ implies $a\ (S \cup T)^{m_2}\ b$ because of transitivity of S and T, Contradiction (with minimality of m). $\square$

Exercise 33 *1. What happens in case of an infinite number of strands?*

2. Proposition 32.2 can be expressed cryptically as $+-+ = +-$. Dually it holds that $-+- = -+$. Furthermore $++ = +$ hence $-- = -$. Give an example exemplifying $-+ \neq +-$.

Lemma 34 *Suppose u and v to be parallel moves from $<$, Then*

1. $u \sqcup v$ is the parallel move from $<$ to $[u \sqcup v]$, and

2. $v \setminus u$ is the parallel move from $[u]$ to $[u \sqcup v]$.

Proof

1. Since $u \sqcup v$ clearly is a transitive subrelation of $<$, it suffices by Proposition 32.1 to show that it is scopic. $u \cup v$ is scopic being the relational union of two scopic relations (dual to the fact that the intersection of two transitive relations is transitive). Hence $u \sqcup v = (u \cup v)^+$ is scopic by (the dual of) Proposition 32.2, since it is the transitive closure of a scopic relation.

2. Unfolding the definition of 'the parallel move from $[u]$ to $[u \sqcup v]$' yields $(\complement u \cup u^{\top}) \cap (\complement(u \sqcup v) \cup ((u \sqcup v)^{\top}))^{\top}$. Using $u \subseteq u \sqcup v \subseteq <$ and totality of $<$ we find after some calculation that it is equal to $(u \sqcup v) - u$. $\square$

Orthogonality of a rewrite system is expressed by the so-called *prism theorem* [Hue94]. The theorem roughly says that the residual of a parallel move after another one, does not depend on the way either of them is split (see Figure 14).

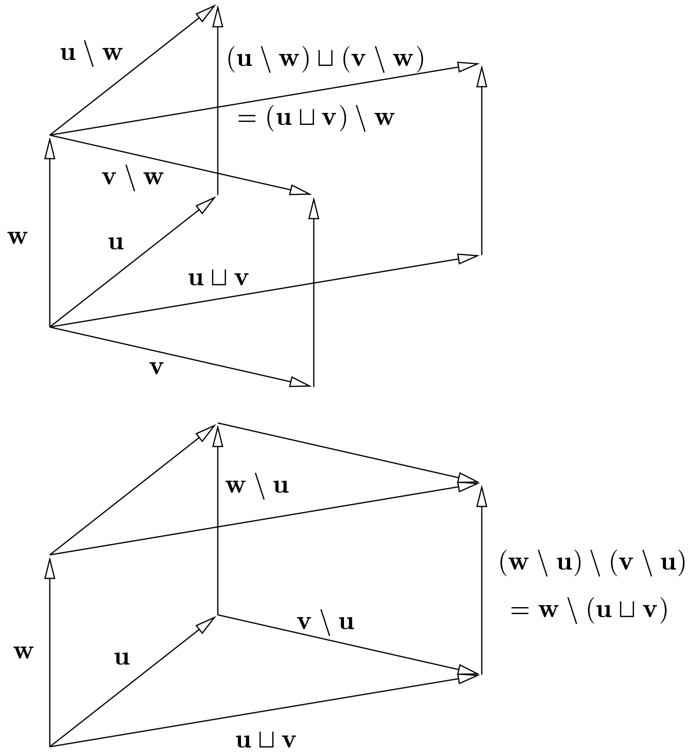


Figure 14: Arrow and Prism

Theorem 35 (Arrow and Prism) *Let u, v, and w be parallel moves from $<$.*

$$
\begin{aligned}
(u \sqcup v) \setminus w &= (u \setminus w) \sqcup (v \setminus w) \\
w \setminus (u \sqcup v) &= (w \setminus u) \setminus (v \setminus u)
\end{aligned}
$$

Proof

$$
\begin{array}{lrcl}
1. & (u \sqcup v) \setminus w & = & (u \sqcup v \sqcup w) - w \\
 & & = & ((u \sqcup w) \cup (v \sqcup w))^+ - w \\
 & & = & (((u \sqcup w) \cup (v \sqcup w)) - w)^+ \\
 & & = & (((u \sqcup w) - w) \cup ((v \sqcup w) - w))^+ \\
 & & = & (u \setminus w) \sqcup (v \setminus w)
\end{array}
$$

$$
\begin{array}{lrcl}
2. & (w \setminus u) \setminus (v \setminus u) & = & ((w \setminus u) \sqcup (v \setminus u)) - (v \setminus u) \\
 & & = & (((w \sqcup u) - u) \cup ((v \sqcup u) - u))^+ - (v \setminus u) \\
 & & = & (((w \sqcup u) \cup (v \sqcup u)) - u)^+ - (v \setminus u) \\
 & & = & (((w \sqcup u) \cup (v \sqcup u))^+ - u) - (v \setminus u) \\
 & & = & ((w \sqcup v \sqcup u) - u) - ((v \sqcup u) - u) \\
 & & = & (w \sqcup v \sqcup u) - (v \sqcup u) \\
 & & = & w \setminus (u \sqcup v)
\end{array}
$$

All equalities are consequences of the algebraic properties, except for the third and fourth equalities where we've made use of Proposition 32.3. Note that w and u are transitive because of (the dual of) Proposition 32.1. □

Exercise 36 *Turn the prism and arrow equalities into rewrite rules by orienting them from left to right. Is the resulting TRS complete?*

Proposition 37 *1. $\sqsubseteq$ is a quasi-order,*

2. $u \sqsubseteq u \sqcup v$, and

3. $u = v \iff u \equiv v$.

Proof

1. Reflexivity follows directly from Proposition 29. Suppose $u \sqsubseteq v \sqsubseteq w$. Then

$$u \setminus w = u \setminus (v \sqcup w) = (u \setminus v) \setminus (w \setminus v) = \varnothing \setminus (w \setminus v) = \varnothing$$

by the prism theorem, hence $\sqsubseteq$ is transitive.

2. By the prism theorem and Proposition 29.

3. By unfolding the definition and by $u = v \iff u \subseteq v \,\&\, v \subseteq u$. □

3.4 Orthogonality of multi-derivations[15]

In the preceding subsection we've seen that parallel moves are orthogonal. In this subsection we will lift this result to *sequences of parallel moves*. The construction employed is an instance of a canonical construction in [HL91], for

[15]This subsection is based on [HL91, KV]

constructing an orthogonal system for sequence of elementary steps (here: multiderivations) from an orthogonal system for elementary steps (here: parallel moves).

Definition 38 Multiderivations *(U, V, W, $\ldots$) are of the following kind:*

1. *A* zero *multiderivation from $<$ to $<$, denoted by $0_<$, or simply 0 if $<$ can be deduced from the context.*
2. *For every parallel move u from $<$ to $\ll$, there is an* elementary *multiderivation $\langle u \rangle$ from $<$ to $\ll$.*[16]
3. *For multiderivations U from $<$ to $\ll$ and V from $\ll$ to $\lll$, there is a* composite *multiderivation $U\,;V$ from $<$ to $\ll$.*

Multiderivations are considered up to the monoid-equations:

$$\begin{array}{rcl} 0\,;U & = & U \\ U\,;0 & = & U \\ (U\,;V)\,;W & = & U\,;(V\,;W) \end{array}$$

Let U, V, and W be multiderivations, and let u, v be parallel moves, all from the same state.

1. *The* residual *operation $\setminus$ is defined by:*

$$\begin{array}{rcl} U \setminus 0 & = & U \\ 0 \setminus U & = & 0 \\ \langle u \rangle \setminus \langle v \rangle & = & \langle u \setminus v \rangle \\ (U\,;V) \setminus W & = & (U \setminus W)\,;(V \setminus (W \setminus U)) \\ U \setminus (V\,;W) & = & (U \setminus V) \setminus W \end{array}$$

2. *The* union *operation $\sqcup$ is defined by $U \sqcup V = U\,;(V \setminus U)$.*
3. *The equational theory obtained by adjoining the equation $0 = \langle \varnothing \rangle$, is denoted by $=_\varnothing$. U is* contained in *V, $U \sqsubseteq V$, if $U \setminus V =_\varnothing 0$. They're* permutation equivalent, *$U \equiv V$, if V is contained in U as well.*

The size *of the zero multiderivation and of elementary multiderivations is 1, the size of a composite multiderivation is the sum of its components, and the size of the residual of some multiderivation after another one is the size of the former. The size of U is denoted by $|U|$.*

Note that it is not clear whether the residual operation is well-defined: e.g. two clauses apply in case $(U\,;U') \setminus (V\,;V')$.

[16] In general for this construction to work one needs to consider elementary multiderivations up to (elementary) permutation equivalence. From Proposition 37 we learn that permutation equivalence coincides with equality in case of parallel moves.

Proposition 39 *The residual operation on multiderivations is well-defined.*

Proof Orient the monoid equations and the defining equations of the residual operation from left to right. We will demonstrate that this yields a complete TRS. Proving local confluence is matter of simple casuistics. We only check two interesting cases of overlap between rules.

1. The term $(U\,;U')\setminus(V\,;V')$ can be rewritten in two different ways:

$$\begin{aligned}
&\to\ ((U\,;U')\setminus V)\setminus V'\\
&\to\ ((U\setminus V)\,;(U'\setminus(V\setminus U)))\setminus V'\\
&\to\ ((U\setminus V)\setminus V')\,;((U'\setminus(V\setminus U))\setminus(V'\setminus(U\setminus V)))
\end{aligned}$$

   and

$$\begin{aligned}
&\to\ (U\setminus(V\,;V'))\,;(U'\setminus((V\,;V')\setminus U))\\
&\to\ ((U\setminus V)\setminus V')\,;(U'\setminus((V\setminus U)\,;(V'\setminus(U\setminus V))))\\
&\to\ ((U\setminus V)\setminus V')\,;((U'\setminus(V\setminus U))\setminus(V'\setminus(U\setminus V)))
\end{aligned}$$

2. The term $((U\,;V)\,;W)\setminus U'$ can be rewritten as

$$\begin{aligned}
&\to\ ((U\,;V)\setminus U')\,;(W\setminus(U'\setminus(U\,;V)))\\
&\to\ ((U\setminus U')\,;(V\setminus(U'\setminus U)))\,;(W\setminus((U'\setminus U)\setminus V))
\end{aligned}$$

   and as

$$\begin{aligned}
&\to\ (U\,;(V\,;W))\setminus U'\\
&\to\ (U\setminus U')\,;((V\,;W)\setminus(U'\setminus U))\\
&\to\ (U\setminus U')\,;((V\setminus(U'\setminus U))\,;(W\setminus((U'\setminus U)\setminus V)))
\end{aligned}$$

This analysis shows that all critical pairs are confluent, hence the TRS is locally confluent [DI, Lemma 2.4.9]. Proving termination is a bit more difficult since directly applying recursive or lexicographic path orders fails. We solve the problem by the *semantic labelling* technique, where symbols in a term/rule may be *labelled* with labels which are determined by the *semantics* of its arguments. The size of a term is a correct semantics in the sense that it never increases by the application of one of the rewrite rules of the TRS (it decreases only in case of the rules for zero). Labelling the residual operator by the sum of the size of its argument, yields the following TRS.

$$\begin{array}{rcl}
0 \,;U & \to & U \\
U \,;0 & \to & U \\
(U \,;V)\,;W & \to & U \,;(V \,;W) \\
U \setminus_{x+1} 0 & \to & U \\
0 \setminus_{1+x} U & \to & 0 \\
\langle u\rangle \setminus_2 \langle v\rangle & \to & \langle u \setminus v\rangle \\
(U \,;V) \setminus_{x+y+z} W & \to & (U \setminus_{x+y} W)\,;(V \setminus_{y+z} (W \setminus_{z+x} U)) \\
U \setminus_{x+y+z} (V \,;W) & \to & (U \setminus_{x+y} V) \setminus_{x+z} W
\end{array}$$

It is easy to show this labelled TRS terminating using a lexicographic path order, which implies termination of the original TRS. From local confluence and termination we have confluence (hence completeness) by Newman's Lemma ([DI, Theorem 1.1.8.(ii)]). Finally, note that 'residual-normal forms' are preserved by application of the 'monoid rules', hence (by completeness) residuals of multiderivations are well-defined. □

Next we check that the laws for residual and union hold for their multiderivation incarnations.

Theorem 40 *For multiderivations U, V, and W we have*

$$\begin{array}{rcll}
U \sqcup 0 & = & U & \\
0 \sqcup U & = & U & \\
U \setminus U & =_\varnothing & 0 & \\
U \sqcup U & =_\varnothing & U & \\
U & \sqsubseteq & U \sqcup V & \\
(U \sqsubseteq V) & \Longleftrightarrow & (V =_\varnothing V \sqcup U) & \\
U \sqcup V & \equiv & V \sqcup U & \\
W \setminus (V \sqcup U) & = & (W \setminus V) \setminus (U \setminus V) & \textit{(Prism)} \\
(V \sqcup U) \setminus W & = & (V \setminus W) \sqcup (U \setminus W) & \textit{(Arrow)} \\
(U \sqcup V) \sqcup W & = & U \sqcup (V \sqcup W) &
\end{array}$$

$\sqsubseteq$ *is a quasi-order, and* $\equiv$ *an equivalence relation which is a congruence for* ; *and* $\setminus$, *hence for* $\sqcup$.

Proof The first two equalities are simple. The third is proven by induction on the structure of U, where in case of an elementary multiderivation the equality $\langle\varnothing\rangle = 0$ is needed. Idempotence of $\sqcup$ follows from the third equality. The following two equalities are implied by

$$U \setminus (U \sqcup V) = U \setminus (U \,;\ldots) = (U \setminus U) \setminus \ldots =_\varnothing 0 \setminus \ldots = 0 \;,$$

$$(U \setminus V =_\varnothing 0) \implies V = V \,;\, 0 =_\varnothing V \,;\, (U \setminus V) = V \sqcup U \text{ , and}$$

$$(V =_\varnothing V \sqcup U) \implies U \setminus V =_\varnothing U \setminus (V \sqcup U) = (U \setminus V) \setminus (U \setminus V) =_\varnothing 0$$

Commutativity of $\sqcup$ by

$$\begin{array}{rcl} (U \sqcup V) \setminus (V \sqcup U) & = & (U \,;\, (V \setminus U)) \setminus (V \,;\, (U \setminus V)) \\ & = & ((U \setminus V) \setminus ((V \setminus U) \setminus (V \setminus U))) \setminus (U \setminus V) \\ & =_\varnothing & 0 \end{array}$$

Prism is obtained by unfolding the definitions. Unfolding of the definitions learns that arrow follows from

$$U \setminus (V \sqcup W) = U \setminus (W \sqcup V) \quad \text{(Cube)}$$

which is proven by induction on the sum of the size of U, V, and W. If either U, V, or W is zero, then Cube follow from the first two equalities. If all three are elementary multiderivations, then

$$\begin{array}{rcl} \langle u \rangle \setminus (\langle v \rangle \sqcup \langle w \rangle) & = & \langle u \rangle \setminus (\langle v \rangle \setminus (\langle w \rangle \setminus \langle v \rangle)) \\ & = & (\langle u \rangle \setminus \langle v \rangle) \setminus (\langle w \rangle \setminus \langle v \rangle) \\ & = & \langle (u \setminus v) \setminus (w \setminus v) \rangle \\ & = & \langle u \setminus (v \sqcup w) \rangle \end{array}$$

by the prism theorem (for parallel moves). By commutativity of $\sqcup$ (for parallel moves) the result follows symmetrically. If at least one of U, V, and W is a composite multiderivation, then Cube follows by induction hypothesis:

1. If $U = U_1 \,;\, U_2$, then

$$\begin{array}{rcl} (U_1 \,;\, U_2) \setminus (V \sqcup W) & = & (U_1 \setminus (V \sqcup W)) \,;\, (U_2 \setminus ((V \sqcup W) \setminus U_1)) \\ & = & (U_1 \setminus (W \sqcup V)) \,;\, (U_2 \setminus ((W \sqcup V) \setminus U_1)) \\ & = & (U_1 \,;\, U_2) \setminus (W \sqcup V) \end{array}$$

2. If $V = V_1 \,;\, V_2$, then

$$\begin{array}{rcl} U \setminus ((V_1 \,;\, V_2) \sqcup W) & = & U \setminus (V_1 \,;\, (V_2 \sqcup (W \setminus V_1))) \\ & = & (U \setminus V_1) \setminus (V_2 \sqcup (W \setminus V_1)) \\ & = & (U \setminus V_1) \setminus ((W \setminus V_1) \sqcup V_2) \\ & = & U \setminus (V_1 \,;\, ((W \setminus V_1) \sqcup V_2)) \\ & = & U \setminus ((V_1 \sqcup W) \,;\, (V_2 \setminus (W \setminus V_1))) \\ & = & (U \setminus (V_1 \sqcup W)) \setminus (V_2 \setminus (W \setminus V_1)) \\ & = & (U \setminus (W \sqcup V_1)) \setminus (V_2 \setminus (W \setminus V_1)) \\ & = & U \setminus (W \,;\, (V_1 \setminus W) \,;\, (V_2 \setminus (W \setminus V_1))) \\ & = & U \setminus (W \sqcup (V_1 \,;\, V_2)) \end{array}$$

3. $W = W_1 ; W_2$ is left to the reader. □

Associativity of $\sqcup$ follows using arrow by

$$\begin{aligned}
(U \sqcup V) \sqcup W &= U ; (V \setminus U) ; (W \setminus (U \sqcup V)) \\
&= U ; (V \setminus U) ; ((W \setminus U) \setminus (V \setminus U)) \\
&= U ; ((V \setminus U) \sqcup (W \setminus U)) \\
&= U ; ((V \sqcup W) \setminus U) \\
&= U \sqcup (V \sqcup W)
\end{aligned}$$

$\sqsubseteq$ is a quasi-order by the above, analogously to Proposition 37. Being the intersection of two quasi-order $\equiv$ is an equivalence relation. It is a congruence as well by simple pedipulation of the above. Suppose $U \equiv U'$ en $V \equiv V'$. Then

$$\begin{aligned}
&(U \setminus V) \setminus (U' \setminus V') \\
&=_\varnothing \quad ((U \sqcup U') \setminus (V \sqcup V')) \setminus ((U' \sqcup U) \setminus (V' \sqcup V)) \\
&=_\varnothing \quad ((U \setminus (V \sqcup V')) \sqcup (U' \setminus (V \sqcup V'))) \setminus ((U' \setminus (V' \sqcup V)) \sqcup (U \setminus (V' \sqcup V))) \\
&=_\varnothing \quad 0
\end{aligned}$$

by applying Arrow and Cube. Congruence for ; and $\sqcup$ are just as simple. □

Summarising: we've constructed an orthogonal system for multiderivations by lifting an orthogonal system for parallel moves in a canonical way. In the next subsection parallel moves are related to developments, multiderivations to braids, and permutation equivalence to braid equivalence.

3.5 Confluence by Orthogonality

Of course, we want to relate the notion of a parallel move as introduced above to ordinary braidings. We show that, firstly, every ordinary crossing can be viewed as a parallel move, and secondly, that parallel moves can be *developed*[17] as a sequence of crossings, transforming permutation equivalence into braid equivalence. Subsequently, the correspondence between parallel moves and developments is lifted to a correspondence between multiderivations and braids.

Definition 41 *Let u, v be parallel moves from $< = a_1 \dots a_n$.*

1. *u is* elementary *if it is not the union of (non empty) parallel moves. Scopicness implies that u has shape $\{(a_i, a_{i+1})\}$ (a crossing of two neighbouring strands).* **i** *is called* the crossing associated with *u.*

2. *A* development *of the parallel move u is*

   ($\varnothing$) the trivial braiding o if no elementary move is possible, or

[17]The notion of a development in Subsection 3.2 will turn out to be a special (inductively defined) case of this new notion of development.

($\neg\varnothing$) *a braiding* $\mathbf{iu}$*, where* $\mathbf{i}$ *is the crossing associated with an elementary move* v *such that* $v \sqsubseteq u$*, where* $\mathbf{u}$ *is a development of the parallel move* $u \setminus v$ *from* $[v]$*. This can be viewed as a* state transition

$$(<, u) \rightsquigarrow_i ([v], u \setminus v)$$

from a state $<$ *where* u *still has to be developed into the state* $[v]$ *where* v *has been applied and* $u \setminus v$ *remains to be developed.*

3. *The ARS* $\langle \mathrm{Ter}(\Sigma)/E, \multimap\!\!\rightarrow \rangle$ *of* developments *is generated by:*

$$o \multimap\!\!\rightarrow_u \mathbf{u}$$

where $\mathbf{u}$ *is a development of an arbitrary parallel move* u*.*

4. *A* development *of a multiderivation* U *is*

   (0) o *if* $U = 0$*,*

   ($\langle\cdot\rangle$) *a development of* u *if* $U = \langle u \rangle$*, and*

   ($;$) $\mathbf{U}_1\mathbf{U}_2$ *if* $\mathbf{U}_i$ *is a development of* U_i *and* $U = U_1 \,;U_2$*.*

In Item 3 of the definition the symbol $\multimap\!\!\rightarrow$ is overloaded (cf. Definition 15). This is harmless, as will be shown in Proposition 51. Finally note that we may assume w.l.o.g. that $< = 1 \dots n$ in the definition of a development, since the definition is parametric in the names of the strands (their order is the only thing that matters).

Example 42 1. *Consider the parallel move* $(1, 2), (1, 3)$ *from* 123*. The pair* $(1, 3)$ *is not a parallel move, but the pair* $(1, 2)$ *is (why?) and* $\{(1, 2)\} \setminus \{(1, 2), (1, 3)\} = \varnothing$*. The residual of* $(1, 2), (1, 3)$ *after* $(1, 2)$ *is the elementary move* $(1, 3)$ *from* 213*. The development associated with doing* $(1, 2)$ *followed by* $(1, 3)$ *is* $\mathbf{12}$*. This is the only development possible here.*

2. *The parallel move* $(1, 2), (1, 3), (2, 3)$ *from* 123 *has two developments:* $\mathbf{121}$ *and* $\mathbf{212}$*.*

Exercise 43 1. *Compute the parallel move* $\{(i, i + 1)\} \sqcup \{(j, j + 1)\}$ *and its developments, for* $i = j$*,* $i = j + 1$*, and* $i > j + 1$*, (from* $1 \dots n$*). Cf. these to Figure 4.*

2. *A development of a multiderivation has been defined here as a sequence of developments of its constituting parallel moves. Show that developments are preserved by the monoid equalities, but not by permutation equivalence. Try to find a notion of* family development *which is preserved by permutation equivalence and such that all family developments are finite (cf. [Oos97b]).*

Lemma 44 *Let* $\mathbf{u}$ *be a development of the parallel move* u *from* $<$*.*

1. $\mathbf{u}$ *is a prefix of some development of* $u \sqcup v$*, for every parallel move* v *from* $<$*. If moreover* $\mathbf{u}$ *is finite, then it is a suffix of a development of* $v \setminus u$*.*
2. $\mathbf{u}$ *is finite* ($\rightsquigarrow$ *is terminating).*

Proof

1. For the first part it suffices to show that if the conditions of the lemma hold, and if it is possible to do $\mathbf{i}$ according to u, then $\mathbf{i}$ is also possible from $u \sqcup v$ *and* we end up in a state which satisfies the conditions again. Let w be the elementary move from $<$ with which $\mathbf{i}$ is associated.

   (a) $w \sqsubseteq u \sqsubseteq u \sqcup v$, where the second equality follows by the prism theorem,

   (b) In the same way $u \setminus w$ is a parallel move from $[w]$, $(u \sqcup v) \setminus w$ is one as well. Furthermore, the latter can be written as a union $(u \setminus w) \sqcup (v \setminus w)$ because of the arrow theorem. Hence after doing the move $\mathbf{i}$ the conditions are satisfied.

   For the second part it suffices to note that

   $$\begin{aligned} v \setminus u &= v \setminus (w \sqcup u) \\ &= (v \setminus w) \setminus (u \setminus w). \end{aligned}$$

   by the choice of w and the prism theorem. Since by repeated application it follows that

   $$\begin{aligned} v \setminus u &= (u \sqcup v) \setminus u \\ &= (\ldots((u \sqcup v) \setminus w_1) \ldots \setminus w_m) \setminus (\ldots (u \setminus w_1) \ldots \setminus w_m) \\ &= (\ldots((u \sqcup v) \setminus w_1) \ldots \setminus w_m) \end{aligned}$$

   where $w_1, \ldots, w_m$ is the elementary move associated with the development $\mathbf{u}$. The last equality follows from the fact that $\mathbf{u}$ is a development of u.

2. Let R, S be relations and R transitive, such that $S \sqcup R = R$. Then $R \setminus S = (R \sqcup S) - S = R - S$, hence $R \setminus S$ consists of less pairs than R (if S is not empty). This directly implies that the length of a development of a parallel move is bounded by the number of pairs in it. $\square$

Note that the first part of the lemma is abstract in the sense that it holds for an arbitrary orthogonal system, hence also for systems where developments are not necessarily finite[18] Hence to prove finiteness definitions had to be unfolded.

Proposition 45 $\rightarrow \subseteq \mathrel{-\!\!\circ\!\!\rightarrow} \subseteq \twoheadrightarrow$.

[18] Think of an infinite number of strands, or infinite terms.

Proof We demonstrate both inclusions.

1. A crossing $\mathbf{i}$ is the development of the elementary move (a_i, a_{i+1}) from $a_1 \ldots a_n$.

2. By definition of developments as sequences of crossings and Lemma 44, guaranteeing that those sequences are finite. □

Applied to TRSs, this proposition asserts that to show confluence of $\rightarrow$, it suffices to show that $\multimap\!\!\rightarrow$ has the diamond property. In case of braids, confluence itself is a weak statement, since it only asserts that the starting and ending of two braids agree with one another, but nothing about how this was achieved. The first part does imply that we can associate a multiderivation with every braid, which is constructed from the sequence of elementary parallel moves.

Lemma 46 *1. Let u and v be parallel moves from $<$, with developments $\mathbf{u}$, $\mathbf{v}$. There exist developments $\mathbf{u}'$ and $\mathbf{v}'$ of $v \setminus u$ and $u \setminus v$, such that $\mathbf{u}\mathbf{u}' =_E \mathbf{v}\mathbf{v}'$.*

2. Let U and V be multiderivations from $<$, with developments $\mathbf{U}$ and $\mathbf{V}$. There exist developments $\mathbf{U}'$ and $\mathbf{V}'$ of $V \setminus U$ and $U \setminus V$, such that $\mathbf{U}\mathbf{U}' =_E \mathbf{V}\mathbf{V}'$.

Proof (see Figure 15).

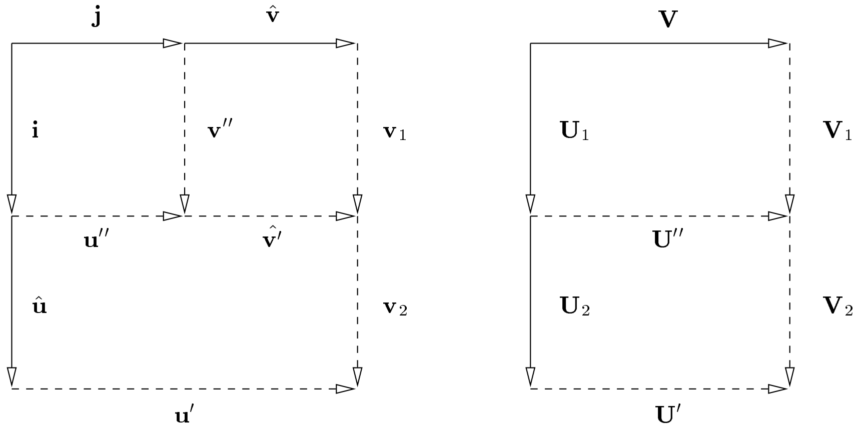


Figure 15: Equivalence of developments

1. This is proven by well-founded induction on the initial state $(<, u \sqcup v)$, ordered by $\rightsquigarrow^+$.

- If $u = \varnothing$, then $\mathbf{u} = o$. Furthermore $u \setminus v = \varnothing$ and $v \setminus u = \varnothing$, we can take $\mathbf{u}' = \mathbf{v}$ and $\mathbf{v}' = o$.
- The case $v = \varnothing$ is dealt with symmetrically.
- If neither of the parallel moves is empty, then $\mathbf{u} = \mathbf{i}\hat{\mathbf{u}}$ and $\mathbf{v} = \mathbf{j}\hat{\mathbf{v}}$, for crossings $\mathbf{i}$ and $\mathbf{j}$ associated with the elementary parallel moves i and j such that $i \sqsubseteq u$ and $j \sqsubseteq v$. Furthermore $\hat{\mathbf{u}}$ is a development of $u \setminus i$ and $\hat{\mathbf{v}}$ is a development of $v \setminus j$. $\mathbf{i}$ and $\mathbf{j}$ are the first crossings of the developments of $i \sqcup j$, say $\mathbf{iu}''$ and $\mathbf{jv}''$. By the induction hypothesis there exist development $\mathbf{v}_1$ of $i \setminus v$ and $\hat{\mathbf{v}'}$ of $v \setminus (i \sqcup j)$ such that $\hat{\mathbf{v}}\mathbf{v}_1 =_E \mathbf{v}''\hat{\mathbf{v}'}$. Another application of the induction hypothesis yields developments $\mathbf{u}'$ and $\mathbf{v}_2$ such that $\mathbf{u}''\hat{\mathbf{v}'}\mathbf{v}_2 =_E \hat{\mathbf{u}}\mathbf{u}'$. Defining $\mathbf{v}' = \mathbf{v}_1\mathbf{v}_2$ entails

$$\begin{aligned}
\mathbf{vv}' &=_E \mathbf{j}\hat{\mathbf{v}}\mathbf{v}_1\mathbf{v}_2 \\
&=_E \mathbf{jv}''\hat{\mathbf{v}'}\mathbf{v}_2 \\
&=_E \mathbf{iu}''\hat{\mathbf{v}'}\mathbf{v}_2 \\
&=_E \mathbf{i}\hat{\mathbf{u}}\mathbf{u}' \\
&=_E \mathbf{uu}'
\end{aligned}$$

2. This is proven by induction on the size of $U \sqcup V$ which is naturally ordered.

   - If either is the zero multiderivation, then it is not hard to find suitable U' and V'.
   - If both are elementary multiderivations, then we conclude using the first part.
   - If at least one of U and V is a composite multiderivation, say $U = U_1 \,; U_2$, then we reason as follows. By the induction hypothesis there exist developments $\mathbf{U}''$ and $\mathbf{V}_1$ of $V \setminus U_1$ and $U_1 \setminus V$ respectively, such that $\mathbf{U}_1\mathbf{U}'' =_E \mathbf{VV}_1$. Another application of the induction hypothesis yields developments $\mathbf{U}'$ and $\mathbf{V}_2$ of $V \setminus U$ and $U_2 \setminus (V \setminus U_1)$, such that $\mathbf{U}_2\mathbf{U}' =_E \mathbf{U}''\mathbf{V}_2$. Defining $\mathbf{V}' = \mathbf{V}_1\mathbf{V}_2$ entails

$$\begin{aligned}
\mathbf{VV}' &=_E \mathbf{VV}_1\mathbf{V}_2 \\
&=_E \mathbf{U}_1\mathbf{U}''\mathbf{V}_2 \\
&=_E \mathbf{U}_1\mathbf{U}_2\mathbf{U}' \\
&=_E \mathbf{UU}'
\end{aligned}$$

We are now ready to reap the fruits from our hard labour and present an alternative proof of confluence of braids.

Proof [of Theorem 20] Every pair of braids $\mathbf{U}$ and $\mathbf{V}$ can be viewed as developments of certain multiderivations U and V. According to Lemma 46 there exist developments $\mathbf{U}'$ and $\mathbf{V}'$ such that $\mathbf{U}\mathbf{U}' =_E \mathbf{V}\mathbf{V}'$. □

We can even say more.

Corollary 47 *If the multiderivations associated with two braids are permutation equivalent, then the braids are equivalent.*

Proof Since and because: if the multiderivations U and V associated with the braids $\mathbf{U}$ and $\mathbf{V}$ are permutation equivalent, then by definition $U \setminus V =_\varnothing 0$ and $V \setminus U =_\varnothing 0$. Adjoining the rule $\langle\varnothing\rangle \to 0$ to the TRS in the proof of Proposition 39 preserves completeness. Furthermore, the application of rewrite rules containing 0 (two monoid rules and the adjoined rules) can be postponed, implying that if if for some multiderivation W it holds that $W =_\varnothing 0$, then $W = \langle\varnothing\rangle\,;\ldots;\langle\varnothing\rangle$, hence o is the only development of W. According to Lemma 46 there exist developments $\mathbf{U}'$ and $\mathbf{V}'$ off $U \setminus V$ and $V \setminus U$, such that $\mathbf{U}\mathbf{U}' =_E \mathbf{V}\mathbf{V}'$. From $\mathbf{U}' = o = \mathbf{V}'$ we deduce $\mathbf{U} =_E \mathbf{V}$. □

The reverse holds as well.

Lemma 48 *If two braids are equivalent, then the multiderivations associated with the braids are permutation equivalent.*

Proof Since permutation equivalence is an equivalence relation, it suffices to show this fore an elementary braid equivalence, i.e. the replacement of one side of an elementary diagram by another one. So suppose $\mathbf{U} = \mathbf{W}_1\mathbf{U}'\mathbf{W}_2$, $\mathbf{V} = \mathbf{W}_1\mathbf{V}'\mathbf{W}_2$, where $(\mathbf{U}' = \mathbf{V}') \in E$. The multiderivations U and V associated with these braids can be written as: $U = W_1\,;U'\,;W_2$ and $V = W_1\,;V'\,;W_2$, where U' and V' are the multiderivations associated with $\mathbf{U}'$ and $\mathbf{V}'$. We calculate as follows:

$$\begin{array}{rcl} U \setminus V & = & (W_1\,;U'\,;W_2) \setminus (W_1\,;V'\,;W_2) \\ & =_\varnothing & (U'\,;W_2) \setminus (V'\,;W_2) \\ & =_\varnothing & W_2 \setminus W_2 \\ & =_\varnothing & 0 \ \square \end{array}$$

Theorem 49 *Two braids are equivalent iff their associated multiderivations are permutation equivalent.*

Proof Direct consequence of Corollary 47 and Lemma 48. □

The theorem suggest that residual and union operations on braids can be defined via the residual and union operations on the associated multiderivations. The only remaining problem is that multiderivations can be developed into braids in many different ways. In the next subsection suitable (canonical) developments are constructed by means of tiling.

Exercise 50 *Give a definition of the notion of a* family development *(cf. Exercise 43) such that*

$$\mathbf{U} =_E \mathbf{V} \iff U \equiv V$$

holds for all multiderivations U and V and their family developments $\mathbf{U}$ *and* $\mathbf{V}$.

To conclude this subsection we show, as promised, that our overloading of the definition of a development is harmless.

Proposition 51 *Developments in the sense of Definition 15 are development in the sense of Definition 41.*

Proof The proof is by induction on n

(0) The only braid consisting of one strand, o, is a development of $\varnothing$.

$(n+1)$ Consider the braid $\mathbf{u}[n+1,i\rangle$, where by induction hypothesis $\mathbf{u}$ is a development of a parallel move u from $1 \dots n+1$ to $a_1 \dots a_{n+1}$. Define a parallel move $u' = u \cup \{(a_m, n+2) \mid i < m \leq n+1\}$ from $1 \dots n+2$ to $a_1 \dots a_i n+2 a_{i+1} \dots a_{n+1}$. □

Exercise 52 1. *Complete the proof of Proposition 51.*

2. *Compute the relation corresponding to a complete development on a braid consisting of* 4 *strands.*

3.6 Orthogonality of Braiding[19]

The tiling process which has been intuitively described above, is formalised as a TRS. Subsequently, this TRS is employed to define residual and union operations on braids, such that braiding is orthogonal. The construction is abstract in the sense that well-definedness of the tiling process only depends on finiteness of developments of parallel moves and on canonicity of tilings (because elementary diagrams are canonical).

Definition 53 (Tiling TRS) Conversions *consist just like braidings of sequences of crossings* $\mathbf{1}, \dots, \mathbf{n}$, *but this time* inverse *crossings* $\mathbf{1}^\top, \dots, \mathbf{n}^\top$ *are allowed as well. The tiling rules have, for arbitrary $1 \leq i, j \leq n$, left-hand side* $\mathbf{i}^\top(\mathbf{j}(x))$ *and right-hand side:*

$$\begin{array}{ll} x & \text{if } |i-j| = 0 \\ \mathbf{j}(\mathbf{i}(\mathbf{j}^\top(\mathbf{i}^\top(x)))) & \text{if } |i-j| = 1 \\ \mathbf{j}(\mathbf{i}^\top(x)) & \text{if } |i-j| \geq 2 \end{array}$$

For a given conversion x, $x{\downarrow}$ denotes the 'positive part' $\mathbf{U}$ *of the tiling normal form* $\mathbf{U}(\mathbf{V})^\top$ *of x.*

[19] This subsection is based on [Klo80, Oos94].

Note the correspondence between the tiling rules and the elementary diagrams of Figure 4 and moreover that the application of a tiling rule indeed corresponds to the 'tiling' by an elementary diagram.

Proposition 54 *The tiling-normal forms have shape* $\mathbf{i}_1 \ldots \mathbf{i}_m \mathbf{j}_1^\top \ldots \mathbf{j}_l^\top$.

Proof Trivial. □

Since crossings can be viewed as transformations on states (as remarked above), at any moment in a conversion (i.e. for any subterm) the state is completely determined by the initial state or even by an arbitrary state somewhere in the conversion. For this reason states are left implicit in the proof of the following theorem.

Theorem 55 *The tiling TRS is terminating.*

Proof The global idea is that tiling any 'square' in Figure 16 terminates by finiteness of developments, hence the complete process terminates by finiteness of the number of squares. To formalise this informal description, a labelled

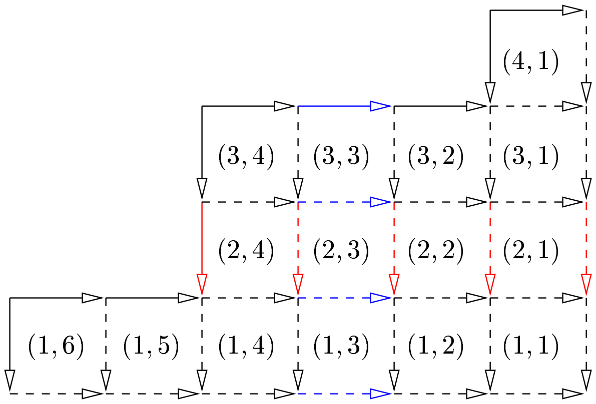


Figure 16: Termination of tiling

version of the tiling TRS is introduced. We show that every tiling can be lifted to a *well* labeled tiling, and that well-labeled tilings are terminating.

1. A *label* is a quadruple consisting of two *coordinates* (natural numbers) and two parallel moves, called the *domain* and the *image*.

   (a) The alphabet of the labelled tiling TRS consists of the constant o, labelled crossings, an labelled inverse crossings. A labelled conversion is *good*, if for every occurrence of a crossing in the conversion it holds that

      i. the image is the residual of the domain after the crossing (and mutatis mutandis for the inverse).

ii. for the coordinates (r, c) and (r', c') of the crossing and its successor, we have
   - $r \leq r'$, and if $r = r'$ then the image of the former is contained in the domain of the latter,
   - $c' \leq c$, and if $c' = c$ then the domain of the latter is contained in the image of the former.

(b) Consider arbitrary labelled crossings $\mathbf{i}^{\top}_{(r,c,v,u)}$ and $\mathbf{j}_{(r',c',u',v')}$. Let $\hat{r}$ and $\hat{c}$ be the minima of r and r', and c and c' respectively. Then there exists a labelled tiling rule with left-hand side $\mathbf{i}^{\top}_{(r,c,v,u)}(\mathbf{j}_{(r',c',u',v')}(x))$ and right-hand side:

$$\begin{array}{ll} x & \text{if } |i-j| = 0 \\ \mathbf{j}_{(\hat{r},\hat{c},\hat{v},w)}(\mathbf{i}_{(\hat{r},\hat{c},w,y)}(\mathbf{j}^{\top}_{(\hat{r},\hat{c},y,w')}(\mathbf{i}^{\top}_{(\hat{r},\hat{c},w',\hat{v}')}(x)))) & \text{if } |i-j| = 1 \\ \mathbf{j}_{(\hat{r},\hat{c},\hat{v},w)}(\mathbf{i}^{\top}_{(\hat{r},\hat{c},w,\hat{u}')}(x)) & \text{if } |i-j| \geq 2 \end{array}$$

where the domains and images are obtained by taking residuals 'along the sides of the diagram', starting with $\hat{u} = u \sqcup u'$.

We first show that good conversions are preserved under reduction. The part of the conversion that remains fixed is still good. Furthermore, the domains and images created by the application of a labelled tiling rule satisfy the clause for goodness. Finally, consider a 'created succession' of two crossings having labels (r_1, c_1, u_1, v_1) and (r_2, c_2, u_2, v_2).

- If both crossings are preserved ones, then the first ('collapsing') tiling rule must have been applied, hence $r_1 \leq r_2$ and $c_2 \leq c_1$ follow from goodness of the original conversion and transitivity of $\leq$. Furthermore, if e.g.. the first coordinates are the same, then the first coordinates in the rule are the same and $v_1 \sqsubseteq u_2$ follows by goodness of the original conversion and transitivity of $\sqsubseteq$.
- If w.l.o.g. the second crossing is a created one, then $(r_2, c_2, u_2, v_2) = (\hat{r}, \hat{c}, \hat{v}, w)$, and $r_1 \leq \hat{r}$, $\hat{c} \leq c_1$ follow from the definitions of $\hat{r}$, $\hat{c}$ and goodness of the original conversion. Furthermore, if e.g. the first coordinates are the same, then $v_1 \sqsubseteq v \sqsubseteq \hat{v}$.

Good conversions are terminating. Measure such a conversion by the multiset of all labels occurring in it. Order labels by the lexicographic product of the order on coordinates and the order on parallel moves, where coordinates are ordered by the product ordering of the usual order $>$ on the naturals, $\rightsquigarrow^+$. Conversions are ordered by the usual multiset extension of the ordering on the labels. By [DI, Theorem 4.5.5] this ordering is terminating, since both $>$ (naturally so) and $\rightsquigarrow^+$ (Lemma 44) are terminating. This measure is decreased (in this ordering) by the application of any tiling rule. Since either the coordinates of the created labels (of the crossings) are (all) smaller than the coordinates of the removed labels, of they are (all) the same. In the latter case it must hold by goodness of the original conversion and by Proposition 37 that the image of the first of the removed crossings is the same as the domain of the second one, that is, $\hat{u} = u = u'$. Per construction the created labels are reachable by state transitions (via $\rightsquigarrow$-steps) hence smaller.

We still need to check that every tiling can be lifted to a well-labelled tiling. Obviously, the crossings of a (finite) conversion can be labelled, since the first coordinates can be labelled in increasing order, and the second coordinates in decreasing order, (see Figure 16), and every crossing is associated with and (elementary) move having the empty relation as residual. Moreover, tiling steps can always be lifted to labelled tiling steps, since for every labelling of the left-hand side of a tiling rule, there exists a right-hand side which is a labelling of the right-hand side of the tiling rule, per construction. □

This proof is abstract in the sense that it only uses orthogonality and finiteness of developments. One of its consequences is that tiling is terminating for orthogonal TRSs. Since the tiling TRS has no critical pairs, tiling is locally confluent ([DI, Lemma 2.4.9]) and terminating, hence complete. The next proposition expresses that residuals can be computed by tiling.

Proposition 56 *1. Let* $\mathbf{u}$ *and* $\mathbf{v}$ *be developments of parallel moves* u *and* v*. If* $\mathbf{u}'(\mathbf{v}')^{\top}$ *is the tiling-normal form of* $\mathbf{u}^{\top}\mathbf{v}$*, then* $\mathbf{u}'$ *and* $\mathbf{v}'$ *are developments of the parallel moves* $v \setminus u$ *and* $u \setminus v$*.*

2. Let $\mathbf{U}$*,* $\mathbf{V}$ *be braids, and* U*,* V *their associated multiderivations. If* $\mathbf{U}'(\mathbf{V}')^{\top}$ *is the tiling-normal form of* $\mathbf{U}^{\top}\mathbf{V}$ *then* $\mathbf{U}'$ *and* $\mathbf{V}'$ *are developments of* $V \setminus U$ *and* $U \setminus V$*.*

Proof [Sketch]

1. The proof is analogous to the second item. In addition we note that there exists a well-labelled version of $\mathbf{u}^{\top}\mathbf{v}$ where all coordinates are $(0, 0)$, which implies that the 'residuals' obtained in the end, are themselves developments of parallel moves.

2. Associate with a well-labelled version of $\mathbf{U}^{\top}\mathbf{V}$ a graph, such that its edges correspond to state transitions. Tiling with an elementary diagram transforms a conversion into a new conversion and with it we can associate an extension of the graph (see Figure 17). In the initial situation we have:

   (a) All paths in the graph between two edges are permutation equivalent,

   (b) Every path from the root to some vertex is contained in $U \sqcup V$.

   These properties are preserved by tiling (use Arrow for the latter property) hence hold in the finally constructed diagram. By construction, U as well as V is contained in a (every) path W from the root to the (unique) end

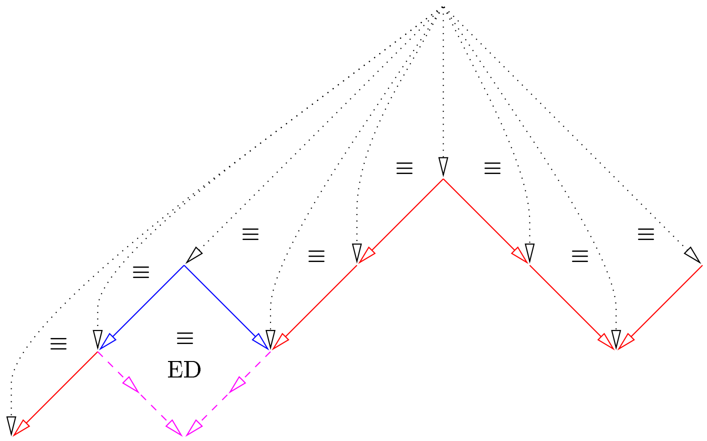


Figure 17: Equivalence by Tiling

point in the finally constructed diagram. Hence $W \equiv U \sqcup V$, implying the proposition. $\square$

Now, the residual of a braid after another braid is defined as a function taking as input the (uniquely existing) final diagram obtained by the tiling process.

Definition 57 *Let* $\mathbf{U}$ *and* $\mathbf{V}$ *be braids. Let* $\mathbf{V}'(\mathbf{U}')^{\top}$ *be the tiling-normal form of* $\mathbf{V}^{\top}\mathbf{U}$*. We define*

1. *the* residual of $\mathbf{U}$ after $\mathbf{V}$ *by* $\mathbf{U} \setminus \mathbf{V} = \mathbf{V}'$*,*
2. *the* union of $\mathbf{V}$ and $\mathbf{U}$ *by* $\mathbf{V} \sqcup \mathbf{U} = \mathbf{V}(\mathbf{U} \setminus \mathbf{V})$*, and*
3. $\mathbf{U}$ is contained in $\mathbf{V}$, $\mathbf{U} \sqsubseteq \mathbf{V}$ *by* $\mathbf{U} \setminus \mathbf{V} = o$*.* $\mathbf{U}$ is equivalent to $\mathbf{V}$, $\mathbf{U} \equiv \mathbf{V}$*, if* $\mathbf{V}$ *is contained in* $\mathbf{U}$ *as well.*

Note that the tiling TRS is complete, hence the operations and notions are well-defined. Combined with the correspondence between braid equivalence and permutation equivalence of the preceding subsection, the proposition implies that braiding is orthogonal.

Theorem 58 *Braiding is orthogonal.*

Proof $\setminus$, $\sqcup$, o, and $\sqsubseteq$ have the properties required for orthogonality as described in Subsection 3.3, by the fact that the corresponding properties hold for the corresponding operations on multiderivations. $\square$

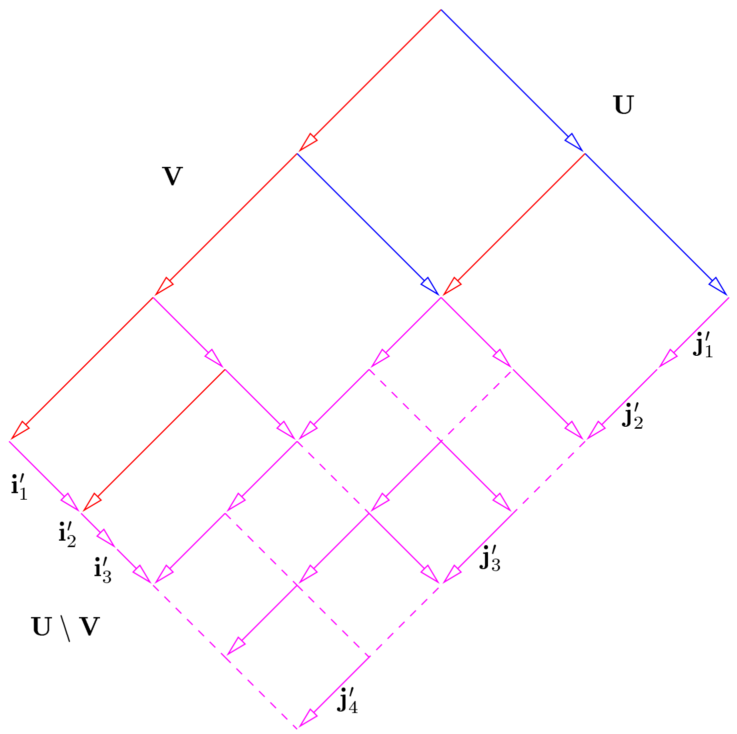


Figure 18: Residual by tiling

Exercise 59 *1. Computing residuals can be formalised by the following residual TRS. The alphabet of the residual TRS is the alphabet of the tiling TRS, extended with binary function symbols A and L, and unary function symbols R, ϵ, and $\epsilon^\top$. The rules of the residual TRS are the rules of the rules od the tiling TRS extended with*

$$\begin{array}{rcl@{\qquad}rcl}
A(x,y) & \to & L(y,R(x)) & \epsilon(\epsilon^\top(x)) & \to & x \\
L(o,y) & \to & \epsilon(y) & R(o) & \to & \epsilon^\top(o) \\
L(\mathbf{i}(x),y) & \to & L(x,\mathbf{i}^\top(y)) & R(\mathbf{i}(y)) & \to & \mathbf{i}(R(y))) \\
\epsilon(\mathbf{i}(x)) & \to & \mathbf{i}(\epsilon(x)) & \mathbf{i}^\top(\epsilon^\top(x)) & \to & \epsilon^\top(x)
\end{array}$$

For braids $\mathbf{U}$ and $\mathbf{V}$ $\mathbf{U} \setminus \mathbf{V}$ is defined to be the residual-normal form of $A(\mathbf{U}, \mathbf{V})$.

Show that the residual TRS does what it name suggest it does.

2. Find braids $\mathbf{U}$ and $\mathbf{V}$ such that tiling results in the diagram in Figure 18. Compute the normal form of $A(\mathbf{U}, \mathbf{V})$ for these braids, using the residual rules.

Orthogonality of braiding expresses that braid equivalence is a congruence relation with respect to the residual operations. We can say more.

Theorem 60 *For arbitrary braids* $\mathbf{U}$, $\mathbf{V}$ *and* $\mathbf{W}$*:*

$$\begin{array}{rclrcl} \mathbf{U}\setminus o & = & \mathbf{U} & o\setminus\mathbf{U} & = & o \\ \mathbf{U}\setminus(\mathbf{V}\mathbf{W}) & = & (\mathbf{U}\setminus\mathbf{V})\setminus\mathbf{W} & (\mathbf{V}\mathbf{W})\setminus\mathbf{U} & = & (\mathbf{V}\setminus\mathbf{U})(\mathbf{W}\setminus(\mathbf{U}\setminus\mathbf{V})) \end{array}$$

Proof We only present the proof of $(\mathbf{V}\mathbf{W})\setminus\mathbf{U} = (\mathbf{V}\setminus\mathbf{U})(\mathbf{W}\setminus(\mathbf{U}\setminus\mathbf{V}))$.

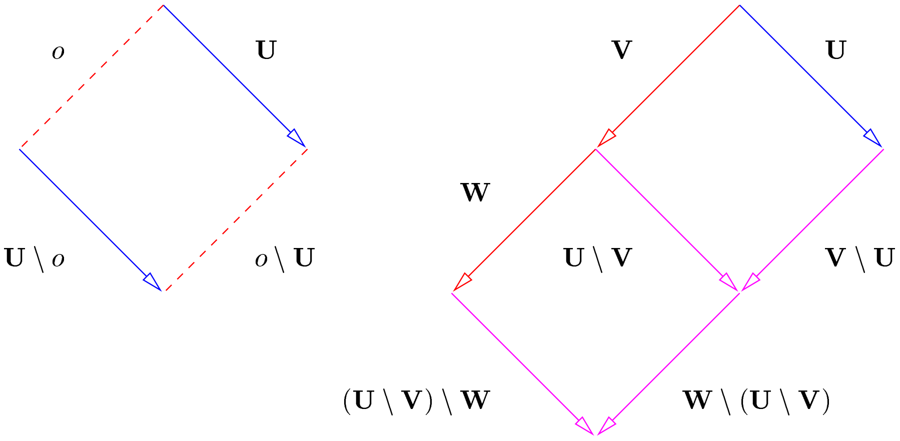


Figure 19: Residual equalities

See Figure 19.

$$\begin{array}{rcl} (\mathbf{V}\mathbf{W})\setminus\mathbf{U} & = & (\mathbf{U}^{\top}(\mathbf{V}\mathbf{W}))\!\downarrow \\ & = & ((\mathbf{U}^{\top}\mathbf{V})\mathbf{W})\!\downarrow \\ & = & (((\mathbf{V}\setminus\mathbf{U})(\mathbf{U}\setminus\mathbf{V})^{\top})\mathbf{W})\!\downarrow \\ & = & (\mathbf{V}\setminus\mathbf{U})(\mathbf{W}\setminus(\mathbf{U}\setminus\mathbf{V})) \end{array}$$

where for the third equation symmetry of elementary diagrams was employed. □

The theorem expresses that computing the residual of a braid after another braid via tiling, does not depend on the way in which either of them is split.

Exercise 61 *1. Formalise the proof of the theorem.*

2. Find three braids such that if the braids are put on the three $3D$ *axes, tiling of the cube 'deadlocks' (i.e. the sides of neighbouring diagrams cannot be made to match).*

The theorem holds for arbitrary orthogonal rewrite systems (having canonical elementary diagrams).

Example 62 *TRSs (and the* λ*-calculus) do not possess canonical elementary diagrams, a priori. For example, consider the TRS with one rule* $D(x) \to$

$x+x$. The residual of $D(1)$ after the rewrite step $D(D(1)) \to D(1)+D(1)$ consists of both $D(1)$-redexes. These can in principle be contracted in arbitrary order, resulting in two (equivalent) elementary diagrams. Of course, we can choose *some fixed order thereby restoring canonicity. [Bar84] chooses to contract redexes from left to right (in the λ-calculus).*

3.7 Confluence by Completion (the sequel)

We've seen in Subsection 3.1 that the subcommufication process terminates for braids having 3 or 4 strands. Here we extend this result to braids having an arbitrary number of strands.

Theorem 63 *Subcommufication of the R rules ends in a confluent rewrite system for braids.*

Proof Theorem 55 and Proposition 56 imply that tiling two developments ends in two braids which are developments. That is, right-hand sides of adjoined rules are always developments. Since developments are finite, and since at any moment there are only finitely many possibilities for applying a crossing (n for a braid having $n+1$ strands), the subcommufication process ends. Confluence follows by Proposition 56. $\Box$

4 Minimality

In the preceding section we have shown braiding to be orthogonal. In particular, we've shown that for arbitrary braids $\mathbf{U}$ and $\mathbf{V}$, their union $\mathbf{U} \sqcup \mathbf{V}$ is a braid extending both. Does there exist a shorter braids extending both $\mathbf{U}$ and $\mathbf{V}$. In this subsection we show that $\mathbf{U} \sqcup \mathbf{V}$ is the shortest common extension (up to equivalence). Consider an arbitrary common extension $\mathbf{U}\ \mathbf{V}' =_E \mathbf{V}\ \mathbf{U}'$ of $\mathbf{U}$ and $\mathbf{V}$. We compute:

$$\begin{aligned}
(\mathbf{U} \setminus \mathbf{V}) \setminus \mathbf{U}' &=_E \mathbf{U} \setminus (\mathbf{V}\ \mathbf{U}') \\
&=_E \mathbf{U} \setminus (\mathbf{U}\ \mathbf{V}') \\
&=_E (\mathbf{U} \setminus \mathbf{U}) \setminus \mathbf{V}' \\
&=_E o \setminus \mathbf{V}' \\
&=_E o
\end{aligned}$$

From this it is easy to deduce that $\mathbf{V}\ \mathbf{U}'$ extends $\mathbf{U} \sqcup \mathbf{V}$:

$$\begin{aligned}
\mathbf{V}\ \mathbf{U}' &=_E \mathbf{V}\ \mathbf{U}'\ o \\
&=_E \mathbf{V}\ \mathbf{U}'\ ((\mathbf{U} \setminus \mathbf{V}) \setminus \mathbf{U}') \\
&=_E \mathbf{V}\ (\mathbf{U}' \sqcup (\mathbf{U} \setminus \mathbf{V})) \\
&=_E \mathbf{V}\ (\mathbf{U} \setminus \mathbf{V})\ (\mathbf{U}' \setminus (\mathbf{U} \setminus \mathbf{V})) \\
&=_E (\mathbf{U} \sqcup \mathbf{V})\ (\mathbf{U}' \setminus (\mathbf{U} \setminus \mathbf{V}))
\end{aligned}$$

Since equivalent braids have the same length, we are done.

Note that, except for the length argument, this computation goes through for arbitrary orthogonal rewrite systems. The following example shows that for TRSs the union operation yields a common extension which is minimal in a somewhat strange way.

Example 64 *Consider the one-rule orthogonal TRS $I(x) \to x$ and the two (different) steps $I(I(x)) \to I(x)$. The union of these steps is $I(I(x)) \mathrel{-\!\!\circ\!\!\rightarrow} x$ where both redexes are contracted simultaneously. Notice that a common reduct ($I(x)$) had been reached already.*

The example shows the existence in term rewriting of so-called *syntactical accidents*; there exist rewrite sequences which differ from each other in an essential way, but which do have the same initial and final term. The difference between braiding and term rewriting is that in case of braiding a rewrite sequence can be reconstructed from the initial and final terms, which is unique up to equivalence. This does not hold true in general, for TRSs as witnessed by the step $I(I(x)) \to I(x)$ in the example. We call a TRS having this reconstruction property *extreme*. Although not all orthogonal TRSs are extreme, every orthogonal TRS can be embedded in an extreme TRS in a natural way, by enriching the TRS with an 'action-stamping' mechanism [Lév78, Mar92, Oos96].

5 The Uniform Wordproblem

The uniform wordproblem for braids, i.e. the question whether two braids are equivalent, is not very interesting from a decidability point of view: equivalent braids consist of the same number of crossings (why?) hence all possibilities can be enumerated, This is not very efficient. Orthogonality of braiding yields an efficient procedure for checking equivalence of braids: $\mathbf{U}$ and $\mathbf{V}$ are equivalent iff $\mathbf{U} \setminus \mathbf{V} = o$ and $\mathbf{V} \setminus \mathbf{U} = o$, i.e. if tiling results in two empty braids.

Exercise 65

1. *Prove decidability of the uniform wordproblem.*
2. *Determine the complexity of checking equivalence both by enumerating all possibilities and by tiling.*

6 Conclusion

Techniques from rewriting theory can be applied to solve every day (non-trivial) problems.

Exercise 66 *Of course, there are countless variations possible on the theme of braiding. One can thank of e.g. (in increasing order of number of generators and axioms, see Figure 20):*

1. *The strands are on a cylinder (the last strand is a neighbour of the first strand) There's an extra generator, $\mathbf{0}$, for expressing a crossing of the first and last strand.*

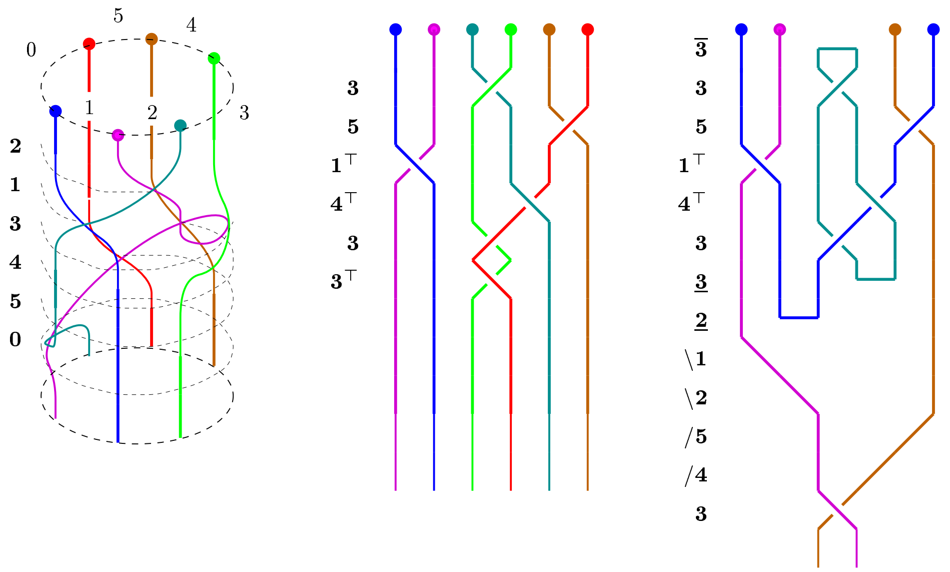


Figure 20: Four variations on braids

2. *Real braids: a crossing can be both 'right over left' as well as 'left over right' Every generator* $\mathbf{i}$ *has an inverse* $\mathbf{i}^{\top}$.
3. *Two neighbouring strands may be joined. There are extra generators* $\bar{\mathbf{i}}$, $\underline{\mathbf{i}}$, $\backslash\mathbf{i}$, *en* $/\mathbf{i}$, *for top, bottom, moving to left, and moving to right, respectively.*
4. *etc.*

Present axioms for these variations, pose interesting problems and solve them.

Most formal methods concentrate on terms. For (an attempt at) two and higher-dimensional rewriting techniques Lafont [Laf92] can be consulted.

References

[Art26] E. Artin. Theorie der Zöpfe. *Hamburger Abhandlungen*, 4:47–72, 1926.

[Art47] E. Artin. Theory of braids. *Annals of Mathematics*, 48(1):101–126, January 1947.

[Bar84] H. P. Barendregt. *The Lambda Calculus, Its Syntax and Semantics*, volume 103 of *Studies in Logic and the Foundations of Mathematics*. North-Holland, Amsterdam, revised edition, 1984.

[Boh47] F. Bohnenblust. The algebraical braid group. *Annals of Mathematics*, 48(1):127–136, January 1947.

[DI] Collegediktaat termherschrijven 96/97, deel I. Vrije Universiteit, Faculteit der Wiskunde en Informatica.

[DII] Collegediktaat termherschrijven 96/97, deel II. Vrije Universiteit, Faculteit der Wiskunde en Informatica.

[Gar69] F.A. Garside. The braid group and other groups. *Quarterly Journal of Mathematics*, 20:235–254, 1969.

[HL91] Gérard Huet and Jean-Jacques Lévy. Computations in orthogonal rewriting systems, I. In Jean-Louis Lassez and Gordon Plotkin, editors, *Computational Logic: Essays in Honor of Alan Robinson*, chapter 11. The MIT Press, 1991.

[Hue94] Gérard Huet. Residual theory in λ-calculus: a formal development. *Journal of Functional Programming*, 4(3):371–394, July 1994.

[Klo80] J. W. Klop. *Combinatory Reduction Systems.* PhD thesis, Rijksuniversiteit Utrecht, June 1980. Mathematical Centre Tracts 127.

[KV] Jan Willem Klop and Roel de Vrijer. A topological proof of confluence by decreasing diagrams. Draft version of July 18, 1996.

[Laf] Yves Lafont. Equational reasoning with 2-dimensional diagrams. Preliminary version of July 29, 1992.

[Laf92] Y. Lafont. Penrose diagrams and 2-dimensional rewriting. In M.P. Fourman, P.T. Johnstone, and A.M. Pitts, editors, *Applications of Categories in Computer Science*, volume 177 of *London Mathematical Society Lecture Notes Series*, pages 191–201. Cambridge University Press, 1992.

[Lév78] Jean-Jacques Lévy. *Réductions correctes et optimales dans le λ-calcul.* Thèse de doctorat d'etat, Université Paris VII, 1978.

[Mar92] Luc Maranget. *La stratégie paresseuse.* Thèse de doctorat, Université Paris VII, 6 Juilliet 1992.

[Mel] Paul-André Melliès. Braids described as an orthogonal rewriting system. Draft version of June 21, 1995.

[Oos94] Vincent van Oostrom. *Confluence for Abstract and Higher-Order Rewriting.* PhD thesis, Vrije Universiteit, Amsterdam, March 1994.

[Oos96] Vincent van Oostrom. Higher-order families. In Harald Ganzinger, editor, *Rewriting Techniques and Applications, 7th International Conference, RTA-96*, volume 1103 of *Lecture Notes in Computer Science*, pages 392–407. Springer, 1996.

[Oos97a] Vincent van Oostrom. Developing developments. *Theoretical Computer Science*, 175(1):159–181, March 1997.

[Oos97b] Vincent van Oostrom. Finite family developments. In Hubert Comon, editor, *Rewriting Techniques and Applications, 8th International Conference, RTA-97*, volume 1232 of *Lecture Notes in Computer Science*, pages 308–322. Springer, 1997.

[SS91] G. Schmidt and T. Ströhlein. *Relations and Graphs - Discrete Mathematics for Computer Scientists.* EATCS Monographs on Theoretical Computer Science. Springer-Verlag, 1991.

[Tak95] Masako Takahashi. Parallel reductions in λ-calculus. *Information and Computation*, 118:120–127, 1995.

[Zan95] Hans Zantema, 1995. Email to the TeReSe mailing-list.