Decreasing proof orders
Interpreting conversions in involutive monoids

Vincent van Oostrom[a]

[a] *Utrecht University, Department of Philosophy*
Janskerkhof 13, 3512 BL Utrecht, Netherlands

Abstract

We introduce the *decreasing* proof order. It orders a conversion above another conversion if the latter is obtained by filling any peak in the former by a decreasing diagram. The result is developed in the setting of involutive monoids.

Keywords: Involutive monoid, Proof order, Decreasing diagram, Lexicographic path order
1998 MSC: F.3.1, F.4.2

1. Introduction

Consider the problem of deciding whether two objects are equivalent with respect to the equivalence relation generated by some rewrite relation. From that perspective, a conversion between two objects in the rewrite relation is a proof that the objects are equivalent. Confluence of the rewrite relation is a desirable property as then such proofs may be assumed to be *rewrite* proofs, which are conversions having the shape of a valley: a number of forward rewrite steps followed by a number of backward rewrite steps.

Referring the reader to [3, 11] for the study of properties of rewrite relations in general and confluence in particular, we focus in this short paper on contributing to the proof theory of confluence. In particular, we present a novel proof order [4], i.e. a well-founded order on conversions. We dub it the *decreasing* proof order as it is compatible with the decreasing diagrams technique of proving confluence [10] in the sense that filling a peak in a conversion by a decreasing diagram yields a conversion that is smaller with respect to this proof order.

We develop our results in the setting of *involutive* monoids, see e.g. [6], observing that conversions can not only be composed to yield monoidal structure, but that they can also be *mirrored* to yield involutive structure. Involutive monoids thus being natural for interpreting conversions, but largely absent from the rewriting literature, we devote in Section 2 considerable attention to developing such interpretations. In particular, we give an interpretation of conversions

Email address: `Vincent.vanOostrom@phil.uu.nl` (Vincent van Oostrom)

into what we call *French* terms, a set of terms over the free involutive monoid that itself has a (free) involutive monoidal structure.

The decreasing proof order on conversions is defined in Section 3, via the interpretation of conversions into French terms and a certain lexicographic path order [3, 11, 8] on the latter. We show that the decreasing proof order is compatible with the decreasing diagrams technique in the sense mentioned above.

The decreasing proof order has the following features distinguishing it from the first, and thusfar only other, published proof order compatible with the decreasing diagrams technique, as developed by Jouannaud in [7]:

- The interpretation gives insight. It shows a decreasing diagram to be a 'lexicographic combination' of 'square' diagrams as in the Lemma of Hindley–Rosen and 'splitting' diagrams as in Newman's Lemma;

- Interpretations are small. The interpretation of a conversion (French term) is linear in the size of the conversion;

- The proof order is flexible. Well/better-behaved interesting subrelations, e.g. monotonic proof orders, can be easily 'carved out' from it;

- The set-up is flexible. Rewriting–modulo conversions are naturally represented by elements of a non-free involutive monoid, and, more generally, interpretations into other involutive monoids are easily accommodated.

We will illustrate each of these points in the rest of the paper, except for the last. We decided to concentrate here on establishing the basic set-up, and to present variations on it such as rewriting modulo, later and elsewhere.

We assume knowledge of rewriting [3, 11], in particular of the confluence by decreasing diagrams technique [10, 11] and of lexicographic path orders [3, 11, 8].

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

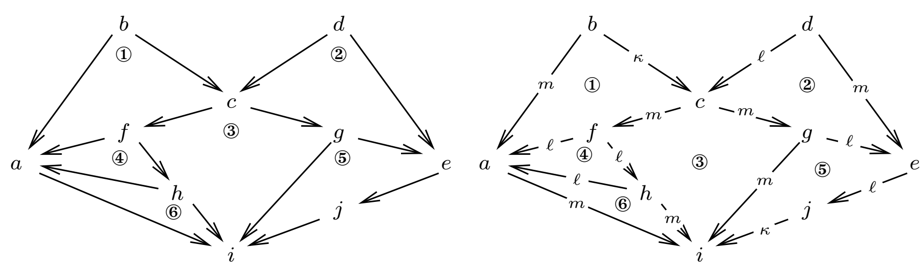

Figure 1: Decomposing a rewrite relation (left) into a family of such (right)

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

$$
\begin{aligned}
\to_\kappa &= \{(b,c),(j,i)\} \\
\to_\ell &= \{(d,c),(f,a),(f,h),(g,e),(h,a),(e,j)\} \\
\to_m &= \{(b,a),(d,e),(c,f),(c,g),(g,i),(a,i),(h,i)\}
\end{aligned}
$$

We will show how each of the transformation steps, indicated by the numbers, leading from the initial conversion $a \leftarrow_m b \to_\kappa c \leftarrow_\ell d \to_m e$ to the final valley $a \to_m i \leftarrow_\kappa j \leftarrow_\ell e$ entails a decrease in the proof order.

2. Interpreting conversions in involutive monoids

We present an interpretation of the conversions of a given family of rewrite relations index by a set of labels into, what we call, French terms. Both the interpretation as well as, in the next section, the proof order on French terms are naturally expressed by means of homomorphisms on the free involutive monoid over the set of labels. Therefore, we first recapitulate and illustrate involutive monoids, see e.g. [6].

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 involutive anti-automorphism (-1), see Table 1.

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$	(associative)
$a \cdot e = a$	(right identity)
$e \cdot a = a$	(left identity)
$(a^{-1})^{-1} = a$	(involutive)
$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$	(anti-automorphic)

Table 1: Involutive monoid laws

Note $e^{-1} = e$ derives from $e^{-1} = e \cdot e^{-1} = (e^{-1})^{-1} \cdot e^{-1} = (e \cdot e^{-1})^{-1} = (e^{-1})^{-1} = e$. We first illustrate involutive monoids by means of examples from algebra.

Example 3. (i) The *trivial* involutive monoid comprises a singleton set endowed with the binary, nullary, and unary constant maps;

(ii) The integers with addition, zero, and unary minus $(\mathbb{Z}, +, 0, -)$ constitute an involutive monoid as do the positive rationals with multiplication, one, and inverse $(\mathbb{Q}^+, \cdot, 1, {}^{-1})$. Groups constitute involutive monoids;

(iii) 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 gives rise to involutive monoids in this way;

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

After these general examples, we turn to involutive monoids on which both our interpretation of conversions and our proof order will be based.

Example 4. (i) For a given alphabet L, let a *French* letter be an accented (grave $\grave{\ell}$ or acute $\acute{\ell}$) letter.[1] 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.[2] 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 $\diagdown, \diagup$. French strings (of accents) can be given a geometric interpretation as diagrams, as illustrated in Figure 2 left (middle).

(ii) 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;

(iii) 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. For instance, associativity is established by computing

$$\begin{aligned}
&((n_1, m_1, k_1) \cdot (n_2, m_2, k_2)) \cdot (n_3, m_3, k_3) \\
&= (n_1 + n_2, m_1 + k_1 \cdot n_2 + m_2, k_1 + k_2) \cdot (n_3, m_3, k_3) \\
&= (n_1 + n_2 + n_3, m_1 + k_1 \cdot n_2 + m_2 + (k_1 + k_2) \cdot n_3 + m_3, k_1 + k_2 + k_3) \\
&= (n_1 + n_2 + n_3, m_1 + k_1 \cdot (n_2 + n_3) + m_2 + k_2 \cdot n_3 + m_3, k_1 + k_2 + k_3) \\
&= (n_1, m_1, k_1) \cdot (n_2 + n_3, m_2 + k_2 \cdot n_3 + m_3, k_2 + k_3) \\
&= (n_1, m_1, k_1) \cdot ((n_2, m_2, k_2) \cdot (n_3, m_3, k_3))
\end{aligned}$$

[1] 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 standard in rewriting since the 1930s (Church–Rosser,Newman), see Figure 2.

[2] As a historical aside note that boustrophedon texts as found in ancient manuscripts can be linearly represented as French strings by interpreting the accents as instructions for writing letters either forward or bɿɒwʞɔɒd. The representation is natural in the same way strings represent ordinary text naturally; composition of (boustrophedon) texts is represented by composition of (French) strings, so length, prefixes, and suffixes are all preserved. The obvious map from boustrophedon texts to ordinary texts is also natural in the technical sense of being a homomorphism of involutive monoids, cf. Example 8(ii).

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 2 right.

Conversions can be interpreted naturally into the French strings.

Definition 5. The *interpretation* of a conversion for an L-indexed family of rewrite relations, is the 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 6. 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:

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

The proof order we define in the next section will be based on an isomorphism between the French strings and a certain class of terms, that we therefore call French terms, based on a well-founded order, i.e. a transitive and terminating relation, $\succ$ on the set L of labels. As usual, an isomorphism is a homomorphism having an inverse, with a homomorphism being a structure preserving map.

Definition 7. 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.

The identity is a homomorphism and homomorphisms are closed under composition. Before presenting the isomorphism mentioned, we give some examples of homomorphisms linking up the various involutive monoids presented above. These homomorphisms will be auxiliary to the construction of both our isomorphism and, in the next section, the decreasing proof order.

Example 8. (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 triple $(1,0,0)$ induces a (unique) homomorphism from French strings over accents to 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 2.

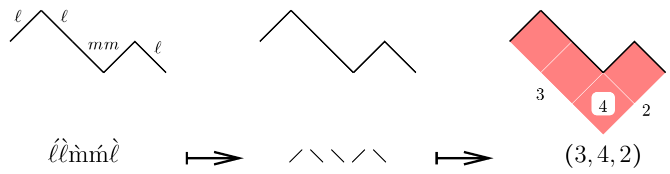

Figure 2: Mapping French strings via strings of accents into triples

The involutive monoid on French strings $\widehat{L}$ is of special interest in that it is *free*: 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 $\widehat{L}$.

Proposition 9 ([6, Proposition 2])**.** The involutive monoid on French strings $\widehat{L}$ is the free involutive monoid over L.

Proof. For a 'rewriting' proof of this fact, consider the result of completing the term rewrite system obtained by orienting the identities of Table 1 from left to right into term rewrite rules, with the last rule being adjoined by completion:

$$\begin{aligned}
c(c(x,y),z) &\to c(x,c(y,z)) \\
c(x,e) &\to x \\
c(e,x) &\to x \\
i(i(x)) &\to x \\
i(c(x,y)) &\to c(i(y),i(x)) \\
i(e) &\to e
\end{aligned}$$

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

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

Therefore, endowing 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 $\ell \mapsto \grave{\ell}$. $\square$

We conclude this section by introducing French terms, an involutive monoid on terms isomorphic to French strings, on which our proof order introduced in the next section will be based. The intuition for this term representation is that the proof order should compare conversions first with respect to their maximal labels (the head of the term; with respect to both their multiset and area), and recursively (the direct subterms) with respect to the the remaining labels next. To single out the maximal labels

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

Definition 10. The *French* term signature over L is denoted by $L^{\sharp}_{\succ}$ and comprises the French strings over L having $\succ$-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 $m \succ \ell$.

The height of French terms is bounded by the longest path in $\succ$. If $\succ$ is the empty relation then the signature comprises all French strings and terms are flat. 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 in it.

Example 11. Well-foundedly ordering the set L of labels of Example 1 as $m \succ \ell, \kappa$, some examples of French terms over L are

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

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

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

Lemma 12. The inorder-traversal map $\flat$ *flattening* French terms over L into French strings over L is a bijection.

Proof. Let the *stratification* map from French strings over L to French terms over L be inductively be defined by:[3]

$$\begin{aligned} \varepsilon^{\sharp} &= \varepsilon \\ (s_0\hat{\ell}_1 \dots \hat{\ell}_n s_n)^{\sharp} &= \hat{\ell}_1 \dots \hat{\ell}_n(s_0^{\sharp}, \dots, s_n^{\sharp}) \end{aligned}$$

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 symbol of the term. $\square$

Flattening and stratification are easily computed and are linear in the size.

Example 13. Stratifying the French strings $\acute{m}\grave{\kappa}\acute{\ell}\grave{m}$, $\acute{\ell}\grave{\ell}\grave{m}\acute{m}\grave{\ell}$, and $\grave{m}\acute{\kappa}\acute{\ell}$ with respect to $\succ$ as given in Example 11 yields the French terms given there.

Corollary 14. *The French terms over L give the free involutive monoid over L, when endowed with the operations on French strings, via the flattening and stratification maps, e.g. $t \cdot u = (t^{\flat}u^{\flat})^{\sharp}$,*

[3] 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 corollary we might as well think of the interpretation of conversions (Definition 5) as yielding French terms instead of French strings.

Example 15. The three French terms in Example 11 are the respective interpretations of the first, fourth, and last conversion in Example 1 (see Figure 1).

3. A proof order for decreasing diagrams

We introduce the *decreasing* proof order on conversions based on comparing their interpretation as French terms (see Corollary 14 and the text below it) with respect to some lexicographic path order. This is in concordance with the intuition provided above: in the lexicographic path order the head symbols of terms are compared first, which corresponds to comparing the $\succ$-maximal labels of the corresponding conversions first, as desired.

After that we will justify naming it the *decreasing* proof order by showing that it is compatible with the decreasing diagrams technique, in the sense that filling a local peak in a conversion by a decreasing diagram yields a conversion that is smaller with respect to the proof order.

Definition 16. Let $\gg$ be 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 8), relating these by the lexicographic product of the multiset-extension $\succ_{mul}$ of $\succ$ and the greater-than relation $>$.

The *decreasing proof order* on French terms is the iterative lexicographic path order [8, Definition 2][4] induced by the relation $\gg$, where argument places are ordered *lexicographically* by choosing an arbitrary but fixed total order on them compatible with the accents: if the $i+1^{st}$ label has a grave (acute) accent, then the i^{th} argument place comes before (after) the $i+1^{st}$.

The decreasing proof order $\gg_{ilpo}$ is extended to French strings via their stratification and to conversions via their interpretation.

By [8, Theorem 1] $\gg_{ilpo}$ is a well-founded order, since $\gg$ is terminating as the lexicographic product of the terminating relations $\succ_{mul}$ and $>$. It is easy to see that the head symbol of a French term is $\gg$-related to each symbol occurring in its proper subterms, by comparing their respective multisets of labels. Note that one way to order the argument places of a given function symbol totally is to successively take the leftmost argument place as allowed by the accents.

Example 17. We have $\grave{\kappa}\acute{\ell} \gg \grave{\ell}$ since the multiset $[\ell, \kappa]$ of the former is $\succ_{mul}$-related to the multiset $[\ell]$ of the latter; we have $\acute{\ell}\grave{\ell} \gg \grave{\ell}\acute{\ell}$ 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).

[4] We prefer this presentation of the lexicographic path order since it does not assume the relation on the signature to be an order.

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; the leftmost way to order them mentioned above would yield $0, 2, 1$. 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 leftmost way of ordering them yields $1, 0, 2$.

The sequence of transformation steps of Example 6 yields a $\succ_{ilpo}$-sequence:

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

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.

Remark 18. On [10, p. 315] we wrote:

> ...one could be led to believe the decreasing diagrams technique is just the sum of Newmans Lemma and the Lemma of Hindley–Rosen. The following examples show it is much more powerful ...

The intuition for interpreting conversions as French terms and the function symbols in $L^{\sharp}_{\succ}$ as pairs as in Definition 16, is that the decreasing diagrams technique combines the essential ingredients of both lemmas, the multiset of labels respectively the area, in a lexicographic and hierarchical way. To be a bit more precies, the idea captured by taking the subsequence of a conversion comprising its $\succ$-maximal (within the conversion) steps as *head* of the French term, is that this subsequence of maximal step is the first approximation to the conversion. Then filling in a locally decreasing diagrams in a conversion for a peak of such $\succ$-maximal steps corresponds at first approximation to filling in square diagrams, i.e. at first approximation confluence is obtained by the Lemma of Hindley–Rosen; the *area* decreases by filling in. The idea captured by letting the remaining non-maximal steps in the conversion (recursively) determine the *subterms* of the French term of the conversion, is that these correspond to deeper levels of approximation to the conversion, and taking the *path order* then captures that changes at the first approximation outweigh those at deeper levels, i.e. at deeper levels of approximation confluence is obtained by Newman's Lemma; the *paths through multisets* decrease by filling in. Finally, taking the *lexicographic* path order captures the interaction allowed between maximal and non-maximal steps. Filling in a peak between such steps with a locally decreasing diagram does not change the first approximation to the conversion, but it does lead to a decrease at the deeper approximations; filling in decreases the subterms with which the maximal step still has to interact, *lexicographically*, as determined by its *accent*.

Lemma 19. 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
- $s\acute{\ell}\grave{m}r \succ_{ilpo} s\{\ell{\succ}\}[\grave{m}]\{\ell,m{\succ}\}[\acute{\ell}]\{m{\succ}\}r$

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

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

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

  (yes) then the head symbol of the lhs $\succ$-relates to the head symbol of the rhs, because the multiset has become smaller, hence the head symbol of the lhs $\succ$-relates to the other function symbols in the rhs as well;

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

- We distinguish cases on whether or not ℓ, m are $\succ$-maximal in $s\acute{\ell}\grave{m}r$, illustrated in Figures 3–5, where $\succ$-maximal labels are coloured blue and non-$\succ$-maximal labels are coloured red:

  (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 3;

  (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 4;

  (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, see Figure 5; $\square$

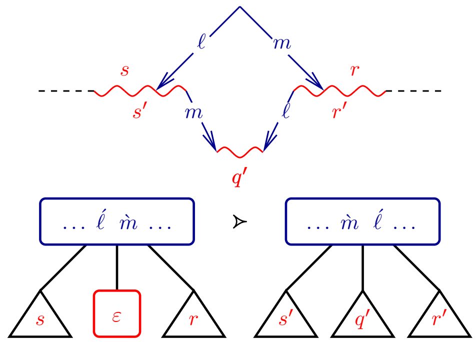

Figure 3: (both) Decrease in area

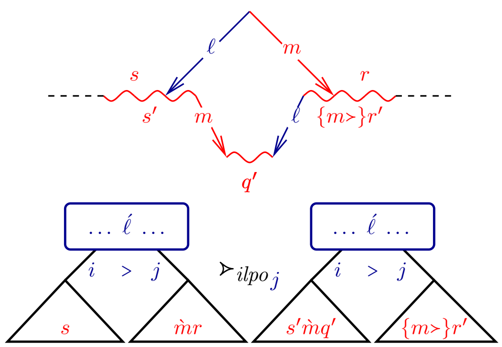

Figure 4: (one) Decrease in jth argument, lexicographically before ith argument

Theorem 20. *The decreasing proof order is compatible with the decreasing diagrams technique [10, Definition 3] in the sense that if a peak* $\leftarrow_\ell \cdot \rightarrow_m$ *in a conversion is replaced by a conversion of shape* $\leftrightarrow^*_{\ell\succ} \cdot \rightarrow^=_m \cdot \leftrightarrow^*_{\ell,m\succ} \cdot \leftarrow^=_\ell \cdot \leftrightarrow^*_{m\succ}$ *(see Figure 6 left) forming a so-called* decreasing diagram*, then the interpretation of the former is* $\succ_{ilpo}$*-related to the interpretation of the latter (see Figure 6 right).*

Proof. Immediate by the second item of Lemma 19. ☐

Recall from [10] that a rewrite relation $\rightarrow$ is said to be *decreasing* if $\rightarrow = \bigcup_{\ell\in L} \rightarrow_\ell$ for some family of rewrite relations $(\rightarrow_\ell)_{\ell\in L}$ and well-founded order $\succ$ on L, every peak can be replaced by a conversion forming a decreasing diagram.

Corollary 21 ([10, Theorem 3])**.** *A decreasing rewrite relation is confluent.*

Proof. Given a conversion, choose any L-labelling of it. As long as it contains peak, the conversion can be tranformed another one to which it $\succ_{ilpo}$-relates.

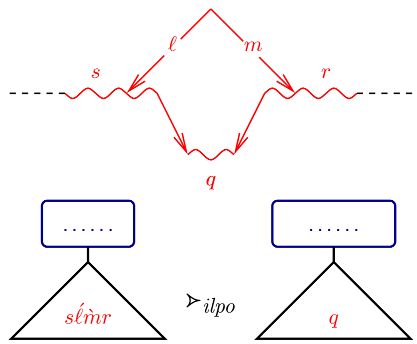

Figure 5: (neither) Decrease in argument both labels are in

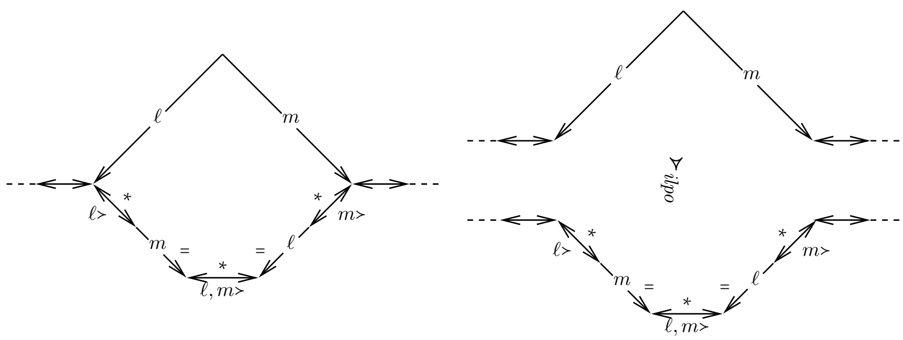

Figure 6: Compatibility of decreasing proof order with decreasing diagrams

Since $\succ_{ilpo}$ is terminating, this process must terminate, yielding a conversion without peaks, i.e. a valley. $\square$

Example 22. The rewrite relation of Example 1 is decreasing as one easily checks by verifying all peaks in Figure 1 (right). Hence the rewrite relation is confluent by Corollary 21.

4. Well-behaved subrelations of the decreasing proof order

We investigate whether the decreasing proof order $\succ_{ilpo}$ has good properties other than termination, and if not, whether it has subrelations that do have such good properties.

The first observation is that $\succ_{ilpo}$ is technically not a proof order, cf. [11, Definition 7.5.2] as it is not monotonic with respect to composition with French strings.

Example 23. Composition of $\diagdown$ to the right *reverses* the way in which $\diagdown\diagup\diagup\diagup\diagdown$ and $\diagup\diagdown\diagdown\diagdown\diagdown$ are ordered by the decreasing proof order.

The problem witnessed by the example is that although the first string of accents has a smaller area than the latter, the number of grave accents in it is greater leading to a greater increase of its area when extended on the right with an acute accent.

A second observation, due to [5] is that the decreasing proof order $\succ_{ilpo}$ is not monotonic with respect to extending $\succ$.

Example 24. Extending the empty order to $m \succ \ell,\kappa$ *reverses* the way in which $\acute{\ell}\acute{\kappa}\acute{m}$ and $\acute{m}\acute{\kappa}$ are ordered by the decreasing proof order.

The problem witnessed by the example is that when $\succ$-incomparable the (left-to-right) order of elements in a French strings does not matter, something which may change when made $\succ$-comparable.

Neither phenomenon occurs when filling in local peaks by decreasing diagrams. Filling in decreasing diagrams is obviously monotonic with respect to relation extension [12] and composition with French strings. Hence one may wonder whether a well-hehaved order may be 'carved out' from $\succ_{ilpo}$, well-behaved in the sense that it is monotonic in both senses. More generally, one may ask the same question for other good properties, such as e.g. decidability. That we can easily accommodate these desiderata within our set-up, as we show now, which is an indication that that set-up is flexible.

The main idea is that the monotonicity properties can be created by universal quantification. Concretely, one may define French strings s,r to be related if for all well-founded orders $\succ'$ extending $\succ$, and for all French strings p_1,p_2, it holds $p_1sp_2 \succ'_{ilpo} p_1rp_2$. By this definition via universal quantification the relation is clearly 'carved out' from $\succ_{ilpo}$, in the sense that it is a subrelation of $\succ_{ilpo}$. Apart from that it inherits the good property of $\succ_{ilpo}$ being a well-founded order, both monotonicity with respect to composition and relation extension of it are properties created by the definition via universal quantification. However, for automation it is also needed that the proof order (or a good approximation to it) be decidabe. To address decidability, which is not clear for the relation just defined, we propose the following adaptation of it, still based on the same idea.

Definition 25. Define the order $\ggg$ on the French term signature $L^{\sharp}_{\succ}$ 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 $s \gg r$ to hold if for all well-orders $\succ'$ extending $\succ$, i.e. for all *total* terminating transitive relations $\succ'$ such that $\succ \subseteq \succ'$, it holds $s \ggg'_{ilpo} r$, where $\ggg'_{ilpo}$ is the iterative lexicographic path order induced by the order $\ggg'$ on $L^{\sharp}_{\succ'}$, which is in turn induced by the extension $\succ'$ of $\succ$. 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/composition of French strings as well.

Note that the above leftmost (as permitted by the accents) way of ordering argument places not only respects the accents as illustrated in Example 17, but also is preserved under concatenation.

Theorem 26. *The relation $\ggg$ is a decidable well-founded order closed under relation extension and composition with French strings (on both sides), is compatible with the decreasing diagrams technique.*

Proof. We verify each of the properties the relation $\ggg$ is claimed to have separately.

Decidability of $\ggg$ follows from that there are only finitely many labels in any given pair of French strings, that there are (restricted to those labels) only finitely many relations $\succ'$ extending $\succ$ and well-ordering the labels, and that comparing two strings with respect to the iterative lexicographic path order $\ggg'_{ilpo}$, as induced by $\succ'$ via $\ggg'$, is decidable.

That $\ggg$ is well-founded follows from the fact that for each $\succ'$ it's a subrelation of $\ggg'_{ilpo}$, each of which is well-founded as the iterative lexicographic path order induced by $\ggg'$, which in turn is well-founded because it is induced by a well-order $\succ'$ extending $\succ$.

Transitivity of $\ggg$ follows from transitivity of each of the $\ggg'_{ilpo}$, which holds since the iterative lexicographic path order creates transitive relations.

That $\ggg$ is closed under relation extension follows by its definition via all well-orders $\succ'$ extending $\succ$; the well-orders extending an extension of $\succ$ are contained in the well-orders extending $\succ$.

Compatibility with the decreasing diagrams technique follows from Lemma 19 and the fact [12] that decreasing diagrams are preserved under relation extension. Observe that the universal quantification over s,r in the statement of the lemma is not needed anymore, because $\ggg$ is monotonic with respect to French string composition, as we show now.

Note that taking the whole area triple into account in $\ggg$ (so including the numbers of grave and acute accents instead of just the middle component as in $\succ$), makes the order $\ggg$ on the alphabet $L^{\sharp}_{\succ}$ closed under composition (in case concatenation yields an element of $L^{\sharp}_{\succ}$ again). We show by induction on the length of strings that this extends to monotonocity of composition of each $\ggg'_{ilpo}$ induced by a well-order $\succ'$ extending $\succ$. By $\succ'$ being total, the corresponding alphabet $L^{\sharp}_{\succ'}$ of French strings of $\succ'$-incomparable letters in fact consists of French strings on a single label only. Therefore, concatenating a single French letter, say $\hat{\ell}$, to French strings s,r such that $s \ggg'_{ilpo} r$ splits into cases depending on how ℓ relates to the $\succ'$-maximal labels m and κ of which the head symbols s' and r' of s and r are composed.

- if $m \succ' \kappa$ then observe that s' is $\ggg'$-related to each symbol in the French term corresponding to r.
  - if $\ell \succ' m$ then the French terms corresponding to $s\hat{\ell}$ and $r\hat{\ell}$ are obtained from those of s and r by putting the binary function symbol $\hat{\ell}$ on top of both (having these as left arguments and the empty French

string as right argument), and we conclude to $s\hat{\ell} \ggg'_{ilpo} r\hat{\ell}$ by closure of the lexicographic path order under contexts;

  - if $\ell = m$ then the French term corresponding to $s\hat{\ell}$ has $s'\hat{\ell}$ as head symbol which we claim is $\ggg'$-related to each symbol in the French term corresponding to $r\hat{\ell}$. For its head symbol this amounts to $s'\hat{\ell} \ggg' \hat{\ell}$, which obviously holds. For the other symbols this follows by transitivity of $\ggg'$ from $s'\hat{\ell} \ggg' s'$ and the observation above, since these symbols are the symbols of the French term corresponding to r;
  - If $m >' \ell$ then s' is the head symbol of the French string corresponding to $s\hat{\ell}$ as well, and we conclude noting that s' is $\ggg'$-related to each of the function symbols in the French term corresponding to $r\hat{\ell}$, as for each symbol in the latter there is a symbol in s' that is $>'$-related to it. For ℓ this holds since $m >' \ell$ and for the other labels this holds by the observation above.

- if $m = \kappa$ then

  - if $\ell >' m$ then we proceed as above in the corresponding case;
  - if $\ell = m$ then $s'\hat{\ell}$ and $r'\hat{\ell}$ are the head symbols of the French terms corresponding to $s\hat{\ell}$ respectively $r\hat{\ell}$, and we further split cases on whether or not $s' \ggg' r'$.

    If $s' \ggg' r'$ then $s'\hat{\ell} \ggg' r'\hat{\ell}$ follows by monotonicity of $\ggg'$. From this we conclude as above in the corresponding case.

    If $s' = r'$ then the French terms corresponding to $s\hat{\ell}$ and $r\hat{\ell}$ have the same subterms as the ones corresponding to s respectively r, except for an extra empty string subterm in both cases. Because the order on the arguments was assumed to be preserved under concatenation, these subterms are compared lexicographically in the same order as before, hence comparing them yields the same result as before, that is, $s\hat{\ell} \ggg'_{ilpo} r\hat{\ell}$;
  - if $m >' \ell$ then s' and r' are the head symbols of the French terms corresponding to $s\hat{\ell}$ respectively $r\hat{\ell}$, and we further split cases on whether or not $s' \ggg' r'$.

    If $s' \ggg' r'$ then s' is $\ggg'$-related to all function symbols in the French term corresponding to $r\hat{\ell}$ from which we conclude.

    If $s' = r'$ then $s \ggg'_{ilpo} r$ must hold because there is a lexicographically first argument of the head symbol s' such that the corresponding subterms are $\ggg'_{ilpo}$-related (the earlier ones being equal). If this is not the last argument, then we conclude immediately; Otherwise, we conclude by the induction hypothesis for that argument and monotonocity of the lexicographic path order for it. $\square$

Although the above shows already the flexibility of our set-up by 'carving out' a decidable monotonic proof order from the decreasing proof order, it remains to be investigated whether the same can be done to yield decision procedures having low complexity.

5. Conclusion

We have presented a novel proof order, the decreasing proof order, that 'lexicographically combines' the main ingredients of standard proofs of Newman's Lemma (multisets) and of the Lemma of Hindley–Rosen (area). This resulted in a proof order that is compatible with the decreasing diagrams technique, which it extends in the sense that the proof of confluence for the latter can be seen as establishing termination of a particular *strategy* for filling peaks in conversions by decreasing diagrams. Termination of the decreasing proof order entails that *any* strategy for filling peaks would work, i.e. is guaranteed to end in a valley, i.e. in a rewrite proof.

We have developed our results in the setting of involutive monoids. Indeed, the fact that the decreasing proof order is well-founded can be viewed as showing how to lift (in an interesting novel way!) a well-founded order on a set of labels to a well-founded order on the free involutive monoid over that set of labels. We have given two presentations of the latter monoid, with the set of French strings respectively terms as carriers, and this isomorphism was put to good use, devising an order on conversions/French strings via a lexicographic path order on the French terms.

We have focussed attention on giving the foundations of our approach via involutive monoids, but already note here that our set-up is flexible. Two points in case are confluence modulo or up to an equivalence relation, and factorisation of rewrite sequences. One idea in the former case is to let the interpretation of conversion also contain *symmetric* letters $\dot{\ell}$, i.e. for which $\dot{\ell}^{-1} = \dot{\ell}$, the dot suggesting the geometric interpretation (cf. Figure 2 and also the intuition for the proof order based on approximations, provided above) of symmetric letters as points (so that they do not contribute to the area of a French string). In the latter case the main, standard, idea is to employ that factorisation of $\to_1,\to_2$ corresponds to commutation for $\leftarrow_1,\to_2$. Although we claim that extant results as e.g. in [9, 2] and [1] respectively, can be easily accommated in our set-up, we will present substantiation of this claim elsewhere.

Acknowledgments. We would like to thank the participants of TeReSe and the members of the Innsbruck Computational Logic reading group for useful comments. In particular we would like to thank Bertram Felgenhauer for questions on a draft of this paper.

References

[1] Accattoli, B., 2012. An abstract factorization theorem for explicit substitutions calculi. In: Tiwari, A. (Ed.), Rewriting Techniques and Applications, 23rd International Conference, RTA 2012, Nagoya, Japan, May–June 2012. Proceedings. p. 15 pp., to appear in LIPIcs.

[2] Aoto, T., Toyama, Y., 2011. A reduction-preserving completion for proving confluence of non-terminating term rewriting systems. In: Schmidt-

Schauß, M. (Ed.), Rewriting Techniques and Applications, 22nd International Conference, RTA 2011, Novi Sad, Serbia, May–June 2011. Proceedings. Vol. 10 of Leibniz International Proceedings in Informatics (LIPIcs). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, pp. 91–106.

[3] Baader, F., Nipkow, T., 1998. Term rewriting and all that. Cambridge University Press.

[4] Bachmair, L., Dershowitz, N., 1994. Equational inference, canonical proofs, and proof orderings. Journal of the ACM 41 (2), 236–276.

[5] Felgenhauer, B., April 5 2012. Personal communication.

[6] Jacobs, B., 2011. Involutive categories and monoids, with a GNS-correspondence. Foundations of Physics, 1–22.

[7] Jouannaud, J.-P., Oostrom, V. v., 2009. Diagrammatic confluence and completion. In: 36th International Colloquium on Automata, Languages and Programming, ICALP 2009, Rhodes, Greece, July 2009, Proceedings. Vol. 5556 of Lecture Notes in Computer Science. Springer, pp. 212–222.

[8] Klop, J. W., Oostrom, V. v., Vrijer, R. d., 2006. Iterative lexicographic path orders. In: Algebra, Meaning and Computation: Essays dedicated to Joseph A. Goguen on the Occasion of His 65th Birthday. Vol. 4060 of Lecture Notes in Computer Science. pp. 541–554.

[9] Ohlebusch, E., 1998. Church–Rosser theorems for abstract reduction modulo an equivalence relation. In: Nipkow, T. (Ed.), Rewriting Techniques and Applications, 9th International Conference, RTA 1998, Tsukuba, Japan, March–April 1998, Proceedings. Vol. 1379 of Lecture Notes in Computer Science. pp. 17–31.

[10] Oostrom, V. v., 2008. Confluence by decreasing diagrams, converted. In: Voronkov, A. (Ed.), Rewriting Techniques and Applications, 19th International Conference, RTA 2008, Hagenberg, Austria, July 2007. Proceedings. Vol. 5117 of Lecture Notes in Computer Science. Springer, pp. 306–320.

[11] Terese, 2003. Term rewriting systems. Vol. 55 of Cambridge Tracts in Theoretical Computer Science. Cambridge University Press.

[12] Zantema, H., March 29 1994. Personal communication.