Proof Orders for Decreasing Diagrams

Bertram Felgenhauer[1] and Vincent van Oostrom[2]

1 **Institute for Computer Science, University of Innsbruck**
`bertram.felgenhauer@uibk.ac.at`
2 **Department of Philosophy, Utrecht University**
`Vincent.vanOostrom@phil.uu.nl`

Abstract

We present and compare some well-founded proof orders for decreasing diagrams. These proof orders order a conversion above another conversion if the latter is obtained by filling any peak in the former by a (locally) decreasing diagram. Therefore each such proof order entails the decreasing diagrams technique for proving confluence. The proof orders differ with respect to monotonicity and complexity. Our results are developed in the setting of involutive monoids. We extend these results to obtain a decreasing diagrams technique for confluence modulo.

1998 ACM Subject Classification F.4 Mathematical Logic and Formal Languages

Keywords and phrases involutive monoid, confluence modulo, decreasing diagram, proof order

Digital Object Identifier 10.4230/LIPIcs.RTA.2013.174

1 Introduction

In this paper we revisit the decreasing diagrams technique [10] for proving confluence. We exhibit several well-founded orders on proofs that allow us to prove termination of the proof transformation system defined by the locally decreasing diagrams. A similar approach is used in the correctness proof for completion by Bachmair and Dershowitz [2]. Rather than working on proofs directly, we develop our orders in the setting of involutive monoids, which capture the essential structure of proofs—proofs may be concatenated and reversed.

This work is partly inspired by [5], where a well-founded order on proofs is defined in order to establish that local decreasingness implies confluence. In [4], a simplified version of this proof order is defined. The orders presented here are much simpler.

The remainder of this paper is structured as follows: In Section 2 we introduce basic notions used in our paper. Section 3 presents involutive monoids. In Section 4 we develop orders on so-called French strings that entail the decreasing diagrams technique. Then, in Section 5, we extend our approach to the Church–Rosser modulo property, using an extension of French strings that we call Greek strings, leading to a generalisation of a results by Ohlebusch [8] and Jouannaud and Liu [4]. Finally, we conclude in Section 6.

Throughout we illustrate our constructions by means of the following running example.

▸ **Example 1.** The rewrite relation $\to$ on objects $\{a,\dots,j\}$ as presented on the left in Figure 1 is the union of the family of rewrite relations $(\underset{\ell}{\to})_{\ell\in L}$ on its right, indexed by concrete labels $L = \{\ell, m, \kappa\}$ and having individual rewrite relations:

$$\underset{\kappa}{\to} = \{(b,c),(j,i)\}$$

$$\underset{\ell}{\to} = \{(d,c),(f,a),(f,h),(g,e),(h,a),(e,j)\}$$

$$\underset{m}{\to} = \{(b,a),(d,e),(c,f),(c,g),(g,i),(a,i),(h,i)\}$$

24th International Conference on Rewriting Techniques and Applications (RTA'13).
Editor: Femke van Raamsdonk; pp. 174–189
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

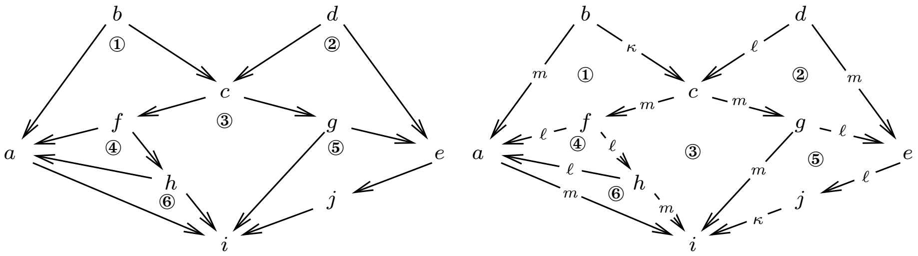
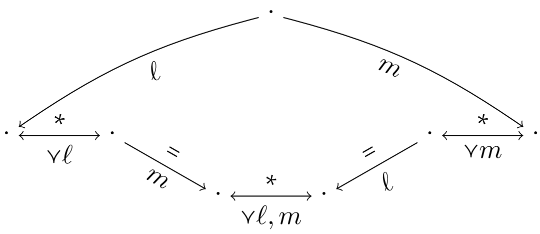


Figure 1 Decomposing a rewrite relation (left) into a family of such (right).



$\acute{\ell}\grave{m}$

$\{\ell\succ\}[\grave{m}]\{\ell,m\succ\}[\acute{\ell}]\{m\succ\}$

Figure 2 Locally decreasing diagram (left). Interpretations of peak and joining conversion (right).

We will show how each of the transformation steps, indicated by the numbers, leading from the initial conversion $a \underset{m}{\longleftarrow} b \underset{\kappa}{\rightarrow} c \underset{\ell}{\leftarrow} d \underset{m}{\longrightarrow} e$ to the final valley $a \underset{m}{\longrightarrow} i \underset{\kappa}{\leftarrow} j \underset{\ell}{\leftarrow} e$ entails a decrease in each of our proof orders, which are based on some well-founded order $\succ$ on L.

2 Preliminaries

We use standard notions of term rewriting. For a comprehensive overview, see [9].

We use arrow-like notations like $\rightarrow$ for rewrite relations, i.e. binary relations on a set (also called abstract rewrite systems), and symmetric notations like $\vdash\!\dashv$ for symmetric rewrite relations. The inverse of $\rightarrow$, its reflexive closure, transitive closure, reflexive–transitive closure, and its n-th power of $\rightarrow$ are denoted by $\leftarrow$, $\xrightarrow{=}$, $\xrightarrow{+}$, $\xrightarrow{*}$, and $\xrightarrow{n}$ respectively. In particular, $\xrightarrow{0}$ is the identity relation. If $(\underset{\ell}{\rightarrow})_{\ell\in L}$ is a family of rewrite relations and $M \subseteq L$, we let $\underset{M}{\longrightarrow} = \bigcup_{\ell\in M} \underset{\ell}{\rightarrow}$.

Given an alphabet L of labels endowed with a well-founded order (precedence) $\succ$, we define $\curlyvee\ell = \{\kappa \in L \mid \ell \succ \kappa\}$ and $\curlyvee\ell, m = \curlyvee\ell \cup \curlyvee m$. The gist of the decreasing diagrams technique [10] is that to show that a rewrite relation is confluent, we can decompose it into an L-indexed family of rewrite relation $(\underset{\ell}{\rightarrow})_{\ell\in L}$. Then, if every local peak $u \underset{\ell}{\leftarrow} \cdot \underset{m}{\longrightarrow} v$ can be joined decreasingly, that is, there is a joining conversion $u \underset{\curlyvee\ell}{\overset{*}{\longleftrightarrow}} \cdot \underset{m}{\overset{=}{\longrightarrow}} \cdot \underset{\curlyvee\ell,m}{\overset{*}{\longleftrightarrow}} \cdot \underset{\ell}{\overset{=}{\longleftarrow}} \cdot \underset{\curlyvee m}{\overset{*}{\longleftrightarrow}} v$ (see Figure 2, left), the relation $\underset{L}{\rightarrow}$ is confluent.

Throughout we assume $\succ$ is a well-founded partial order on the labels L.

Rewriting modulo is concerned with pairs of relations $\rightarrow$ and $\vdash\!\dashv$, where $\vdash\!\dashv$ is symmetric. Let $\Leftrightarrow = \leftrightarrow \cup \vdash\!\dashv$. We say that $\rightarrow$ is Church–Rosser modulo $\vdash\!\dashv$ iff $\overset{*}{\Leftrightarrow} \subseteq \overset{*}{\rightarrow} \cdot \overset{*}{\vdash\!\dashv} \cdot \overset{*}{\leftarrow}$. In order to apply the decreasing diagrams technique, we distinguish between local peaks $\leftarrow \cdot \rightarrow$ and local cliffs $\leftarrow \cdot \vdash\!\dashv$ or $\vdash\!\dashv \cdot \rightarrow$. (There are other notions of confluence for rewriting modulo. See [8] for a systematic discussion.)

$$\frac{t \to u}{t = u}\ (\text{step}) \qquad \frac{}{t = t}\ (\text{reflexive}) \qquad \frac{u = t}{t = u}\ (\text{symmetric}) \qquad \frac{t = u \quad u = v}{t = v}\ (\text{transitive})$$

Figure 3 Equational logic for rewrite relations.

$$\cfrac{\cfrac{t = u \quad u = v}{t = v} \quad v = w}{t = w} \xRightarrow{\text{assoc}} \cfrac{t = u \quad \cfrac{u = v \quad v = w}{u = w}}{t = w} \qquad \cfrac{\cfrac{t = u \quad u = v}{t = v}}{v = t} \xRightarrow[\text{automorph}]{\text{anti-}} \cfrac{\cfrac{u = v}{v = u} \quad \cfrac{t = u}{u = t}}{v = t}$$

$$\cfrac{t = u \quad \cfrac{}{u = u}}{t = u} \xRightarrow{\text{right id}} t = u \qquad \cfrac{\cfrac{}{t = t} \quad t = u}{t = u} \xRightarrow{\text{left id}} t = u \qquad \cfrac{\cfrac{t = u}{u = t}}{t = u} \xRightarrow{\text{invol}} t = u \qquad \cfrac{\cfrac{}{t = t}}{t = t} \xRightarrow{\text{inv id}} \cfrac{}{t = t}$$

Figure 4 Normalising equational logic proofs into conversions.

3 Involutive monoids

A conversion $t \overset{*}{\leftrightarrow} u$ for a rewrite relation $\to$ is a witness to a proof that t is equal to u in the equational logic induced by $\to$, see Figure 3.

▸ Remark. Because of the absence of term structure the equational logic is particularly simple: terms t,u,v are constants and the usual substitution and congruence rules are superfluous.

However, conversions correspond only to a subset of the equational logic proofs. For example, in a conversion symmetry is never applied below transitivity. In general, conversions can be identified with equational logic proofs that are in normal form with respect to the transformations in Figure 4.[1] Since these transformations are confluent and terminating, every equational logic proof can be transformed into a conversion so one may restrict attention to the latter, a result known as logicality of rewriting with respect to equational logic.

Involutive monoids, see e.g. [3], are the natural algebraic structure to interpret such equational proofs *and* their transformations. In a slogan: involutive monoids are to conversions what monoids are to reductions.[2] More precisely, involutive monoids are obtained by abstracting the equalities into primitives a,b,c,..., interpreting transitivity as composition $(\cdot)$, symmetry as inversion (-1), reflexivity as identity (e), and equipping these with the laws in Definition 2 corresponding to the transformations of Figure 4.

▸ **Definition 2.** A *monoid* is a (*carrier*) set endowed with an associative binary operation $(\cdot)$ and an identity element (e). An *involutive* monoid is a monoid endowed with an anti-automorphic involution (-1), i.e. satisfying the following laws:[3]

$$\begin{array}{rcll rcll}
(a \cdot b) \cdot c & = & a \cdot (b \cdot c) & (\text{associative}) & (a \cdot b)^{-1} & = & b^{-1} \cdot a^{-1} & (\text{anti-automorphic}) \\
a \cdot e & = & a & (\text{right identity}) & (a^{-1})^{-1} & = & a & (\text{involutive}) \\
e \cdot a & = & a & (\text{left identity}) & e^{-1} & = & e & (\text{inverse identity})
\end{array}$$

Involutive monoids are the main algebraic structure into which conversions and transformations on them will be interpreted, in this paper. This will be the topic of the next section. We

[1] Reductions can be identified with proofs of rewrite logic in normal form.
[2] For *term* rewriting the involutive monoid is to be extended with operations corresponding to the function symbols and laws for them yielding (equational) proof term algebras.
[3] $e^{-1} = e$ is superfluous as it is derivable: $e^{-1} = e \cdot e^{-1} = (e^{-1})^{-1} \cdot e^{-1} = (e \cdot e^{-1})^{-1} = (e^{-1})^{-1} = e$.

now illustrate involutive monoids first by some (mostly well-known) examples from algebra to be used later, and next by our main example, the involutive monoid of French strings.

▸ **Example 3.** (i) The integers with addition, zero, and unary minus $(\mathbb{Z}, +, 0, -)$ constitute an involutive monoid. In general, any group constitutes an involutive monoid;

(ii) The monoid of natural numbers with addition and zero $(\mathbb{N}, +, 0)$ constitute an involutive monoid when endowed with the identity map, as do the multisets over L with multiset sum and the empty multiset $([L], \uplus, [])$. Commutative monoids give rise to involutive monoids in this way;

(iii) (Ordinary) strings over an alphabet L of *labels* or *letters* ℓ, endowed with juxtaposition, the empty string ε, and string reversal constitute an involutive monoid.

(iv) Natural number pairs with pointwise addition, the pair $(0,0)$, and swapping constitute an involutive monoid. In fact, any monoid $(A, \cdot, e)$ gives rise to an involutive monoid on $A \times A$ by endowing it with pointwise composition, the pair (e, e), and swapping;

(v) Natural number triples endowed with $\cdot$ defined by

$$(n_1, m_1, k_1) \cdot (n_2, m_2, k_2) = (n_1 + n_2, m_1 + k_1 \cdot n_2 + m_2, k_1 + k_2)$$

zero $(0,0,0)$, and $(n, m, k)^{-1} = (k, m, n)$, constitute an involutive monoid. In fact, we will only employ triples such that the middle component does not exceed the product of the other components. Such triples can be given a geometric interpretation as diagrams, as illustrated in Figure 5 right, and for this reason we will refer to them as *area* triples.

Our interpretations of conversions with respect to a family $(\underset{\ell}{\to})_{\ell \in L}$ of rewrite relations indexed by labels in L, will all factor through an interpretation (see Definition 8) that only keeps the labels, equipping them with accents according to the direction (forward or backward) of the individual steps in the conversion. We call such strings of accented labels French strings.[4]

▸ **Definition 4.** For a given alphabet L, let a *French* letter be an accented (grave $\grave{\ell}$ or acute $\acute{\ell}$) letter. We will use the circumflex as in $\hat{\ell}$ to denote a French letter having ℓ as label and carrying either a grave or acute accent. The set $\widehat{L}$ of *French* strings over L, i.e. strings of French letters, endowed with juxtaposition, the empty string, and mirroring -1 given by $\grave{\ell}^{-1} = \acute{\ell}$ and $\acute{\ell}^{-1} = \grave{\ell}$, constitute an involutive monoid. The order $>$ on labels is extended to French letters: we let $\hat{\ell} > \hat{m}$ and $\ell > \hat{m}$ iff $\ell > m$.

For instance, mirroring the French string $\acute{m}\grave{k}\acute{\ell}\grave{m}$ over the alphabet of Example 1 yields $\acute{m}\grave{\ell}\acute{k}\grave{m}$. In case the alphabet is a singleton set, the French letters over the alphabet are identified with the accents, denoted by $\diagdown$ and $\diagup$. French strings (of accents) can be given a geometric interpretation as diagrams, as illustrated in Figure 5 left (middle). French strings are to involutive monoids what (ordinary) strings are to monoids. To make this precise, we need the standard notion of a homomorphism as a structure preserving map.

▸ **Definition 5.** A *homomorphism* from the involutive monoid $(A, \cdot, e, -1)$ to the involutive monoid $(B, \cdot', e', -1')$ is a map h from A to B such that for all a, b, c in A, $h(a \cdot b) = h(a) \cdot' h(b)$, $h(e) = e'$, and $h(a^{-1}) = h(a)^{-1'}$. The homomorphism is an *isomorphism* if there exists a homomorphism that is inverse to it.

---

[4] Meta-footnote: Our naming is tentative. We are open to any suggestion that clearly distinguishes what we call French letters/strings/terms from ordinary ones. We do however insist on using accents because of their intuitive relationship to the geometric representation of conversions as is standard in rewriting since the 1930s (Church–Rosser, Newman), see Figure 5.

▸ **Proposition 6.** *The involutive monoid on French strings $\widehat{L}$ is the free involutive monoid over L. That is, any map from L into the carrier of some involutive monoid, extends, via the map $\ell \mapsto \grave{\ell}$, uniquely to an involutive monoid homomorphism on $\widehat{L}$.*

This is a well-known fact and moreover easy to show. It is implicit in the old proofs of logicality of rewriting for the special case of (abstract) rewrite relations as noted above (recapitulated in Appendix A) and explicitly proven in e.g. [3, Proposition 2].

We conclude this section by giving some examples of homomorphisms linking up the various involutive monoids presented above. These homomorphisms are auxiliary to and illustrative of (see Figure 5) our subsequent constructions of proof orders.

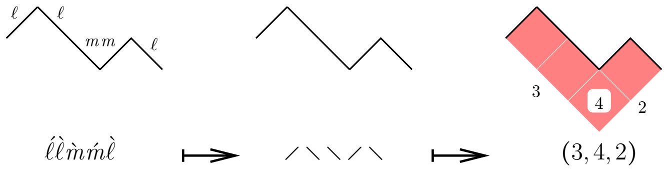


Figure 5 Mapping French strings via strings of accents into area triples.

▸ **Example 7.** (i) Mapping a French string over L to the natural number pair of grave, acute accents in it, is a homomorphism. In turn, mapping a natural number pair to its sum is also a homomorphism. Their composition maps a French string to its *length*, e.g. $\acute{\ell}\grave{\ell}\grave{m}\acute{m}\grave{\ell} \mapsto (3,2) \mapsto 5$.

(ii) Mapping a French string over L to an ordinary string over L by forgetting accents, is a homomorphism. In turn, mapping a string over L to the multiset of letters in it is also a homomorphism. Their composition maps a French string to its *multiset*, e.g. $\acute{\ell}\grave{\ell}\grave{m}\acute{m}\grave{\ell} \mapsto \ell\ell mm\ell \mapsto [\ell,\ell,\ell,m,m]$.

(iii) Mapping a French string over L to the French string of its accents by forgetting the letters is a homomorphism. In turn, mapping the accent $\diagdown$ to the area triple $(1,0,0)$ induces a (unique) homomorphism from French strings over accents to area triples. Their composition maps a French string to its *area*, e.g. $\acute{\ell}\grave{\ell}\grave{m}\acute{m}\grave{\ell} \mapsto \diagup\diagdown\diagdown\diagup\diagdown \mapsto (3,4,2)$, see Figure 5.

4 Proof orders and confluence

In this section we present two novel proof orders, i.e. well-founded orders on proofs in equational logic, factoring these through their interpretation into the French string of their (accented) labels. They are shown both to be proof orders for decreasing diagrams, yielding alternative proofs showing that a locally decreasing rewrite relation is confluent. Both proof orders are flexible, in a sense to be explained in the next section.

4.1 Proof orders via French strings

A proof order is a well-founded order on conversions, i.e. on proofs in equational logic. Proof orders can be generated by proof rewrite systems as introduced in the context of completion by Bachmair and Dershowitz [2]. The objects of a proof rewrite system are conversions and its rewrite steps allow one to replace a subproof, i.e. a conversion between two terms, occurring in it by another such conversion between the same two terms.[5] The idea is to

[5] As before, we deal here only with the special case where the terms are constants.

stepwise transform proofs into simpler ones, the usual goal being to obtain a valley proof (sometimes called a rewrite proof), i.e. a pair of reductions from the source and target of the original conversion, to a common reduct. Here, we adapt these ideas by factoring through an interpretation into the involutive monoid of French strings, the advantage being that they can easily be dealt with algebraically.

▸ **Definition 8.** The *interpretation* of a conversion for an L-indexed $(\underset{\ell}{\to})_{\ell \in L}$ family of rewrite relations, is the French string over L that is the stepwise juxtaposition of the labels in the conversion, where a label carries a grave (acute) accent in case the corresponding step in the conversion is a forward (backward) step.

▸ **Example 9.** The successive conversions of Example 1 are interpreted as the successive French strings in the following transformation, where we have underlined in each step the substring being replaced:

$$\underline{\acute{m}\grave{k}}\acute{\ell}\grave{m} \Rightarrow_{①} \acute{\ell}\acute{m}\underline{\acute{\ell}\grave{m}} \Rightarrow_{②} \acute{\ell}\underline{\acute{m}\grave{m}}\grave{\ell} \Rightarrow_{③} \underline{\acute{\ell}\grave{\ell}}\grave{m}\acute{m}\grave{\ell} \Rightarrow_{④} \acute{\ell}\grave{m}\underline{\acute{m}\grave{\ell}} \Rightarrow_{⑤} \underline{\acute{\ell}\grave{m}}\acute{k}\acute{\ell} \Rightarrow_{⑥} \grave{m}\acute{k}\acute{\ell}$$

Equipping French strings with a well-founded order or with a terminating (French string) rewrite system, gives rise to a proof order, via this interpretation. Among the well-founded orders on French strings, the monotonic ones are of special interest.

▸ **Definition 10.** A *well-founded* involutive monoid is an involutive monoid endowed with a well-founded order $\gg$ on its carrier. It is *monotonic* if the algebraic operations are so with respect to the order, that is, all French string s, t, p satisfy:

1. if $s \gg t$ then $ps \gg pt$ and $sp \gg tp$.
2. if $s \gg t$ then $s^{-1} \gg t^{-1}$

▸ **Theorem 11.** *Let $>$ be a well-founded order on L and let the French strings endowed with $\gg$ be a well-founded involutive monoid. Then if for all labels $\ell, m \in L$ and French strings s, r over L (only over $\varnothing$ if $\gg$ is monotonic, i.e. then $s = r = \varepsilon$): $\gg$ is monotonic):*

$$s\acute{\ell}\grave{m}r \gg s\{\ell{>}\}[\grave{m}]\{\ell, m{>}\}[\acute{\ell}]\{m{>}\}r$$

and $(\underset{\ell}{\to})_{\ell \in L}$ is locally decreasing, then $\underset{L}{\to}$ has the Church–Rosser property.

In the statement of the theorem we have employed the EBNF notations [ ] and { } to express option and arbitrary repetition respectively, and used $\vec{\ell}{>}$ to denote a French letter to which (at least) one letter in the vector $\vec{\ell}$ $>$-relates. For instance, $[\grave{m}]$ denotes either ε or $\grave{m}$, and $\{\ell{>}\}$ denotes an arbitrary French string of letters to which ℓ $>$-relates.

Proof. It suffices to show that any conversion between two objects a and b that is not yet a valley, can be transformed into another conversion between a and b that is more like a valley w.r.t. some well-founded order. If a conversion is not yet a valley, then it contains some local peak, say with interpretation $\acute{\ell}\grave{m}$. By the assumption that the rewrite relation is locally decreasing, the local peak can be transformed into a conversion having interpretation of shape $\{\ell{>}\}[\grave{m}]\{\ell, m{>}\}[\acute{\ell}]\{m{>}\}$, see Figure 2, right. Using the assumption that $s\acute{\ell}\grave{m}r \gg s\{\ell{>}\}[\grave{m}]\{\ell, m{>}\}[\acute{\ell}]\{m{>}\}r$ and well-foundedness of $\gg$, eventually a conversion without local peaks, i.e. a valley proof, is obtained.
If $\gg$ is monotonic, then the comparison for $s = r = \varepsilon$ extends to arbitrary s,r immediately. ◂

A well-founded order satisfying the (displayed) condition of the theorem is called a well-founded involutive monoid *for decreasing diagrams*. The two well-founded involutive monoids for decreasing diagrams to be presented below are obtained via further homomorphisms of the French strings into well-founded involutive monoids. The first one is not monotonic but has 'small' images, whereas the second one is monotonic but has 'large' images.

4.2 An lpo-based order

In this section we turn the involutive monoid of French strings into a well-founded one by showing that it is isomorphic to a set of terms, that we therefore call French terms, and equipping the latter with a certain lexicographic path order. We then show that the resulting monoid is a well-founded involutive monoid for decreasing diagrams.

The simple observation at the basis of our term representation is that when filling in a locally decreasing diagram the multiset (or area) of the French string of *maximal* labels can never increase; labels in the local peak of a locally decreasing diagrams can only cause *smaller* ones to appear in the joining conversion.[6] Accordingly, we recursively stratify a French string into a term having the (French string of its) maximal labels as its head, with the term being of finite height due to the assumed well-foundedness of the order on the labels.

▸ **Definition 12.** The *French* term signature over L is denoted by $L^{\sharp}_{\succ}$ and comprises the French strings over L that have $\succ$-incomparable letters, assigning arity zero to ε and to other strings their length plus one. A *French* term over L is a term over $L^{\sharp}_{\succ}$ such that each function symbol s occurring in it is related to its ancestor function symbol, say r, by the *Hoare* order for $\succ$, i.e. for each French letter $\hat{\ell}$ in s, there exists a French letter $\hat{m}$ in r such that $m \succ \ell$.

If $\succ$ is the empty relation then the signature comprises all French strings and terms are flat, i.e. have only ε as proper subterms. If on the other hand $\succ$ is total then the signature comprises strings over a single label and the height of a term is the number of distinct labels.

▸ **Example 13.** Well-foundedly ordering the set L of labels of Example 9 as $m \succ \ell, \kappa$, some examples of French terms over L are

$$\acute{m}\grave{m}(\varepsilon, \grave{\kappa}\acute{\ell}(\varepsilon,\varepsilon,\varepsilon), \varepsilon) \qquad \grave{m}\acute{m}(\acute{\ell}\grave{\ell}(\varepsilon,\varepsilon,\varepsilon), \varepsilon, \grave{\ell}(\varepsilon,\varepsilon)) \qquad \grave{m}(\varepsilon, \acute{\kappa}\acute{\ell}(\varepsilon,\varepsilon,\varepsilon))$$

▸ **Lemma 14.** *The inorder-traversal map* $\flat$ flattening *French terms over L into French strings over L, defined inductively by* $\varepsilon^{\flat} = \varepsilon$ *and* $(\hat{\ell}_1 \dots \hat{\ell}_n(s_0, \dots, s_n))^{\flat} = t_0^{\flat}\hat{\ell}_1 s_1^{\flat} \dots \hat{\ell}_n s_n^{\flat}$*, is a bijection.*

Proof. Let the *stratification* map[7] from French strings over L to French terms over L be inductively defined by setting $\varepsilon^{\sharp} = \varepsilon$ and $(s_0\hat{\ell}_1 \dots \hat{\ell}_n s_n)^{\sharp} = \hat{\ell}_1 \dots \hat{\ell}_n(s_0^{\sharp}, \dots, s_n^{\sharp})$ with $n > 0$ and the $\hat{\ell}_i$ all occurrences of $\succ$-maximal French letters in the string. We claim that flattening $\flat$ and stratification $\sharp$ are each other's inverse.

That $\flat \circ \sharp$ is the identity is shown by induction on the length of French strings.

That $\sharp \circ \flat$ is the identity is shown by induction on French terms, using that all function symbols in the direct subterms of a French term are related in the Hoare order to the head. ◂

The images of flattening and stratification are *small*; linear in the size of their input.

▸ **Example 15.** Flattening the terms given in Example 13 yields the French strings $\acute{m}\grave{\kappa}\acute{\ell}\grave{m}$, $\acute{\ell}\grave{\ell}\grave{m}\acute{m}\grave{\ell}$, and $\grave{m}\acute{\kappa}\acute{\ell}$ and stratifying them with respect to $\succ$ yields the original French terms again. These are the interpretations of the first, fourth, and last conversion in Example 1.

---

[6] Forgetting in a first approximation all non-maximal steps while trying to prove confluence by repeatedly filling in locally decreasing diagrams, the diagrams are simply the (square) ones appearing in a diagrammatic proof of the Lemma of Hindley–Rosen. Only at further approximations the non-maximal labels will play a role analogous to the situation in a diagrammatic proof of Newmans's Lemma.

[7] The idea of the stratification map $\sharp$ is a special case of that of the `maxsplit` method/function found in programming languages such as Java/Python.

By the lemma, the French terms over L are (isomorphic to) the free involutive monoid over L, when endowed with the operations on French strings via the bijection, e.g. $t \cdot u = (t^\flat u^\flat)^\sharp$.

▸ **Definition 16.** Let $\succ$ be the relation on the French term signature $L^\sharp_\succ$ defined by interpreting each function symbol, i.e. French string, in $L^\sharp_\succ$ as the pair consisting of its multiset and the middle component of the area (see Example 7), relating these by the lexicographic product of the multiset-extension $\succ_{mul}$ of $\succ$ and the greater-than relation $>$.

We endow French terms with the order $\succ_{ilpo}$ defined as the iterative lexicographic path order [6, Definition 2] induced by the relation $\succ$, where argument places are ordered *lexicographically* by choosing an arbitrary but fixed total order on them *compatible* with the accents, that is, if $\hat{\ell}_{i+1}$ of the $n+1$-ary function symbol $\hat{\ell}_1 \dots \hat{\ell}_n$ has a grave (acute) accent, then the i^{th} argument place of the symbol comes lexicographically before (after) the $i+1^{st}$.[8] For French strings s,t we define $s \succ_{ilpo} t$ as $s^\sharp \succ_{ilpo} t^\sharp$, lifting the strings to French terms first.

▸ **Example 17.** We have $\grave{\kappa}\acute{\ell} \succ \grave{\ell}$ since the multiset $[\ell,\kappa]$ of the former is $\succ_{mul}$-related to the multiset $[\ell]$ of the latter; we have $\acute{\ell}\grave{\ell} \succ \grave{\ell}\acute{\ell}$ since although both have the same multiset $[\ell,\ell]$, the middle component of the area of the former (1) is greater than that of the latter (0).

There are two possible ways to order the argument places of the ternary function symbol $\grave{\kappa}\acute{\ell}$ but the accents dictate that in either case argument place 1 should come after argument places 0 and 2. Similarly, there are two possible ways to order the argument places of $\acute{\ell}\grave{\ell}$ but now 1 should come before the others.

The sequence of transformation steps of Example 9 yields a $\succ_{ilpo}$-sequence:

$$
\begin{array}{lll}
\acute{m}\grave{m}(\varepsilon, \grave{\kappa}\acute{\ell}(\varepsilon,\varepsilon,\varepsilon), \varepsilon) & \succ_{ilpo} ① & \text{decrease of multiset at position 1} \\
\acute{m}\grave{m}(\acute{\ell}(\varepsilon,\varepsilon), \acute{\ell}(\varepsilon,\varepsilon), \varepsilon) & \succ_{ilpo} ② & \text{decrease of multiset at position 1} \\
\acute{m}\grave{m}(\acute{\ell}(\varepsilon,\varepsilon), \varepsilon, \grave{\ell}(\varepsilon,\varepsilon)) & \succ_{ilpo} ③ & \text{decrease of area at the root} \\
\grave{m}\acute{m}(\acute{\ell}\grave{\ell}(\varepsilon,\varepsilon,\varepsilon), \varepsilon, \grave{\ell}(\varepsilon,\varepsilon)) & \succ_{ilpo} ④ & \text{decrease of multiset at position 0} \\
\grave{m}\acute{m}(\acute{\ell}(\varepsilon,\varepsilon), \varepsilon, \grave{\ell}(\varepsilon,\varepsilon)) & \succ_{ilpo} ⑤ & \text{decrease of multiset at the root} \\
\grave{m}(\acute{\ell}(\varepsilon,\varepsilon), \acute{\kappa}\acute{\ell}(\varepsilon,\varepsilon,\varepsilon)) & \succ_{ilpo} ⑥ & \text{decrease of multiset at position 0} \\
\grave{m}(\varepsilon, \acute{\kappa}\acute{\ell}(\varepsilon,\varepsilon,\varepsilon)) & &
\end{array}
$$

Note that in the $\succ_{ilpo}$①-step the subterm at position 0 *increases*, but this is not harmful since it comes lexicographically *after* the subterm at position 1 which *decreases*.

▸ **Lemma 18.** *For all labels ℓ,m in L and all French strings s,r over L:*

- $s\hat{\ell}r \succ_{ilpo} s\{\ell\succ\}r$; *and*
- $s\acute{\ell}\grave{m}r \succ_{ilpo} s\{\ell\succ\}[\grave{m}]\{\ell,m\succ\}[\acute{\ell}]\{m\succ\}r$

Proof. Both items are proved by induction on the length of sr.

- We distinguish cases on whether or not ℓ is $\succ$-maximal in $s\hat{\ell}r$:

  (yes) in this case one occurrence in ℓ in the head symbol of the lifted lhs $(s\hat{\ell}r)^\sharp$ is replaced by smaller (w.r.t. $\succ$) labels in the head symbol of the lifted rhs, so the lhs' head symbol $\succ$-relates to the rhs' head symbol, and therefore to all rhs function symbols;

  (no) then we conclude by the induction hypothesis for the substring/term $\hat{\ell}$ is in.

- We distinguish cases on whether or not ℓ, m are $\succ$-maximal in $s\acute{\ell}\grave{m}r$, where $\succ$-maximal labels are coloured blue and non-$\succ$-maximal labels are coloured red:

[8] The chosen order affects $\succ$, but not its compatibility with decreasing diagrams. Argument places can be totally ordered by successively taking the leftmost argument place as allowed by the accents.

(both are) then the head symbol of the lhs $\succ$-relates to the head symbol of the rhs, because the multiset (or else the area) has become smaller, and we conclude as in the (yes)-case above, see Figure 6, left;

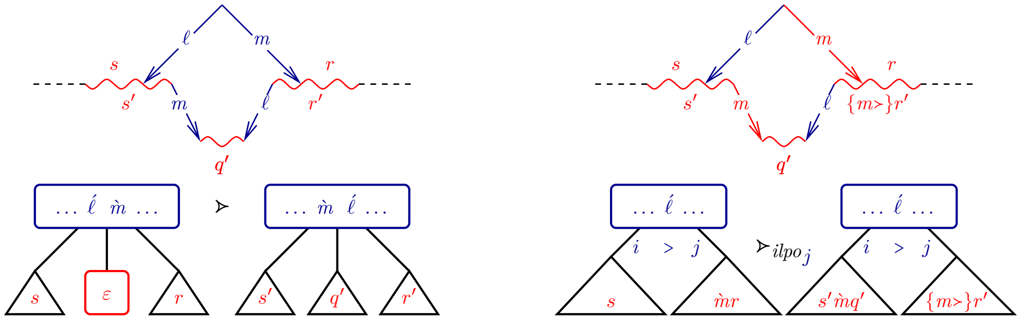


Figure 6 (both,left) Area decrease. (one,right) Lexicographic decrease; jth before ith.

(only $\acute{\ell}$ is) then the substring/term to the right of $\acute{\ell}$ in the lhs $\succ_{ilpo}$-relates to the substring/term to the right of $\acute{\ell}$ in the rhs, using the first item of this lemma, see Figure 6, right;

(only $\grave{m}$ is) as in the previous item but for the substrings/terms to the left of $\grave{m}$;

(neither is) then we conclude by the induction hypothesis for the substring/term the displayed $\acute{\ell}\grave{m}$ is in. ◂

Thus we obtain the main result of this section that French strings endowed with $\succ_{ilpo}$ (via the isomorphism) constitute a well-founded involutive monoid for decreasing diagrams.

Observe that $\succ_{ilpo}$ is *not* monotonic. For instance, composing ╲ to the right of ╲╱╱╱╲ and ╱╲╲╲╲ *reverses* the way in which they are ordered by $\succ_{ilpo}$. Moreover, $\succ_{ilpo}$ is not preserved when extending the relation $>$. Extending the empty order to $m > \ell, \kappa$ *reverses* the way in which $\acute{\ell}\acute{\kappa}\acute{m}$ and $\acute{m}\acute{\kappa}$ are ordered by $\succ_{ilpo}$. Both are overcome by the order introduced in the next section.

▸ Remark. It is possible to overcome non-monotonicity also within the present set-up, the main idea being to quantify over all possible well-orders extending $>$ when comparing. More precisely, define the order $\ggg$ on the French term signature $L^{\sharp}_{>}$ analogous to how $\succ$ was defined in Definition 16, but taking as second component the whole area triple (instead of just its middle component), and comparing these area triples lexicographically on first the pair comprising its first,last component, and then the middle component, with respect to the greater-than (product) order $>$ on the natural numbers. We then define $s \ggg r$ to hold if for all well-orders $>'$ extending $>$ it holds $s \ggg'_{ilpo} r$, where $\ggg'_{ilpo}$ is the iterative lexicographic path order induced by the order $\ggg'$ on $L^{\sharp}_{>'}$, which is in turn induced by the extension $>'$ of $>$. Apart from that the lexicographic order on the argument places should respect the accents as in Definition 16, we now require it to be preserved under concatenation of French strings.

4.3 A monotonic order

▸ **Definition 19.** Let L be an alphabet with precedence $>$. We denote by $\gg_{mul}$ and $(\gg_1, \gg_2)_{lex}$ the multiset extension of $\gg$ and the lexicographic product of $\gg_1$ and $\gg_2$, respectively. The order $\gg_\bullet$ on French strings is defined recursively as follows: $s \gg_\bullet t$ iff

$$\langle s \rangle^f \; ((>, \gg_\bullet)_{lex})_{mul} \; \langle t \rangle^f$$

where $\langle s\rangle^f = [(\acute{\ell}, q) \mid s = p\acute{\ell}q] \cup [(\grave{\ell}, p) \mid s = p\grave{\ell}q]$ collects acute letters together with their suffix in s and grave letters together with their prefix in s into a multiset, and $\succ$ on French letters just compares their labels. For the following discussion, we define $\gg_\bullet^\Lambda = ((\succ, \gg_\bullet)_{lex})_{mul}$.

Note that Definition 19 is a proper recursive definition: The multiset extension of the lexicographic product of two orders can be computed by comparing only elements present in the compared multisets, and all French strings occurring in $\langle s\rangle^f$ are proper substrings of s.

▸ **Example 20.** Recall the interpretations from Example 9. We show how to compare the first to the last one using the same precedence as in Example 13, i.e. $m \succ \ell, \kappa$. Because $\langle\varepsilon\rangle^f = \varnothing$, while $\langle\grave{\kappa}\acute{\ell}\grave{m}\rangle^f$ is a non-empty multiset, we have $\acute{m}\grave{\kappa}\acute{\ell} \gg_\bullet \varepsilon$. Therefore,

$$\langle\acute{m}\grave{\kappa}\acute{\ell}\grave{m}\rangle^f = [(\acute{m}, \grave{\kappa}\acute{\ell}\grave{m}), (\acute{\ell}, \grave{m}), (\grave{\kappa}, \acute{m}), (\grave{m}, \acute{m}\grave{\kappa}\acute{\ell})] \gg_\bullet^\Lambda [(\acute{\kappa}, \acute{\ell}), (\acute{\ell}, \varepsilon), (\grave{m}, \varepsilon)] = \langle\grave{m}\acute{\kappa}\acute{\ell}\rangle^f,$$
$$\acute{m}\grave{\kappa}\acute{\ell}\grave{m} \gg_\bullet \grave{m}\acute{\kappa}\acute{\ell}.$$

Next we show that $\gg_\bullet$ has all the desired properties: it is a well-founded, monotonic, partial order, provided that $\succ$ is a well-founded order on labels.

▸ **Lemma 21.** *If $\succ$ is a strict partial order on labels, then $\gg_\bullet$ is a strict partial order on French strings. Furthermore the construction is incremental: If $\succ \subseteq \succ'$ then $\gg_\bullet \subseteq \gg'_\bullet$, where $s \gg'_\bullet t$ iff $\langle s\rangle^f\ ((\succ', \gg'_\bullet)_{lex})_{mul}\ \langle t\rangle^f$.*

Proof. Consider the map $\Lambda_\succ(\gg) = \{(s,t) \mid \langle s\rangle^f\ ((\succ, \gg)_{lex})_{mul}\ \langle t\rangle^f\}$. By the properties of the lexicographic product and multiset extension of partial orders, $\Lambda_\succ(\gg)$ is monotonic in $\gg$ (with respect to $\subseteq$) and maps strict partial orders to strict partial orders. Therefore, and because the union of an increasing chain (w.r.t. $\subseteq$) of strict partial orders is again a strict partial order, the least fixed point of $\Lambda_\succ$ exists and is a strict partial order. Inspection of the definition shows that this least fixed point equals $\gg_\bullet$. Incrementality follows because $\Lambda_\succ(\gg)$ is monotonic in $\succ$. ◂

▸ **Lemma 22.** *The order $\gg_\bullet$ on French strings is monotonic.*

Proof. First consider monotonicity of the inverse. We have to show that $s \gg_\bullet t$ implies $s^{-1} \gg_\bullet t^{-1}$. We proceed by induction on the length of s. Note that we can express $\langle s^{-1}\rangle^f$ as $\langle s^{-1}\rangle^f = [(\hat{\ell}^{-1}, p^{-1}) \mid (\hat{\ell}, p) \in \langle s\rangle^f]$. Now by assumption, $\langle s\rangle^f \gg_\bullet^\Lambda \langle t\rangle^f$, and we need to show $\langle s^{-1}\rangle^f \gg_\bullet^\Lambda \langle t^{-1}\rangle^f$, that is,

$$[(\hat{\ell}^{-1}, p^{-1}) \mid (\hat{\ell}, p) \in \langle s\rangle^f] \gg_\bullet^\Lambda [(\hat{\kappa}^{-1}, q^{-1}) \mid (\hat{\kappa}, q) \in \langle t\rangle^f] \tag{1}$$

Since $\hat{\ell}^{-1} \succ \hat{\kappa}^{-1}$ iff $\hat{\ell} \succ \hat{\kappa}$ by definition and $p^{-1} \gg_\bullet q^{-1}$ iff $p \gg_\bullet q$ for all proper substrings p of s by the induction hypothesis, the evaluation of $\langle s\rangle^f \gg_\bullet^\Lambda \langle t\rangle^f$ can be mirrored in the comparison (1), which therefore holds.

Next we show that concatenation is monotonic. Assume that $s \gg_\bullet t$. We need to show that $ps \gg_\bullet pt$ for arbitrary French strings p. (Once we have proved that, we know that $s \gg_\bullet t$ implies $s^{-1} \gg_\bullet t^{-1}$, then $p^{-1}s^{-1} \gg_\bullet p^{-1}t^{-1}$, and finally $sp \gg_\bullet tp$ using the monotonicity of the inverse.) It suffices to show the claim if p has length 1; induction on the length of p will complete the proof. There are two cases, $p = \acute{\ell}$ and $p = \grave{\ell}$. We have:

$$\langle\acute{\ell}s\rangle^f = [(\acute{\kappa}, p) \mid (\acute{\kappa}, p) \in \langle s\rangle^f] \cup [(\grave{\kappa}, \acute{\ell}p) \mid (\grave{\kappa}, p) \in \langle s\rangle^f] \cup [(\acute{\ell}, s)]$$
$$\langle\grave{\ell}s\rangle^f = [(\acute{\kappa}, p) \mid (\acute{\kappa}, p) \in \langle s\rangle^f] \cup [(\grave{\kappa}, \grave{\ell}p) \mid (\grave{\kappa}, p) \in \langle s\rangle^f] \cup [(\grave{\ell}, \varepsilon)]$$

Now when comparing $\langle\acute{\ell}s\rangle^f \gg_\bullet^\Lambda \langle\acute{\ell}t\rangle^f$ (respectively $\langle\grave{\ell}s\rangle^f \gg_\bullet^\Lambda \langle\grave{\ell}t\rangle^f$), we have $(\acute{\ell}, s)\ (\succ, \gg_\bullet)_{lex}\ (\acute{\ell}, t)$ by assumption ($(\grave{\ell}, \varepsilon) = (\grave{\ell}, \varepsilon)$ trivially), while the other elements of the multisets originate in $\langle s\rangle^f$ and $\langle t\rangle^f$, and their comparisons carry over to that of $\langle\hat{\ell}s\rangle^f \gg_\bullet \langle\hat{\ell}t\rangle^f$. Note that in the lexicographic product, comparing $(\hat{\kappa}, p)$ and $(\hat{\kappa}', p')$ will only require comparing p to p' if $\hat{\kappa} = \hat{\kappa}'$, and then we know whether $\hat{\ell}$ was prepended to p and p', in which case we apply the induction hypothesis to that comparison, or not. Hence we conclude that $\hat{\ell}s \gg_\bullet \hat{\ell}t$. ◂

▸ **Remark.** None of the previously mentioned orders are monotonic. We have seen an example for $\succ_{ilpo}$ in Section 4.2; for the order from [5], we have $\diagup\diagup\diagup\diagup\diagup \ggg \diagdown\diagup\diagdown\diagdown\diagup$ but $\diagup\diagdown\diagup\diagdown\diagdown\diagup \ggg \diagup\diagup\diagup\diagup\diagup\diagup\diagup$; for [4], $\diagdown\diagup\diagup\diagup \ggg \diagdown\diagup\diagdown\diagup$ but $\diagdown\diagdown\diagup\diagdown\diagup \ggg \diagdown\diagdown\diagup\diagup\diagup$.

We still have to establish well-foundedness of $\gg_\bullet$. The proof is based on simple termination [7].

▸ **Theorem 23.** *If the precedence $>$ is well-founded, then $\gg_\bullet$ is a well-founded, monotonic, partial order on French strings.*

Proof. By Lemmas 21 and 22, $\gg_\bullet$ is a strict partial order and monotonic. We have to show that $\gg_\bullet$ is well-founded as well. Because its construction is incremental by Lemma 21, we may assume w.l.o.g. that $>$ is a (partial) well-order. We can easily see that $\gg_\bullet$ is a simplification order ([7, Definition 5.2]), if we regard French strings a terms over a unary signature as usual: monotonicity means that $\gg_\bullet$ is a rewrite order, while $\hat{\ell} \gg_\bullet \epsilon$ and $\hat{\ell} \gg_\bullet \hat{\kappa}$ if $\hat{\ell} > \hat{\kappa}$ ensure that $\succ_{\mathrm{emb}} \subseteq \gg_\bullet$. Therefore, $\gg_\bullet$ is well-founded by [7, Theorem 5.3]. ◂

▸ **Lemma 24.** *Let $>$ be a strict partial order. Then (recall the notation from Theorem 11)*

1. $\hat{\ell} \gg_\bullet \{\ell{>}\}$*; and*
2. $\acute{\ell}\grave{m} \gg_\bullet \{\ell{>}\}[\grave{m}]\{\ell, m{>}\}[\acute{\ell}]\{m{>}\}$

Proof. 1. Let $t \in \{\ell{>}\}$. We have to establish that $[(\hat{\ell}, \varepsilon)] \gg_\bullet^\Lambda \langle t\rangle^f$. The elements of $\langle t\rangle^f$ are pairs $(\hat{\kappa}, p)$ with $\ell > \kappa$, i.e. smaller than $(\hat{\ell}, \varepsilon)$ lexicographically, so the comparison holds.
2. Let $t \in \{\ell{>}\}[\grave{m}]\{\ell, m{>}\}[\acute{\ell}]\{m{>}\}$. We have to establish that $[(\acute{\ell}, \grave{m}), (\grave{m}, \acute{\ell})] \gg_\bullet^\Lambda \langle t\rangle^f$. Most elements of $\langle t\rangle^f$ are pairs $(\hat{\kappa}, p)$ with $\ell > \kappa$ or $m > \kappa$. There are up to two exceptions, depending on which of the letters $\acute{\ell}$ and $\grave{m}$ are present in t: $(\acute{\ell}, p)$ with $p \in \{m{>}\}$, for which we have $(\acute{\ell}, \grave{m})\ (>, \gg_\bullet)_{lex}\ (\acute{\ell}, p)$ using the first case, and $(\grave{m}, p)$ with $p \in \{\ell{>}\}$, for which we have $(\grave{m}, \acute{\ell})\ (>, \gg_\bullet)_{lex}\ (\grave{m}, p)$ likewise. Thus, every element of $\langle t\rangle^f$ is dominated by an element of $\langle\acute{\ell}\grave{m}\rangle^f$, and the comparison succeeds. ◂

Consequently, French strings equipped with $\gg_\bullet$ are a well-founded involutive monoid for decreasing diagrams.

We have presented two orders on French strings, $\succ_{ilpo}$ and $\gg_\bullet$. The first order, which we defined by mapping French strings to French terms of size linear in that of the strings, is lightweight and allows an intuitive explanation. The definition of $\gg_\bullet$ is more complex (unfolding it naively will result in an exponential number of comparisons), and opaque. On the other hand, $\succ_{ilpo}$ is not monotonic, which makes the proof of Lemma 18 a bit more tedious than that of Lemma 24. Thanks to monotonicity, the validity of new rules like $\grave{\ell}\acute{m}\grave{m} \Rightarrow \grave{m}\acute{m}\grave{m}\grave{\ell}\acute{m}$ if $\ell > m$ is readily established by a direct comparison, $\grave{\ell}\acute{m}\grave{m} \gg_\bullet \grave{m}\acute{m}\grave{m}\grave{\ell}\acute{m}$. Without monotonicity, we would have to consider all possible prefixes and suffixes in the proof.

5 Church–Rosser modulo

In this section we derive a decreasing diagrams technique for Church–Rosser modulo property, in analogy to Section 4. In Section 4.1 we have seen how conversions correspond to French strings. In order to apply this idea to Church–Rosser modulo, we introduce Greek strings, an extension of French strings with self-inverse letters.

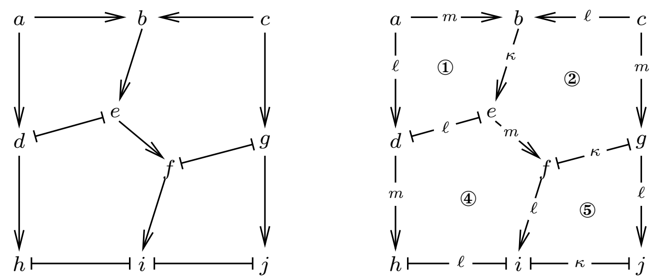


Figure 7 Decomposition of rewrite relations $\to$, $\mapsto$ enjoying the Church–Rosser modulo property.

5.1 Decreasing diagrams

▸ **Definition 25.** Let L be an alphabet. For each $\ell \in L$ there are three *Greek* letters, accented by acute, grave, or macron accents ($\acute{\ell}$, $\grave{\ell}$, or $\bar{\ell}$). We use $\hat{\ell}$ to denote a Greek letter with label ℓ. Mirroring letters is defined by $\acute{\ell}^{-1} = \grave{\ell}$ and $\bar{\ell}^{-1} = \bar{\ell}$. The *Greek* strings $\overline{L}$ are strings over Greek letters, which together with juxtaposition and mirroring form an involutive monoid. Any precedence $>$ on L is extended naturally to Greek letters by letting $\hat{\ell} > \hat{m}$ iff $\ell > m$. The intended purpose of macron (self-inverse) letters is to represent equational steps in proofs, a natural extension of the interpretations (Definition 8) used for confluence in Section 4.

▸ **Example 26.** Consider the rewrite relations in Figure 7. There are several conversions proving the equivalence of d and g, using labels $L = \{m, \ell, \kappa\}$. We list some interpretations:

$$\underline{\acute{\ell}\grave{m}}\acute{\ell}\grave{m} \Rightarrow_{①} \bar{\ell}\acute{\kappa}\underline{\acute{\ell}\grave{m}} \Rightarrow_{②} \bar{\ell}\underline{\acute{\kappa}\grave{\kappa}}\grave{m}\bar{\kappa} \Rightarrow \underline{\bar{\ell}\grave{m}}\bar{\kappa} \Rightarrow_{④} \grave{m}\bar{\ell}\underline{\acute{\ell}\bar{\kappa}} \Rightarrow_{⑤} \grave{m}\bar{\ell}\bar{\kappa}\acute{\ell}$$

We base our order on the monotonic order from Section 4.3 (Definition 19).

▸ **Definition 27.** Let L be an alphabet with precedence $>$. The order $\overline{\gg}_\bullet$ on Greek strings over L is defined by recursion as follows: $s \;\overline{\gg}_\bullet\; t$ iff $\langle s\rangle^g \;((>, \overline{\gg}_\bullet)_{lex})_{mul}\; \langle t\rangle^g$ where $\langle s\rangle^g = [(\acute{\ell}, q) \mid s = p\acute{\ell}q] \cup [(\grave{\ell}, p) \mid s = p\grave{\ell}q] \cup [(\bar{\ell}, \varepsilon) \mid s = p\bar{\ell}q]$ collects acute letters together with their suffixes, grave letters together with their prefixes, and macron letters together with empty strings into a multiset. We also define $\overline{\gg}_\bullet^\Lambda = ((>, \overline{\gg}_\bullet)_{lex})_{mul}$.

▸ Remark. We can regard any French string as a Greek string. If we do that, Definition 27 properly extends Definition 19: The map $\langle\cdot\rangle^g$ is an extension of $\langle\cdot\rangle^f$ that deals with self-inverse letters. One subtle difference is that $>$ is also extended: It compares French letters in Definition 19, but Greek letters in Definition 27.

▸ **Example 28.** Continuing Example 26, we show that the second to last step is decreasing, using the order $m > \ell > \kappa$ on L. In the resulting multiset comparison, it's easy to see that $(\grave{m}, \bar{\ell})$ is larger than every element of the right-hand side multiset:

$$\langle \bar{\ell}\grave{m}\bar{\kappa}\rangle^g = [(\bar{\ell}, \varepsilon), (\grave{m}, \bar{\ell}), (\bar{\kappa}, \varepsilon)] \;\overline{\gg}_\bullet^\Lambda\; [(\grave{m}, \varepsilon), (\bar{\ell}, \varepsilon), (\acute{\ell}, \bar{\kappa}), (\bar{\kappa}, \varepsilon)] = \langle \grave{m}\bar{\ell}\acute{\ell}\bar{\kappa}\rangle^g$$
$$\bar{\ell}\grave{m}\bar{\kappa} \;\overline{\gg}_\bullet\; \grave{m}\bar{\ell}\acute{\ell}\bar{\kappa}$$

The order $\overline{\gg}_\bullet$ shares many properties with $\gg_\bullet$.

▸ **Theorem 29.** *If the precedence $>$ on L is well-founded, then the order $\overline{\gg}_\bullet$ is a well-founded, monotonic, partial order on Greek strings.*

Proof. The similarities between $\gg_\bullet$ and $\overline{\gg}_\bullet$ are so overwhelming that the proofs of Lemmas 21, 22 and Theorem 23 work with straight-forward modifications:

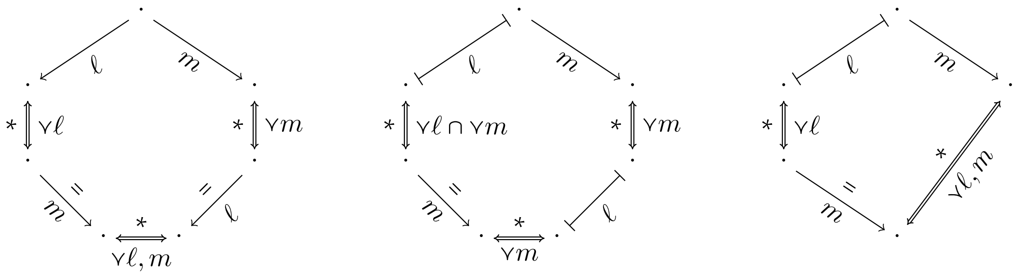


Figure 8 Locally decreasing diagrams for Church–Rosser modulo.

- Replace $\gg_{\bullet}$ by $\overline{\gg}_{\bullet}$, $\gg_{\bullet}^{\Lambda}$ by $\overline{\gg}_{\bullet}^{\Lambda}$ and $\langle\cdot\rangle^f$ by $\langle\cdot\rangle^g$ everywhere.
- In Lemma 21, define Λ by $\Lambda(\gg) = \{(s,t) \mid \langle s\rangle^g\ ((>,\gg)_{lex})_{mul}\ \langle t\rangle^g\}$.
- In Lemma 22, the expression for $\langle s^{-1}\rangle^f$ remains valid for $\langle s^{-1}\rangle^g$. For the monotonicity of concatenation, we have to consider three cases for p of length 1, $p = \acute{\ell}$, $p = \grave{\ell}$ and $p = \bar{\ell}$, and we can express $\langle \hat{\ell} s\rangle^g$ as follows:

$$\langle \acute{\ell} s\rangle^g = [(\hat{\kappa},p) \mid (\hat{\kappa},p) \in \langle s\rangle^g \text{ and } \hat{\kappa} \neq \grave{\kappa}] \cup [(\grave{\kappa},\acute{\ell}p) \mid (\grave{\kappa},p) \in \langle s\rangle^g] \cup [(\acute{\ell},s)]$$
$$\langle \grave{\ell} s\rangle^g = [(\hat{\kappa},p) \mid (\hat{\kappa},p) \in \langle s\rangle^g \text{ and } \hat{\kappa} \neq \grave{\kappa}] \cup [(\grave{\kappa},\grave{\ell}p) \mid (\grave{\kappa},p) \in \langle s\rangle^g] \cup [(\grave{\ell},\varepsilon)]$$
$$\langle \bar{\ell} s\rangle^g = [(\hat{\kappa},p) \mid (\hat{\kappa},p) \in \langle s\rangle^g \text{ and } \hat{\kappa} \neq \grave{\kappa}] \cup [(\grave{\kappa},\bar{\ell}p) \mid (\grave{\kappa},p) \in \langle s\rangle^g] \cup [(\bar{\ell},\varepsilon)]$$

  When comparing $\langle \bar{\ell} s\rangle^g$ and $\langle \bar{\ell} t\rangle^g$, we have $(\bar{\ell},\varepsilon) = (\bar{\ell},\varepsilon)$, and the remaining elements of the multisets originate in $\langle s\rangle^g$ and $\langle t\rangle^g$, respectively. The remainder of the argument in Lemma 22 applies directly.
- Finally, the well-foundedness proof in Theorem 23 requires no further modifications. ◂

▸ **Lemma 30.** *Let $>$ be a strict partial order. Then (recall the notation from Theorem 11)*

1. $\hat{\ell}\ \overline{\gg}_{\bullet}\ \{\ell>\}$ *and* $\acute{\ell}\grave{m}\ \overline{\gg}_{\bullet}\ \{\ell>\}[\grave{m}]\{\ell,m>\}[\acute{\ell}]\{m>\}$*;*
2. $\bar{\ell}\grave{m}\ \overline{\gg}_{\bullet}\ (\{\ell>\} \cap \{m>\})[\grave{m}]\{m>\}\bar{\ell}\{m>\}$ *(the intersection works on sets of strings); and*
3. $\bar{\ell}\grave{m}\ \overline{\gg}_{\bullet}\ \{\ell>\}[\grave{m}]\{\ell,m>\}$*.*

Proof. **1.** The first item is analogous to Lemma 24.

2. Let $t \in (\{\ell>\} \cap \{m>\})[\grave{m}]\{m>\}\bar{\ell}\{m>\}$. We have to show that $[(\bar{\ell},\varepsilon),(\grave{m},\bar{\ell})]\ \overline{\gg}_{\bullet}^{\Lambda}\ \langle t\rangle^g$. Note that $(\bar{\ell},\varepsilon) \in \langle t\rangle^g$, so all other elements of $\langle t\rangle^g$ must be smaller than $(\grave{m},\bar{\ell})$. This is true for $(\grave{m},p)$ with $p \in (\{\ell>\} \cap \{m>\})$ by the first item of this lemma, and all remaining pairs $(\hat{\kappa},p) \in \langle t\rangle^g$ are smaller than $(\grave{m},\bar{\ell})$ because $m > \kappa$. We conclude that $\bar{\ell}\grave{m}\ \overline{\gg}_{\bullet}\ t$.

3. Let $t \in \{\ell>\}[\grave{m}]\{\ell,m>\}$. We show that $[(\bar{\ell},\varepsilon),(\grave{m},\bar{\ell})]\ \overline{\gg}_{\bullet}^{\Lambda}\ \langle t\rangle^g$. All elements $(\hat{\kappa},p)$ of $\langle t\rangle^g$ have $\ell > \kappa$ or $r > \kappa$ (and are thus smaller than one of $(\grave{m},\bar{\ell})$ or $(\bar{\ell},\varepsilon)$), with one possible exception: $(\grave{m},p)$ where $p \in \{\ell>\}$, which is smaller than $(\grave{m},\bar{\ell})$ using the first item of this lemma. Therefore, $\bar{\ell}\grave{m}\ \overline{\gg}_{\bullet}\ t$ is true. ◂

▸ **Theorem 31.** *Let L be an alphabet equipped with a well-founded order $>$. Furthermore, let $(\underset{\ell}{\rightarrow})_{\ell\in L}$ and $(\underset{\ell}{\vdash\!\dashv})_{\ell\in L}$ be families of abstract rewrite relations, where each $\underset{\ell}{\vdash\!\dashv}$ is symmetric. If*

$$\underset{\ell}{\leftarrow} \cdot \underset{m}{\rightarrow} \subseteq \overset{*}{\underset{\curlyvee\ell}{\Leftrightarrow}} \cdot \overset{=}{\underset{m}{\rightarrow}} \cdot \overset{*}{\underset{\curlyvee\ell,m}{\Longleftrightarrow}} \cdot \overset{=}{\underset{\ell}{\leftarrow}} \cdot \overset{*}{\underset{\curlyvee m}{\Longleftrightarrow}}$$

and

$$\underset{\ell}{\vdash\!\dashv} \cdot \underset{m}{\rightarrow} \subseteq \left(\overset{*}{\underset{\curlyvee\ell\cap\curlyvee m}{\Longleftrightarrow}} \cdot \overset{=}{\underset{m}{\rightarrow}} \cdot \overset{*}{\underset{\curlyvee m}{\Leftrightarrow}} \cdot \underset{\ell}{\vdash\!\dashv} \cdot \overset{*}{\underset{\curlyvee m}{\Leftrightarrow}}\right) \cup \left(\overset{*}{\underset{\curlyvee\ell}{\Leftrightarrow}} \cdot \overset{=}{\underset{m}{\rightarrow}} \cdot \overset{*}{\underset{\curlyvee\ell,m}{\Longleftrightarrow}}\right),$$

for all $\ell, m \in L$, where $\underset{\ell}{\Leftrightarrow} = \underset{\ell}{\leftarrow} \cup \underset{\ell}{\vdash\!\dashv} \cup \underset{\ell}{\rightarrow}$ (see Figure 8), then $\underset{L}{\rightarrow}$ is Church–Rosser modulo $\underset{L}{\vdash\!\dashv}$.

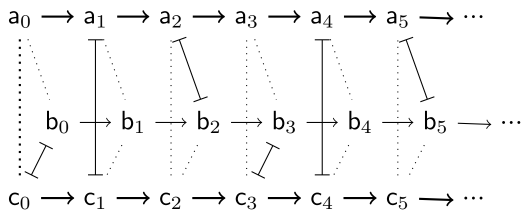


Figure 9 Incompleteness: The rewrite relations $\to$ and $\vdash\!\dashv$.

Proof. The proof follows that of Theorem 11. First we observe that if a conversion between two objects a and b is not a valley of shape $\overset{*}{\to}\cdot\overset{*}{\vdash\!\dashv}\cdot\overset{*}{\leftarrow}$, then it must contain a local peak or cliff. By assumption, we can replace that peak or cliff by an alternative subproof. To show termination, we observe that the interpretation of the replacement proof is smaller than that of the peak or cliff w.r.t. $\ggg_{\bullet}$, by Lemma 30. Thanks to monotonicity this extends to the interpretations of the whole proofs. This implies termination, because $\ggg_{\bullet}$ is well-founded. ◂

The rewrite relations in Figure 7 have the Church–Rosser modulo property, because every local peak and cliff can be joined in a decreasing diagram of the required shape. As an instance of Theorem 31 we obtain the following result by Jouannaud and Liu.

▸ **Corollary 32** ([4, Corollary 2.5.8]). *Let $(\underset{\ell}{\to})_{\ell\in L}$ and $(\underset{\ell}{\vdash\!\dashv})_{\ell\in L}$ be families of abstract rewrite relations, where each $\underset{\ell}{\vdash\!\dashv}$ is symmetric. Then $\underset{L}{\to}$ is Church–Rosser modulo $\underset{L}{\vdash\!\dashv}$, if for all $\ell, m \in L$, $\underset{\ell}{\leftarrow}\cdot\underset{m}{\to} \subseteq \overset{*}{\underset{\curlyvee\ell}{\Leftrightarrow}} \cdot \overset{=}{\underset{m}{\to}} \cdot \overset{*}{\underset{\curlyvee\ell,m}{\Longleftrightarrow}} \cdot \overset{=}{\underset{\ell}{\leftarrow}} \cdot \overset{*}{\underset{\curlyvee m}{\Leftrightarrow}}$ and $\underset{\ell}{\vdash\!\dashv}\cdot\underset{m}{\to} \subseteq \overset{=}{\underset{m}{\to}}\cdot \overset{*}{\underset{\curlyvee\ell,m}{\Longleftrightarrow}}$.*

Furthermore, Ohlebusch's Main Theorem of [8] is a consequence of Corollary 32 by labelling all $\vdash\!\dashv$ steps with a minimal, fresh label $\bot$. As another instance of Theorem 31 we can obtain a key lemma for abstract Church–Rosser modulo from [1]:

▸ **Corollary 33** (Aoto and Toyama [1, Lemma 2.1]). *Let $(\underset{\ell}{\to})_{\ell\in L}$ and $(\underset{\ell}{\vdash\!\dashv})_{\ell\in L}$ be families of abstract rewrite relations, where each $\underset{\ell}{\vdash\!\dashv}$ is symmetric. Then $\underset{L}{\to}$ is Church–Rosser modulo $\underset{L}{\vdash\!\dashv}$, if for all $\ell, m \in L$, $\underset{\ell}{\leftarrow}\cdot\underset{m}{\to} \subseteq \underset{\curlyvee\ell,m}{\Longleftrightarrow}$ and $\underset{\ell}{\vdash\!\dashv}\cdot\underset{m}{\to} \subseteq \underset{\curlyvee\ell,m}{\Longleftrightarrow}$.*

5.2 Incompleteness

It is known that decreasing diagrams are complete for confluence of countable rewrite relations [9, Theorem 14.2.32]. In this section we show that no terminating proof rewrite system can be complete for proving Church–Rosser modulo. To this end, we exhibit a pair of rewrite relations $\to$, $\vdash\!\dashv$ such that $\to$ is Church–Rosser modulo $\vdash\!\dashv$, but there is no terminating proof rewrite system that has only valley proofs of shape $\overset{*}{\to}\cdot\overset{*}{\vdash\!\dashv}\cdot\overset{*}{\leftarrow}$ as normal forms.

▸ Remark. Terminating proof rewrite systems are exactly those which are compatible with some monotonic well-founded order on proofs. However, as we have seen with $\succ_{ilpo}$ in Section 4.2, we can also show termination of proof rewrite systems using non-monotonic orders. The incompleteness result of this section applies to such proofs as well.

▸ **Definition 34.** On the set $A = \{\mathsf{a}_i, \mathsf{b}_i, \mathsf{c}_i \mid i \in \mathbb{N}\}$ we define the relations $\to$ and $\vdash\!\dashv$ as follows:

1. $u_i \to u_{i+1}$ iff $u \in \{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$;

2. $u_i \mapsto\!\!\dashv v_i$ iff $\{u, v\} = \{\mathsf{b}, \mathsf{c}\}$ if $i \equiv 0 \pmod 3$, $\{u, v\} = \{\mathsf{a}, \mathsf{c}\}$ if $i \equiv 1 \pmod 3$ and $\{u, v\} = \{\mathsf{a}, \mathsf{b}\}$ otherwise. (See also Figure 9.)

▸ Remark. Definition 34 may be regarded as a simplified version of [4, Figure 1(a)]. Both examples would serve the purpose of this section, and Theorem 36 subsumes the incompleteness result of [4, Section 4.3].

Note that $\to$ is deterministic and that all $\overset{*}{\vdash\!\dashv}$ equivalence classes have size 1 or 2. Together with the periodic and symmetric nature of the rewrite relations (consider mapping a_i, b_i and c_i to b_{i+1}, c_{i+1} and a_{i+1}, respectively), this restricts valley proofs to just a few possibilities:

▸ **Proposition 35.** *1. The rewrite relation $\to$ is Church–Rosser modulo $\vdash\!\dashv$.*
2. Any valley proof for a peak $\overset{n}{\leftarrow} \cdot \overset{m}{\to}$ has shape $\xrightarrow{l-n} \cdot \overset{*}{\vdash\!\dashv} \cdot \xleftarrow{l-m}$ for some $l \geqslant n, m \geqslant 0$.
3. Any valley proof for a local cliff $\leftarrow \cdot \vdash\!\dashv$ has shape $\xrightarrow{3n-1} \cdot \overset{+}{\vdash\!\dashv} \cdot \xleftarrow{3n}$ for some $n > 0$.

The following result establishes that no terminating proof rewrite system can be complete for Church–Rosser modulo of $\to$, $\vdash\!\dashv$.

▸ **Theorem 36.** *There is no terminating proof rewrite system for $\to$, $\vdash\!\dashv$ that only rewrites local peaks and cliffs and always produces valley proofs as normal forms.*

Proof. By contradiction. Assume that we are given a terminating proof rewrite system whose normal forms are valley proofs. We show coinductively that any proof of shape

$$\vdash\!\dashv \cdot \overset{n}{\to} \cdot \overset{m}{\leftarrow} \cdot \vdash\!\dashv \tag{2}$$

with $n \not\equiv m \pmod 3$ allows an infinite proof rewrite sequence. Note that such proofs exist, for example, we have $\mathsf{b}_0 \vdash\!\dashv \mathsf{c}_0 \to \mathsf{c}_1 \vdash\!\dashv \mathsf{a}_1$. We may assume w.l.o.g. that $n > 0$ (if $n = 0$, then $m > 0$, and we can conclude symmetrically). Then we can rewrite the initial cliff $\vdash\!\dashv \cdot \to$ to a normal form, which must be a valley proof. By Proposition 35, the resulting proof has shape $\xrightarrow{3k} \cdot \overset{+}{\vdash\!\dashv} \cdot \xleftarrow{3k-1} \cdot \xrightarrow{n-1} \cdot \overset{m}{\leftarrow} \cdot \vdash\!\dashv$ for some $k \in \mathbb{N}$. Similarly, we can reduce the new peak $\xleftarrow{3k-1} \cdot \xrightarrow{n-1}$ to a valley proof, which by Proposition 35 results in a proof

$$\xrightarrow{3k} \cdot \overset{+}{\vdash\!\dashv} \cdot \overset{u}{\to} \cdot \overset{p}{\vdash\!\dashv} \cdot \overset{v}{\leftarrow} \cdot \vdash\!\dashv \tag{3}$$

with $u = l - 3k + 1$ and $v = l - n + 1 + m$ for some $l, p \in \mathbb{N}$. for some $l, p \in \mathbb{N}$. Let $u = l - 3k + 1$ and $v = l - n + 1 + m$. It is easy to see that $u \not\equiv v \pmod 3$. If $p = 0$, then (3) contains a subproof of shape (2), namely $\vdash\!\dashv \cdot \overset{u}{\to} \cdot \overset{v}{\leftarrow} \cdot \vdash\!\dashv$. If $p > 0$ and $u \not\equiv 0 \pmod 3$ then the subproof $\vdash\!\dashv \cdot \overset{u}{\to} \cdot \overset{0}{\leftarrow} \cdot \vdash\!\dashv$ of (3) has shape (2). Otherwise, $p > 0$ and $v \not\equiv 0 \pmod 3$, and the subproof $\vdash\!\dashv \cdot \overset{0}{\to} \cdot \overset{v}{\leftarrow} \cdot \vdash\!\dashv$ of (3) has shape (2). Continuing this process on the obtained subproof, we obtain an infinite proof rewrite sequence, contradicting our termination assumption. ◂

▸ Remark. Note that by identifying u_i with u_{i+3} for all $i \in \mathbb{N}$ and $u \in \{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$ we obtain a pair of finite rewrite relations for which Theorem 36 still holds.

6 Conclusion

We have presented two well-founded orders on French strings that entail the decreasing diagrams technique, one based on (i)lpo and the other with a more complex definition (related to rpo) that makes it monotone. Generalising the monotone order to work on Greek strings that include self-inverse letters, we have obtained a new result for Church–Rosser modulo. It would be interesting to generalise the ilpo based order as well, but we leave that to future work. Finally, we have shown that no complete criterion for Church–Rosser modulo can be obtained by considering proof transformations alone; at the least, some sort of strategy for applying proof rewrite rules must be incorporated.

Acknowledgements The first author is supported by FWF (Austrian Science Fund) project P22467. The question of completeness (Section 5.2) was raised by Jouannaud. We would also like to thank the anonymous reviewers for their valuable feedback. In particular, the short proof of Theorem 29 was suggested by one of the reviewers.

A Appendix

Proof of Proposition 6. Consider the term rewrite system obtained by orienting the laws of Definition 2 from left to right into term rewrite rules:

$$\begin{array}{rcl@{\qquad\qquad}rcl} c(c(x,y),z) & \to & c(x,c(y,z)) & i(i(x)) & \to & x \\ c(x,e) & \to & x & i(c(x,y)) & \to & c(i(y),i(x)) \\ c(e,x) & \to & x & i(e) & \to & e \end{array}$$

This term rewriting system is confluent and terminating, as tools nowadays can show automatically, and has as closed normal forms[9] e and the elements of the set N given by:

$$N ::= \ell \mid i(\ell) \mid c(\ell, N) \mid c(i(\ell), N)$$

Therefore, endowing $\{e\} \cup N$ with operations c, e, and i, in each case followed by taking normal forms, constitutes a free involutive monoid. This monoid is easily seen to be isomorphic to the one on French strings via the bijection between N and $\widehat{L}$ induced by $\ell \mapsto \grave{\ell}$. ◂

References

1. T. Aoto and Y. Toyama. A reduction-preserving completion for proving confluence of non-terminating term rewriting systems. *LMCS*, 8(1:31):1–29, 2012.
2. L. Bachmair and N. Dershowitz. Equational inference, canonical proofs, and proof orderings. *Journal of the ACM*, 41(2):236–276, 1994.
3. B. Jacobs. Involutive categories and monoids, with a GNS-correspondence. *Foundations of Physics*, pages 1–22, 2011.
4. J. P. Jouannaud and Jiaxiang Liu. From diagrammatic confluence to modularity. *Theoretical Computer Science*, 464:20–34, 2012.
5. J.-P. Jouannaud and V. van Oostrom. Diagrammatic confluence and completion. In *Proc. 36th ICALP*, volume 5556 of *LNCS*, pages 212–222, 2009.
6. J.W. Klop, V. van Oostrom, and R. de Vrijer. Iterative lexicographic path orders. In *Algebra, Meaning and Computation: Essays dedicated to Joseph A. Goguen on the Occasion of His 65th Birthday*, volume 4060 of *LNCS*, pages 541–554, 2006.
7. A. Middeldorp and H. Zantema. Simple termination of rewrite systems. *Theoretical Computer Science*, 175(1):127–158, 1997.
8. E. Ohlebusch. Church-Rosser theorems for abstract reduction modulo an equivalence relation. In *Proc. 9th RTA*, volume 1379 of *LNCS*, pages 17–31, 1998.
9. Terese. *Term Rewriting Systems*, volume 55 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 2003.
10. V. van Oostrom. Confluence by decreasing diagrams – converted. In *Proc. 19th RTA*, volume 5117 of *LNCS*, pages 306–320, 2008.

[9] Think of these closed normal forms as (empty) conversions.