Confluence of Non-Terminating Left-Linear Higher-Order Rewrite Theories

Gilles Dowek, Gaspard Férey, Jean-Pierre Jouannaud, Jiaxiang Liu

▶ **To cite this version:**

Gilles Dowek, Gaspard Férey, Jean-Pierre Jouannaud, Jiaxiang Liu. Confluence of Non-Terminating Left-Linear Higher-Order Rewrite Theories. 2021. hal-03126111v1

HAL Id: hal-03126111

https://inria.hal.science/hal-03126111v1

Preprint submitted on 2 Feb 2021 (v1), last revised 21 Mar 2022 (v3)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Confluence of Non-Terminating Left-Linear Higher-Order Rewrite Theories

GILLES DOWEK, INRIA-SACLAY, FRANCE
GASPARD FEREY, LSV, ENS DE PARIS-SACLAY, FRANCE
JEAN-PIERRE JOUANNAUD, LSV, ENS DE PARIS-SACLAY, FRANCE
JIAXIANG LIU, SHENZHEN UNIVERSITY, CHINA

User-defined higher-order rewrite rules are becoming a standard in proof assistants based on intuitionistic type theory. This raises the question of proving that they preserve the properties of β-reductions for the corresponding type systems. In a series of papers, we develop techniques based on van Oostrom's decreasing diagrams that reduce confluence proofs to the checking of various forms of critical pairs for higher-order rewrite rules extending beta-reduction on pure lambda-terms. As shown in a previous paper of the two middle authors, confluence of a terminating set of left-linear rewrite rules is obtained when their critical pairs are joinable, beta-rewrite steps being disallowed. The present paper concentrates on the case where arbitrary beta-rewrite steps are allowed for joining critical pars. The rewrite relation used for analyzing confluence, called orthogonal, gives rise to critical pairs, called nested, that overlap both horizontally, as with parallel rewriting, but also vertically, forming chains of successive overlaps. This second paper terminates our investigation of confluence in the case of left-linear rules.

Additional Key Words and Phrases: Church-Rosser property, orthogonal reductions, decreasing diagrams

ACM Reference Format:
Gilles Dowek, INRIA-Saclay, France, Gaspard Ferey, LSV, ENS de Paris-Saclay, France, Jean-Pierre Jouannaud, LSV, ENS de Paris-Saclay, France, Jiaxiang Liu, Shenzhen University, China. 2021. Confluence of Non-Terminating Left-Linear Higher-Order Rewrite Theories. 1, 1 (February 2021), 27 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The two essential properties of a type theory, consistency and decidability of type checking, follow from three simpler ones: type preservation, strong normalization and confluence. In dependent type theories however, confluence is often needed to prove type preservation and strong normalization, making all three properties interdependent if termination is used in the confluence proof. This circularity can be broken in two ways: by proving all properties together within a single induction [8]; or by proving confluence on untyped terms first, and then successively type preservation, confluence on typed terms, and strong normalization. We develop the latter way here, focusing on untyped confluence.

In a previous paper, we have investigated the case of a terminating set of left-linear rules for which critical pairs can be shown joinable by using rules from $\beta^0 \cup \mathcal{R}$, where β^0 is the restriction of the β-rule for redexes of the form $(\lambda x.u\ y)$, where y is a variable. In the same paper, we explained that allowing the use of arbitrary β-steps would require a more complex notion of critical pair, and that parallel critical pairs cannot suffice in general. The goal of this paper is therefore to address the case of left-linear rules whose critical pairs cannot be joined without using arbitrary β-steps.

Author's address: Gilles Dowek, INRIA-Saclay, France
Gaspard Ferey, LSV, ENS de Paris-Saclay, France
Jean-Pierre Jouannaud, LSV, ENS de Paris-Saclay, France
Jiaxiang Liu, Shenzhen University, China.

2021. XXXX-XXXX/2021/2-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

2

critical pairs, the only available tool for proving confluence in our case is based on van Oostrom's decreasing diagrams [20]. Van Oostrom's theorem is abtract: its application to non-terminating term rewriting relations conceals many difficulties, as is stressed in [1]. An essential aspect of our methodology is to exhibit the rewrite relation for which confluence results from an analysis of its critical pairs. Here, this relation is orthogonal higher-order rewriting which pairs up nicely with beta reductions. Orthogonal rewriting was introduced in [19], where it is called *multi-step* rewriting. Multi-step rewriting aims at overcoming the limitations of left-linear, critical pair free rewriting systems introduced in [11], also called *orthogonal systems*. The main idea is to package several rewriting steps together, using possibly different rules provided they do not overlap, therefore achieving orthogonality inside a given multi-step *by definition of rewriting*. Orthogonal rewriting, as defined here, is a variation of the same idea in which the use of a single rule is allowed in a given multi-step. It turns out that the analysis of confluence becomes then much easier, and that less critical pairs need to be considered. The analysis of orthogonal rewriting and the corresponding Nested Critical Pair Lemma are essential technical contributions of this paper. This lemma shows that critical pairs of orthogonal rewriting may need overlapping lefthand side of rules *horizontally* (at parallel positions), as well as *vertically* (at an increasing sequence of ancestor positions. As a consequence, nested critical pairs may be infinitely many.

Our main theoretical result is then that higher-order rewriting in combination with beta reduction is confluent on untyped terms if all its nested critical pairs admit decreasing rewrite diagrams.

Our computational model based on untyped higher-order reductions is recalled in Section 2, which contains a brief statement of our main result. Higher-order orthogonal reductions are defined in Section 3, which culminates with the nested critical peak theorem. Confluence is studied in Section 4: after recalling the notion of decreasing diagrams, algebraic properties of reductions are developed before to give the confluence theorem holding in our computational model.

2 $\lambda\mathcal{F}$: THE COMPUTATIONAL MODEL

We are interested in rewriting terms of an *untyped* lambda calculus generated by three pairwise disjoint sets, a signature $\mathcal{F}$ of *function symbols*, a set $\mathcal{X}$ of *variables*, and a set $\mathcal{Z}$ of *meta-variables*.

2.1 Terms and substitutions

$\lambda\mathcal{F}$ is a mix of the annotated lambda-calculus and Klop's combinatory reduction systems [13] which extends the calculus introduced in [6] by having annotated abstractions to faithfully abstract dependently typed calculi whose confluence properties are our real target.

Terms are those of an untyped lambda calculus equipped with a ternary abstraction $\lambda x : u.v$, whose second argument u is an arbitrary term called *annotation*, and enriched with $\mathcal{F}$*-headed* terms of the form $f(\overline{u})$ with $f \in \mathcal{F}$ and *meta-terms* of the form $Z(\overline{v})$ with $Z \in \mathcal{Z}$. Only variables can be abstracted over. Elements of the vocabulary have arities, denoted by vertical bars as in $|a|$. Variables have arity zero. The grammar of terms is the following:

$$u, v \coloneqq x \in \mathcal{X} \mid (u\ v) \mid \lambda x{:}u.v \mid f(\overline{u}) \mid Z(\overline{v}) \quad \text{where } f \in \mathcal{F},\ |\overline{u}| = |f|,\ Z \in \mathcal{Z} \text{ and } |\overline{v}| \leq |Z|$$

As is usual, we don't duplicate parentheses, writing $f(x\ y)$ for $f((x\ y))$.

$\lambda\mathcal{F}$ is introduced with a unary untyped abstraction in [6]. Our abstraction operator $''\lambda x : .''$ has arity 2, our syntax here is therefore slightly richer in order to enable abstracting step by step derivation in typed lambda calculi by derivations in $\lambda\mathcal{F}$ (we do not know a confluence preserving encoding of dependently typed derivations into the untyped lambda calculus with a unary abstraction). The calculus without annotation being of course itself an abstraction of $\lambda\mathcal{F}$, all

results presented here adapt straightforwardly to that calculus by forgetting annotations. We will use this facility unannounced in examples originating from non-dependent typed lambda calculi.

Unlike function symbols and Klop's meta-variables, meta-variables here have an arity which is not fixed, but bound. This handy feature used in Dedukti [7] provides a simple syntax for expressions of the form $(\dots(X\ a_1)\dots a_n)$. For example, if $|Z|=1$, the two terms $f(X)$ and $f(\lambda x:nat\ \lambda y:x.X(y))$ –standing for $f(\lambda x:nat\ \lambda y:x.(X\ x))$– coexist (and are different in the absence of extensionality –Dedukti is not extensional).

GF: Did you mean $f(\lambda x.X)$? How are type annotation guessed ?

We use the small letters $f,g,h,\dots$ for function symbols and $x,y,z,\dots$ for variables, and reserve capital letters $X,Y,Z,\dots$ for meta-variables. When convenient, a small letter like x may denote any variable in $\mathcal{X}\cup\mathcal{Z}$. We use the notation $|\_|$ to denote various quantities besides arities, such as the length of a list, the size of an expression or the cardinality of a set. Given a list $\overline{u}$, $\overline{u}[m..n]$ denotes the finite sublist $u_m,\dots u_n$, and $\overline{u}[m..n]\setminus\{i_1,\dots,i_p\}$ the sublist of $\overline{u}[m..n]$ whose elements u_{i_j} for $j\in[1..p]$ have been filtered out. $\overline{u}$ may be omitted, in which case it is the list of natural numbers.

Positions in terms are words over the natural numbers (assuming $|\lambda x.|=1$), using $\cdot$ for concatenation, $\wedge$ for the empty word, P/p for $\{q : p\cdot q\in P\}$, $\leq_{\mathcal{P}}$ for the prefix order (*above*), $\geq_{\mathcal{P}}$ for its inverse (*below*), $>_{\mathcal{P}}$ for the strict part of $\geq_{\mathcal{P}}$, and $p\#q$ for $\neg(>_{\mathcal{P}}\vee\leq_{\mathcal{P}})$ (*parallel*).

Given a term M, we use $\mathcal{V}ar(M)$ and $M\mathcal{V}ar(M)$ for its sets of free variables and of meta-variables respectively, $M(p)$ for its symbol at positions p, and $\mathcal{P}os(M)$, $\mathcal{V}\mathcal{P}os(M)$, $M\mathcal{P}os(M)$ for the following respective sets of positions of M: all positions, the positions of free variables, and of meta-variables. A term M is *ground* if $\mathcal{V}ar(M)=\emptyset$, *closed* if $M\mathcal{V}ar(M)=\emptyset$, and linear if $|M\mathcal{P}os(M)|=|M\mathcal{V}ar(M)|$.

Substitutions are *capture-avoiding* homomorphisms written as $\sigma=\{x_1\mapsto M_1,\dots,x_n\mapsto M_n\}$, or $\sigma=\{\overline{x}\mapsto\overline{M}\}$. where M_i has the form $\lambda\overline{y_i}.N_i$, $|\overline{y_i}|=|x_i|$, and N_i is not an abstraction –this condition is important. Note that x_i denotes here an element of $\mathcal{X}\cup\mathcal{Z}$, and that annotations are omitted in abstractions. $\mathcal{D}om(\sigma)=\{x_1,\dots,x_n\}\subseteq\mathcal{X}\cup\mathcal{Z}$ is the *domain* of σ while $\mathcal{R}an(\sigma)=\bigcup_{i=1}^{i=n}\mathcal{V}ar(M_i)$ is its *image*. A substitution σ can be *restricted to* or *deprived from* (meta-)variables in some set V, written $\sigma_{|V}$ and $\sigma_{\setminus V}$ respectively. As in λ-calculus, substituting in terms requires renaming bound variables to avoid capturing free ones. Then, $x_i\sigma=t_i$ and $y\sigma=y$ if $y\notin\mathcal{D}om(\sigma)$; $f(\overline{t})\sigma=f(\overline{t}\sigma)$; $(u\ v)\sigma=(u\sigma\ v\sigma)$; and $(\lambda x.u)\sigma=\lambda x.u\sigma$ if $x\notin\mathcal{D}om(\sigma)\cup\mathcal{R}an(\sigma)$ (otherwise, as announced, x must be renamed in $\lambda x.u$.) The additional rule for meta-variables is as follows: if $Z\mapsto\lambda\overline{x}.s\in\sigma$, then $(Z(\overline{u}))\sigma=(\lambda\overline{x}[m{+}1..n].s\{\overline{x}[1..m]\mapsto\overline{u}\sigma\}\ \overline{x}[m{+}1..n])$, where $|\overline{u}|=m\leq n=|Z|$, hence delaying the replacement of those arguments that are missing. Annotations for variables in $\overline{x}$, were they present, would disappear by applying the substitution, making them useless. Substitution of meta-variables was introduced by Klop in the case of a fixed arity [13].

Substitutions are extended to sequences of terms and to substitutions in the natural way. We use $\sigma_{|\mathcal{Y}}$ for the restriction of σ to $\mathcal{Y}\cap\mathcal{D}om(\sigma)$ and postfix notation for the application of σ to a term t, writing $t\sigma$, or to a vector of terms $\overline{t}$, writing $\overline{t}\sigma$, or to a substitution τ, writing $\tau\sigma$, and call $t\sigma$ (resp., $\overline{t}\sigma$, $\tau\sigma$) the *instance* of t (resp., $\overline{t}$, τ) by σ. The notation $\mathcal{P}os(\sigma)$ will have the obvious meaning of a sequence of $\mathcal{D}om(\sigma)$-indexed sets of positions.

Let for example s be the term $f(X((x\ y),y))$, where X has two arguments, $(x\ y)$ and y, and σ be the substitution $\{X\mapsto\lambda x'y'z'.g(x',y',z'),y\mapsto a\}$. Then, we get $s\sigma=f(\lambda z'.g((x\ y)\sigma,y\sigma,z'\sigma))=f(\lambda z'.g((x\ a),a,z'))$. Let us now compare with the instance by σ of the term $u=f((X\ (x\ y))\ y)$, in which X is applied successively to $(x\ y)$ and y. Then $u\sigma=f((\lambda x'y'z'.g(x',y',z')\ (x\ a))\ a)$. We can see that $u\sigma$ reduces to $s\sigma$ in two β-steps (anticipating on the next section): substitutions of meta-variables hides those reductions. This actually impacts positively confluence in practice, as we shall discover later.

Gilles Dowek, INRIA-Saclay, France
Gaspard Ferey, LSV, ENS de Paris-Saclay, France
Jean-Pierre Jouannaud, LSV, ENS de Paris-Saclay, France
Jiaxiang Liu, Shenzhen University, China

Given a term u and a list $P = \{p_i\}_{i=1}^{i=n}$ of parallel positions in u, we define the term obtained by *splitting* u along P as $\underline{u}_P = u[Z_1(\overline{x_1})]_{p_1} \dots [Z_n(\overline{x_n})]_{p_n}$ (u is cut below P) and its associated substitution by $\overline{u}^P = \{Z_i \mapsto \lambda\overline{x_i}.u|_{p_i}\}_{i=1}^{i=n}$ (u is cut above P), where, for all $i \in [1, n]$, $\overline{x_i}$ is the list of all variables of $u|_{p_i}$ bound in u above p_i and Z_i is a fresh meta-variable of arity (exactly) $|\overline{x_i}|$. The definition of substitution for meta-variables ensures that $\underline{u}_P\overline{u}^P = u$, which justifies writing $u = u[u|_P]_P$ as a familiar shorthand.

2.2 Product of positions

We now introduce an important operation on positions, that belongs to the folklore of term rewriting although never used explicitely to our knowledge. It will play a key role throughout this paper:

Definition 2.1. Let K be a set of parallel *splitting* positions, P a set of positions such that $\forall p \in P\ \forall k \in K : p \not\geq_{\mathcal{P}} k$ and $Q = \{Q_k\}_{k\in K}$ be a K-indexed family of sets of positions. We define the *(tensor) product* of P, Q via K, denoted $P \otimes_K Q$, to be the set of positions $P \cup \{k \cdot q : k \in K \text{ and } q \in Q_k\}$.

As a particular case, K can be the set of positions in a term u of the variables –and meta-variables– in the domain of some substitution σ, Q_k being a subset of the set of positions of $x\sigma$ such that $u|_k = x$. Since, of course, different occurrences of a variable x are replaced by the same term $x\sigma$, it is possible to change the notation so that the family Q is now indexed by the variables in $\mathcal{D}om(\sigma)$. In that case, K can always be seen as the set of positions of all variables in u (extending then σ by the identity for all remaining variables –and meta-variables– of u), hence K is then determined by the term u itself. In that case, we will usually prefer the notation $P \otimes_u Q$.

The following property, which generalizes the first-order case, follows directly from the definition:

Lemma 2.2. *Given a term u, substitution σ and a family of sets of positions $Q = \{Q_x\}_{x\in\mathcal{D}om(\sigma)}$ with $Q_x \subseteq \mathcal{P}os(x\sigma)$, then $P \otimes_u Q \subseteq \mathcal{P}os(u\sigma)$.*

Example 2.3. Let $u = f(\lambda x.h(X(x)), g(b, Y))$, $\sigma = \{X \mapsto \lambda y.g(a, y), Y \mapsto h(a)\}$, hence $K = \{1^3, 2^2\}$ and $u\sigma = f(\lambda x.h(g(a, x)), g(b, h(a)))$. Let then $P = \{\wedge, 2\}$, $Q_X = \{\wedge, 1\}$ and $Q_Y = \{1\}$. Then, $P \otimes_u Q = \{\wedge, 2\} \cup \{1^3 \cdot \{\wedge, 1\}, 2^2 \cdot 1\} = \{\wedge, 2, 1^3, 1^4, 2^21\}$. The symbols at positions of P, Q and $P \otimes_u Q$ appear in blue in u, σ and $u\sigma$, respectively.

An important particular case of use of the product is that of a term s split along a set of parallel positions K, in which case $u = \underline{s}_K$ and $\sigma = \overline{s}^K$. In that case, the product can be used to define sets of positions implicitly, using the following property:

Lemma 2.4. *Let $O \subseteq \mathcal{P}os(u)$ and K a set of parallel splitting positions in u. Then, there exist unique sets of positions P, Q such that $P = \{p \in P : p \not\geq_{\mathcal{P}} K\}$ and $O = P \otimes_K Q$.*

The product can be extended from sets of positions to sets of sets of positions in the natural way. In the particular case of terms which is used here, u becomes a substitution θ, and K and P two sets of sets of positions indexed by $\mathcal{D}om(\theta)$. A major property of the tensor product is then associativity which expresses the associativity property $(u\sigma)\theta = u(\sigma\theta)$ of substitutions:

Lemma 2.5 (Associativity). *Let u be a term, and σ and θ substitutions such that $\forall x \in \mathcal{V}ar(u) : P_x \subseteq \mathcal{P}os(x\sigma)$ and $\forall y \in \mathcal{V}ar(u\sigma) : Q_y \subseteq \mathcal{P}os(y\theta)$. Then $(O \otimes_u P) \otimes_{u\sigma} Q = O \otimes_u (P \otimes_\sigma Q)$.*

2.3 Reductions

Given a binary relation $\longrightarrow$ on terms, called *rewriting*, we use $\longleftarrow$ for its inverse, and, $\longleftrightarrow$, $\longrightarrow\!\!\!\!\!\rightarrow$, and $\twoheadleftarrow\!\!\!\!\!\rightarrow$, for its closures by, resp.: symmetry; reflexivity and transitivity; reflexivity, symmetry and transitivity (also called *convertibility*). Rewriting terms extends to substitutions as expected.

A term s is in *normal form* if there is no t such that $s \longrightarrow t$. If it is not, we define a (not necessarily unique) *normal form* for s as a term t in normal form, denoted by $s{\downarrow}$, such that $s \longrightarrow\!\!\!\!\!\rightarrow t$.

Termination is the impossibility of an infinite rewriting sequence $t_0 \longrightarrow t_1 \longrightarrow \ldots \longrightarrow t_n \longrightarrow \ldots$. Termination garantees the existence of normal forms for every term.

A *peak* (resp., *local peak*) is a triple of terms s.t. $s \longleftarrow\!\!\!\!\!\leftarrow u \longrightarrow\!\!\!\!\!\rightarrow t$ (resp., $s \longleftarrow u \longrightarrow t$). Two terms s, t are *joinable* if $s \longrightarrow\!\!\!\!\!\rightarrow u \longleftarrow\!\!\!\!\!\leftarrow t$ for some u. *Confluence* is the property that every two convertible terms are joinable. Confluence garantees the unicity of normal forms for every term.

Arrow signs are often decorated by the position at which rewriting takes place, as in $s \xrightarrow{p} t$ (rewriting s at position p) or by a property that this position satisfies, as in $u \xrightarrow{\geq_{\mathcal{P}} p}\!\!\!\!\!\rightarrow v$ (rewrites from u to v take place below p) and $u = v{\downarrow}^{\geq_{\mathcal{P}} P}$ (u is obtained from v by normalizing its subterm $v|_{p \in P}$.)

Two different kinds of reductions coexist in $\lambda\mathcal{F}$, functional and higher-order reductions.

2.4 Functional reductions

Arrow signs used for rewriting will often be decorated, below by a name, and above by a position p or set of positions P, as in $s \xrightarrow[R]{p} t$ or by a property that this position or set of positions satisfies, as in $u \xrightarrow[R]{\geq_{\mathcal{P}} p}\!\!\!\!\!\rightarrow v$ and in $u = v{\downarrow}_R^{\geq_{\mathcal{P}} P}$ (u is obtained from v by normalizing its subterms $v|_{p \in P}$ with R.)

Two different kinds of reductions coexist in $\lambda\mathcal{F}$, functional and higher-order reductions. Both are meant to operate on closed terms. However, rewriting open terms will sometimes be needed, in which case rewriting is intended to rewrite all their closed instances at once.

Functional reduction is the relation on terms generated by the rule $(\lambda x.u : v\ w) \underset{\beta_\alpha}{\longrightarrow} u\{x \mapsto w\}$. The usually omitted α-index stresses that renaming bound variables, called *α-conversion*, is built-in. The argument v, which plays no rôle here, will often be omitted as well.

As is customary [17], the particular case for which v is a variable is denoted by β^0. Note that instantiating a β^0-step may yield a full β-step. For example, $s = (\lambda x.(\lambda y.g(y)\ x)\ a) \xrightarrow[\beta^0]{1\cdot 1} (\lambda x.g(x)\ a) \xrightarrow[\beta]{\Lambda} g(a)$ while $s \xrightarrow[\beta]{\Lambda} (\lambda y.g(y)\ a) \xrightarrow[\beta]{\Lambda} g(a)$. This is our main motivation for using Klop's notion of substitution for meta-variables, among whose numerous benefits is the elimination of β^0-steps that are now hidden under the carpet.

We will also use a particular case of extensionality, for meta-variables only: $\lambda z : u.X[\overline{v}, z] =_{M\eta} X[\overline{v}]$ if $|X| > |\overline{v}|$, z fresh. When oriented from left to right, $M\eta$ is terminating and confluent. It has an even more important property: assume σ is a substitution replacing X by $\lambda\overline{x}z.v$. Then $\lambda z.X[\overline{u}, z]\sigma = \lambda z.v\{\overline{x} \mapsto \overline{u}\} = X[\overline{u}]\sigma$. So, $M\eta$-steps disappear when taking instantiations, a key property for us.

2.5 Higher-order reductions

Higher-order reductions result from rules whose left-hand sides are higher-order patterns in Miller's or Nipkow's sense [16], although they need not be typed:

Definition 2.6 (Pattern). A *pre-redex* of arity n in a term L is an unapplied meta-term $Z[\overline{x}]$ whose arguments $\overline{x}$ are n pairwise distinct variables. A *pre-pattern* is a β-normal term all of whose meta-variables occur in pre-redexes. A *pattern* is a ground pre-pattern which is neither a pre-redex nor an abstraction, that is, is not headed by a meta-variable or λ.

Gilles Dowek, INRIA-Saclay, France
Gaspard Ferey, LSV, ENS de Paris-Saclay, France
Jean-Pierre Jouannaud, LSV, ENS de Paris-Saclay, France
Jiaxiang Liu, Shenzhen University, China

It is important to assume, as does Nipkow, that patterns are β-normal. Note also that patterns are ground: free variables are not needed, one can use meta-variables of arity zero instead. Pre-patterns play an important rôle in pattern matching and unification, since patterns must be deconstructed.

Erasing types from a Nipkow's pattern yields a pattern in our sense, since his pre-redexes being of base type, they cannot be applied. This restriction is not important until later, when we address the question of matching and unification of patterns.

Observe that pre-redexes in pre-patterns occur at parallel positions, whose set plays a key rôle:

Definition 2.7 (Fringe). The *fringe* F_L of a pre-pattern L is the set of parallel positions of its pre-redexes. We denote by $\mathcal{FP}os(L) = \{p \in \mathcal{P}os(L) : F_L \not\leq_{\mathcal{P}} p\}$ the set of *functional positions* of L. For convenience, we define $F_\beta = \{1\cdot 1, 1\cdot 2, 2\}$.

Example 2.8. The term $L = f(\lambda xyz.g(X[x,y,z], X[x,y]))$ is a pattern. Its pre-redexes are the terms $X[x,y,z]$ and $X[x,y]$. Its fringe is the set $F_L = \{1^5, 1^4 2\}$. The term $f(\lambda xyz.g(X[x,y,z])\ (a\ X))$ is also a pattern, its fringe is the set $\{1^6, 2^2\}$. Terms $f(\lambda x.X[x,x])$, $f(X[a])$, $f(X[Y])$, and $f(X\ Y)$, are no patterns.

Note that the set of functional positions coincides with the usual notion for first-order terms, and that patterns have a non-empty set of functional positions. Since patterns are ground terms, for all pre-redexes $Z[\overline{x}] = L|_p$ at position $p \in F_L$ in the pattern L, the variables $\overline{x}$ are all locally bound above p in L.

We can now define higher-order rules and rewriting:

Definition 2.9 (Rule). A (higher-order) *rule* is a triple $i : L \longrightarrow R$, whose (possibly omitted) *index* i is a natural number, left-hand side L is a pattern, and right-hand side R is a ground β-normal term such that $M\mathcal{V}ar(R) \subseteq M\mathcal{V}ar(L)$. The rule is *left-linear* if L is linear.

So, rules are pairs of (specific) ground terms, and the left-hand sides must be headed by a function symbol or an application, but cannot be β-reduced. Both terms may have meta-variables, but don't admit free variables. This allows to clearly separate the object language (which has no meta-variables), from the meta-language (which has meta-variables). Rules, critical pairs and splittings belong to the meta-language.

Definition 2.10 (Higher-order untyped rewriting). Given a term u, a position $p \in \mathcal{P}os(u)$, and a rule $i : L \longrightarrow R$, then u rewrites with i at p, written $u \xrightarrow[i]{p} v$, or $u \xrightarrow[L\longrightarrow R]{p} v$, iff $u|_p = L\gamma$ for some substitution γ, and $v = u[R\gamma]_p$. We write $u \xrightarrow[\mathcal{R}]{p} v$ for $\exists i \in \mathcal{R}, u \xrightarrow[i]{p} v$.

Let's now make our splitting notations fully explicit. Whenever $u \xrightarrow[i]{p} v$, we have by definition:

- $\underline{u}_p = u[X[\overline{x}]]_p$ and $\overline{u}^p = \{X \mapsto \lambda\overline{x}.u|_p\}$ with $\overline{x}$ the variables bound above p in u and X a fresh meta-variable of arity $|\overline{x}|$.
- $u = \underline{u}_p\overline{u}^p = \underline{u}_p\{X \mapsto \lambda\overline{x}.u|_p\} = \underline{u}_p\{X \mapsto \lambda\overline{x}.L\gamma\}$
- $v = \underline{u}_p\{X \mapsto \lambda\overline{x}.R\gamma\}$, hence $\underline{v}_p = \underline{u}_p$, $\overline{v}^p = \{X \mapsto \lambda\overline{x}.R\gamma\}$ and $v|_p = R\gamma$.

Example 2.11. Let $L = \mathtt{der}(\lambda x.\mathtt{times}(A, F[x])) \longrightarrow \mathtt{times}(A, \mathtt{der}(\lambda y.F[y])) = R$ and $\sigma = \{A \mapsto 2, F \mapsto \lambda x.x\}$ be the identity substitution for F. Then, $L\sigma = \mathtt{der}(\lambda x.\mathtt{times}(2,x))$ and $R\sigma = \mathtt{times}(2, \mathtt{der}(\lambda y.y))$, hence $\mathtt{der}(\lambda x.\mathtt{times}(2,x)) \longrightarrow \mathtt{times}(2, \mathtt{der}(\lambda y.y))$. □

Note the simplicity of this definition of higher-order rewriting, which is exactly the same as the definition of rewriting for first-order terms. In sharp contrast with Nipkow [16], we observe that we do not need matching *explicitely* modulo β^0, since the corresponding β^0-steps are now

hidden in Klop's definition of substitution for meta-variables. Besides, we do *not* assume that u, or v, is β-normal -or even β^0-normal-, entirely or up to position p. Two reasons prevent it: firstly, β-normal forms may not exist; and secondly, the techniques we use rely on monotonicity and stability properties, which would not be satisfied were normalization steps used in the definition.

2.6 Higher-order matching and unification of patterns

Given a term u and a left-hand side of rule L, the search for a substitution σ such that $L\sigma = u$, called a *match* of $L = u$, is a matching problem. Since L is ground, the domain of σ is a set of meta-variables, and therefore, matching reduces to the textual replacement of the meta-variables in $\mathcal{D}om(L)$ by their value followed by some β^0-steps: matching a term against a pattern is called *higher-order pattern matching*. An algorithm is given in [6] for the syntax adopted here.

Given now two patterns -or pre-patterns- L, G, the search for a substitution σ such that $L\sigma = G\sigma$, called a *solution* of $L = G$, is a unification problem. Again, the terms obtained by textual replacement of the meta-variables in $\mathcal{D}om(L)$ and $\mathcal{D}om(G)$ by their value can't be exactly equal since β^0steps need to be performed: unification of patterns is called *higher-order unification*. An algorithm is given in [6] which computes a most general higher-order unifier, that is a substitution θ of which any solution σ is an instance: $\sigma = \theta\tau$ for some τ (up to variable renaming). Again, $L\sigma, G\sigma, L\theta\tau$ and $G\theta\tau$ are all equal (up to variable renaming), β^0-equality steps being hidden.

So, by incorporating β^0-steps to the substitution calculus, we were able to get rid of them. They won't show up anywhere, hence eliminating a major technical burden of higher-order rewriting.

2.7 Rewrite theories and their confluence

Rewrite theories are used in various type systems, in particular in Dedukti, to define the conversion rule of the calculus, which is, as is customary, untyped.

Definition 2.12. A *$\lambda\mathcal{F}$-rewrite theory* is a pair $(\mathcal{F}, \mathcal{R})$ made of a user's signature $\mathcal{F}$ and a set $\mathcal{R}$ of higher-order rewrite rules on that signature, defining the rewrite relation $\underset{\lambda\mathcal{F}}{\longrightarrow}$ of $\lambda\mathcal{F}$ as $\underset{\mathcal{R}\cup\beta_\alpha}{\longrightarrow}$.

A $\lambda\mathcal{F}$-rewrite theory $(\mathcal{F}, \mathcal{R})$ is *left-linear* if all rules in $\mathcal{R}$ are left-linear.

The problem we consider is whether a left-linear $\lambda\mathcal{F}$-rewrite theory is confluent, and how to show its confluence by inspecting critical pairs of some sort.

We give two successive answers to this question. The first one is a recall, the second one is new:

A left-linear rewrite theory defines a confluent rewrite relation $\underset{\lambda\mathcal{F}}{\longrightarrow}$ in the following cases:

(1) $\mathcal{R}$ is terminating, and its higher-order critical pairs are joinable with $\mathcal{R}$-steps [6];
(2) the nested higher-order critical pairs of $\mathcal{R}$ have decreasing diagrams using $\mathcal{R}\cup\underset{\beta}{\longrightarrow}$-steps.

Nested critical pairs are obtained by overlapping left-hand sides of rules horizontally (as in parallel critical pairs), as well as vertically, see definition 3.16 and Lemma 3.17. Van Oostrom's notion of decreasing diagram is recalled in Section 4.1.

The reader must realize that, although dependently typed rules may be terminating -which is a standard requirement in type theory, their untyped version may become non-terminating. Further, the first confluence criterium forbids β-steps for joining critical pairs, which may be a real obstacle in practice, as we shall see.

We may wonder why there is no intermediate third answer, based on parallel critical pairs. Indeed, there is [5], but it is not very interesting: firstly, the right-hand side of a rewrite rule may not contain a subterm of the form $X(\overline{t})$ such that some meta-variable Y occurs in $\overline{t}$. In particular, the usual encoding of the β rule $(\lambda x.X[x]\ Y) \to X[Y]$ fails that test; secondly, the critical pairs must satisfy the so-called "Toyama variable condition" which imposes a strong constraint on how

Gilles Dowek, INRIA-Saclay, France
Gaspard Ferey, LSV, ENS de Paris-Saclay, France
Jean-Pierre Jouannaud, LSV, ENS de Paris-Saclay, France
Jiaxiang Liu, Shenzhen University, China

a critical pair can be joined; thirdly, it is often the case that nested critical pairs reduce to the usual higher-order critical pairs (or even parallel critical pairs), in which case "Toyama variable condition" need not be checked since our result applies then as well.

2.8 The theory of global states

An important example of higher-order system that will illustrate our results is Plotkin and Power's theory of global states for a single location [18]. It is described by two types (given for the user's understanding, they are of no use here), Val for values and A for states, a unary operation lk for looking up a state, a binary operation ud for updating a state, and five higher-order rules which satisfy our format:

$$lk \quad : \quad (Val \to A) \to A \qquad \Big| \qquad ud \quad : \quad Val, A \to A$$

$lk(\lambda v.t)$ looks up the state, binds its value to v, and continues with t while $ud(v,t)$ updates the state to v, and continues with t.

$$\begin{array}{rrcl}
(ll) & lk(\lambda w.lk(\lambda v.X(v,w))) & \to & lk(\lambda v.X(v,v)) \\
(uu) & ud(V,ud(W,X)) & \to & ud(W,X) \\
(ul) & ud(V,lk(\lambda v.X(v))) & \to & ud(V,X(V)) \\
(lu) & lk(\lambda v.ud(v,X(v))) & \to & lk(\lambda v.X(v)) \\
(l) & lk(\lambda v.X) & \to & X
\end{array}$$

Our presentation is a simplification of Hamana's [9], whose one rule was actually superfluous. This rewrite theory is proved confluent in [6], but will also reveal an interesting phenomenon here. Note also that rule (ul) is self-nested.

2.9 Basic properties of higher-order rewriting [6]

Lemma 2.13 (Splitting). *Let $s \xrightarrow[L\to R]{q} t$ and $K \subseteq \mathcal{P}os(s)$ such that $q \in K$. Then, $\overline{s}^K \xrightarrow[L\to R]{} \sigma$ and $t = \underline{s}_K\sigma$.*

Lemma 2.14 (Monotonicity). *Let $s \xrightarrow[L\to R]{p} t$ and u a term such that $q \in \mathcal{P}os(u)$. Then, $u[s]_q \xrightarrow[L\to R]{q\cdot p} u[t]_q$.*

By $u[s]_q$, we of course mean $u[X[\overline{x}]]_q\{X \mapsto \lambda\overline{x}.s\}$, omitting the annotations of the bound variables that are here useless, where $\overline{x}$ is the set of variable in s which are bound in u.

Lemma 2.15 (Stability). *Let $s \xrightarrow[L\to R]{p} t$ and σ a substitution. Then $s\sigma \xrightarrow[L\to R]{p} t\sigma$.*

Lemma 2.16 (Substitution Lemma). *Let $u \xrightarrow[\mathcal{R}]{} v$ and $\sigma \xrightarrow[\mathcal{R}]{} \tau$. Then, $u\sigma \xrightarrow[\mathcal{R}]{} \!\!\!\!\to\ v\tau$.*

Lemma 2.17 (Preservation). *Let $u \xrightarrow[i:L\to R]{p} v$ and $K \subseteq \mathcal{P}os(u)$ such that $\forall k \in K : k \geq_{\mathcal{P}} p \cdot F_L$. Then $\underline{u}_K \xrightarrow[i]{p} w$ for some w, and $v = w\overline{u}^K$.*

Now come the commutation properties of local ancestor peaks, either *homogeneous*, between higher-order reductions, or *heterogeneous*, which mix functional and higher-order reductions. The so-called linear ancestor peak property (LAP) is straightforward in case β-step occurs above a higher-order step, but follows otherwise from the preservation Lemma 2.17. When rewriting at a position p occurs below a higher-order rule $i : L \to R$, (LAP) stands for the property $q \geq_{\mathcal{P}} p \cdot F_L$. In order to capture the case where a β-step occurs above a higher-order step, we set $F_\beta = \{1\cdot 1, 1\cdot 2, 2\}$.

Lemma 2.18 (LAPβA). *Let $j \in \mathcal{R}$, u be a term, $p, q \in \mathcal{P}os(u)$ such that $q \geq_{\mathcal{P}} p \cdot F_\beta$ and $v \xleftarrow[\beta]{p} u \xrightarrow[j]{q} w$. Then $v \overset{Q}{\underset{j}{\Longrightarrow}} \xleftarrow[\beta]{p} w$ for some set Q of parallel positions of v such that $\forall q \in Q : q \geq_{\mathcal{P}} p$.*

Lemma 2.19 (LAPβB). *Let $i : L \to R \in \mathcal{R}$, u be a term, and $p, q \in \mathcal{P}os(u)$ such that $q \geq_{\mathcal{P}} p \cdot F_L$ and $v \xleftarrow[i]{p} u \xrightarrow[\beta]{q} w$. Then $v \overset{Q}{\underset{\beta}{\Longrightarrow}} \xleftarrow[i]{p} w$ for some set Q of parallel positions of v such that $\forall q \in Q : q \geq_{\mathcal{P}} p$.*

Lemma 2.20 (LAP$\mathcal{R}$). *Let $i : L \to R \in \mathcal{R}$, $j \in \mathcal{R}$, u be a term, and $p, q \in \mathcal{P}os(u)$ such that $q \geq_{\mathcal{P}} p \cdot F_L$ and $v \xleftarrow[i]{p} u \xrightarrow[j]{q} w$. Then, $v \overset{Q}{\underset{j}{\Longrightarrow}} \xleftarrow[i]{p} w$ for some set Q of parallel positions of v such that $\forall q \in Q : q \geq_{\mathcal{P}} p$.*

These linear ancestor peak (LAP) properties are proved in [6] for the case of a unary abstraction. The same proofs go through in the case of a binary abstraction.

3 ORTHOGONAL REWRITING

Since beta-reductions do not terminate on untyped terms, van Oostrom's technique relying on the existence of a decreasing diagram for each local peak will be our main tool for analyzing confluence of $\lambda\mathcal{F}$ [20]. Its use requires labelling all rewrite steps, we shall see later how.

Using van Oostrom's technique is made difficult by the presence of rewrite rules whose right-hand sides are non-linear, because non-linearities make it impossible to have decreasing diagrams for the so-called ancestor peaks. The solution relies on the use of a new relation whose confluence implies that of $\lambda\mathcal{F}$, so that redexes duplicated by non-linear right-hand sides can be reduced in a single rewrite step. Then, because β-reductions can stack up redexes that were previously at parallel positions, we need to define a notion of simultaneous reduction of several non-overlapping redexes in a term. For instance, given the rewrite rule $f(g(f(x))) \to x$, we can rewrite simultaneously the blue- and red-headed redexes in the term $m(f(g(f(c))), f(g(f(d))))$ and get $m(c, d)$. We can also rewrite simultaneously, in the term $f(g(f(f(g(f(c))))))$ the blue- and red-headed redexes and get c. But, because the rule has a critical pair, the term $f(g(f(g(f(c)))))$ contains two overlapping redexes at positions Λ and $1 \cdot 1$, which cannot be both reduced at the same time.

When two redexes do not overlap, their positions are called *orthogonal*: the examples above show us that two redexes are othogonal in a term u iff u can be split at a position p, yielding the term $\underline{u}_p$ and the substitution $\overline{u}^p$, with one redex in $\underline{u}_p$ and the other one in $\overline{u}^p$. Splitting u along a set of parallel positions P ensures that the redexes in $\underline{u}_P$ and those in $\overline{u}^P$ do not interact, allowing them to be reduced simultaneously.

The idea of orthogonal rewriting appears in the literature under at least two different other names, *parallel reductions* and *multi-step rewriting*. Parallel reductions were introduced by Tait and Martin-Löf to show confluence of the pure λ-calculus. Van Oostrom's multi-step rewriting generalizes this construction for both concrete and abstract rewriting relations. These generalizations are extensively studied in [19], where they are used for analyzing orthogonal rewrite relations, as well as, more generally, orthogonal rewrite steps of non-orthogonal rewrite relations, whether operating on first-order terms, higher-order terms or term-graphs. Note that the notion of othogonality of steps is not needed in critical pair free rewrite systems, like the lambda calculus: the absence of critical pairs implies that any two steps are orthogonal. We refer to [19] for a comprehensive survey of the literature on this subject.

Our coming definition of orthogonal rewriting ensures orthogonality of steps by splitting terms, we claim originality of this handy novelty, and records its construction in a label that generalizes the notion of position of a single rewrite step. This makes sense because we define orthogonal rewriting of a given rewrite rule, instead of a given rewrite system as is the case with multi-step

Gilles Dowek, INRIA-Saclay, France
Gaspard Ferey, LSV, ENS de Paris-Saclay, France
Jean-Pierre Jouannaud, LSV, ENS de Paris-Saclay, France
Jiaxiang Liu, Shenzhen University, China

rewriting –we would then need to record pairs made of a rule name and the positions at which that rule applies. A major advantage of our definition is that it eases the critical pair analysis.

3.1 Definition

Definition 3.1. Parallel rewriting a term s to a term t with rule i at a set of parallel positions $P=\{p_j\}_{j=1}^{n\geq 0}\subseteq \mathcal{P}os(s)$, written $s \underset{i}{\overset{P}{\Longrightarrow}} t$, is simultaneous higher-order rewriting at all positions in P, that is: $s|_{p_j} \underset{i}{\longrightarrow} t_j$ and $t=s[t_1]_{p_1}\dots[t_n]_{p_n}$.

Definition 3.2. Orthogonal rewriting a term s to a term t with rule i at a set of positions $O\subseteq\mathcal{P}os(s)$, written $s \underset{i}{\overset{O}{\Longrightarrow\!\!\!\!\otimes}} t$, is the smallest relation equal to $\underset{i}{\overset{O}{\Longrightarrow}}$ when O is a set of parallel positions, and closed under *product* along a set $K\subseteq\mathcal{P}os(s)$ of parallel *splitting* positions, written $s \underset{i}{\overset{P\otimes_K Q}{\Longrightarrow\!\!\!\!\otimes}} t$ or $s \underset{i}{\overset{P\otimes_{\underline{s}_K} Q}{\Longrightarrow\!\!\!\!\otimes}} t$, defined as:

(i) $P\subseteq\mathcal{P}os(\underline{s}_K)$ and $Q=\{Q_Z\subseteq\mathcal{P}os(\overline{s}^K(Z))\}_{Z\in\mathcal{D}om(\overline{s}^K)}$,

(ii) $\underline{s}_K \underset{i}{\overset{P}{\Longrightarrow\!\!\!\!\otimes}} v$, $\overline{s}^K \underset{i}{\overset{Q}{\Longrightarrow\!\!\!\!\otimes}} \tau$, and $t=v\tau$.

(extending orthogonal rewriting from terms to substitutions in the natural way.)

Orthogonal rewriting reduces to the identity if P, Q are both empty, and to parallel rewriting if P is a set of parallel positions and Q is (a set of) empty (sets) or vice versa.

It is important to notice that minimal positions in O may originate either from P or from Q, instead of only from P. This choice aims at generality, and will ease the study of critical pairs in Section 4.5.

By lemma 2.2, $P\otimes_K Q$ is a set of positions in s as stated in the definition. Note further that the meta-variables introduced by splitting s along K are eliminated from $v\tau$ by instantiation, hence $\mathcal{V}ar(t)\cup M\mathcal{V}ar(t)\subseteq\mathcal{V}ar(s)\cup M\mathcal{V}ar(s)$. In particular, if s is closed, then t is closed too. This is a key condition to ensure that orthogonal rewriting is functional, as we shall soon see.

Example 3.3. Let $\mathcal{R}=\{f(x)\to x\}$, $s=\lambda x.f(g(f(x)))$, $t=\lambda x.g(x)$ and $O=\{1,1\cdot 1\cdot 1\}$.

By splitting s along the singleton set $\{1\cdot 1\}$, we get $\underline{s}_{1\cdot 1}=\lambda x.f(Z(x)) \underset{1}{\overset{}{\Longrightarrow\!\!\!\!\otimes}} \lambda x.Z(x)$, $Z\overline{s}^{1\cdot 1}=\lambda x.g(f(x)) \underset{1\cdot 1}{\overset{}{\Longrightarrow\!\!\!\!\otimes}} \lambda x.g(x)$, hence $s \underset{}{\overset{O}{\Longrightarrow\!\!\!\!\otimes}} \lambda x.Z(x)\{Z\mapsto\lambda x.g(x)\}=\lambda x.g(x)=t$.

Not any set of positions is orthogonal, and indeed orthogonality of a set of positions is defined implicitely by Definition 2.1: the positions in P must be parallel or above the positions in K, and if $p\in P$ is a position in P, then condition (ii) $\underline{s}_K \underset{i}{\overset{P}{\Longrightarrow\!\!\!\!\otimes}} v$ imposes further that there is enough room above K for the whole left-hand side of rule i to take place at position p.

Definition 3.4. A set $P\subseteq\mathcal{P}os(s)$ is a set of orthogonal positions for term s wrt rule $i: L\to R$ iff

(1) $\forall p\in P$, $s \underset{i}{\overset{p}{\longrightarrow}} t$ for some t;

(2) $\forall p,q\in P$, either $p\#q$, or $p\geq_{\mathcal{P}} q\cdot F_L$, or $q\geq_{\mathcal{P}} p\cdot F_L$.

A key property of orthogonal rewriting justifies our definition of a set of orthogonal positions:

Lemma 3.5. *Given a terms s, then $s \underset{i:L\to R}{\overset{P}{\Longrightarrow\!\!\!\!\otimes}} t$ for some t iff P is a set of orthogonal positions for s wrt i.*

Proof. Assume first that $s \underset{i}{\overset{P}{\Longrightarrow\!\!\!\!\otimes}} t$. The proof of orthogonality of P is by induction on the definition of orthogonal rewriting. If P is a set of parallel positions, the result is clear. Otherwise $s=u\sigma$ and

$t = v\tau$, where $u = \underline{s}_K \overset{P}{\underset{i}{\otimes\!\!\Longrightarrow}} v$ and $\sigma = \overline{s}^K \overset{Q}{\underset{i}{\otimes\!\!\Longrightarrow}} \tau$. By induction hypothesis, the property holds for P, Q, which implies (1). To show that (2) holds for $P \otimes_K Q$, it suffices to show that it holds for any pair $\langle p, o\cdot q\rangle$, where $p \in P, o \in K, u(o) = X$ and $q \in Q$. If $o\#p$, the result is true. Otherwise, $o \geq_{\mathcal{P}} p$, and since q is a position in the substitution $\sigma(X)$, $o \cdot q \geq_{\mathcal{P}} p \cdot F_L$.

The converse is by induction on $|P|$. If P is a set of parallel positions, the property holds. Otherwise, let K its canonical splitting, hence $P = P_{min} \otimes_K Q$. It is easy to see that P_{min} and Q are sets of orthogonal positions. By lemma 2.17 applied as many times as needed $\overline{u}^K \overset{P_{min}}{\underset{i}{\Longrightarrow}} v$ for some v. By induction hypothesis applied as many times as needed, $\underline{u}_Q \overset{Q}{\underset{i}{\otimes\!\!\Longrightarrow}} \tau$. Hence $u \overset{P_{min}\otimes_K Q}{\underset{i}{\otimes\!\!\Longrightarrow}} v\tau = t$. □

As a simple property that will often be used unannounced, we have:

Lemma 3.6. *Let P be a set of orthogonal positions for s wrt rule i and K a subset of parallel positions of P such that $P = O \otimes_K Q$. Then O, Q are sets of orthogonal positions wrt i for $\overline{s}^K$ and $\underline{s}_K$, respectively.*

Proof. Property (i) of a set of orthogonal positions holds trivially for $\overline{s}^K$, and for $\underline{s}_K$ by lemma 2.17. Property (ii) holds for both $\underline{s}_K$ and $\overline{s}^K$ since it holds for s. □

Lemma 3.5 leaves open whether the result of an orthogonal step depends upon the splitting used. This is of course not the case as shown in Section 3.3

3.2 Monotonicity and stability properties

These properties are of course inherited from higher-order reductions.

Lemma 3.7 (Head montonicity). *Let $s \overset{P}{\underset{i}{\otimes\!\!\Longrightarrow}} t$ with $\Lambda \in P_{min}$. Then, $u[s]_p \overset{p\cdot P}{\underset{i}{\otimes\!\!\Longrightarrow}} u[t]_p$.*

Proof. Since $\Lambda \in s$, the substitution $\{X \mapsto \lambda\overline{x}.s\}$ is preserving. Hence, by Definition 3.2, $u[s]_p = u[X(\overline{x})]_p\{X \mapsto \lambda\overline{x}.s\} \overset{\varnothing\otimes_p P}{\underset{i}{\otimes\!\!\Longrightarrow}} u[t]_p$. Since $\varnothing \otimes_p P = p \cdot P$, we are done. □

jpjWhere do we use it ?

Lemma 3.8 (Context removal). *Let $u \overset{P}{\underset{i}{\otimes\!\!\Longrightarrow}} v$ and $p \in P_{min}$. Then, $u|_p \overset{P'}{\underset{i}{\otimes\!\!\Longrightarrow}} v|_p$ for some $P' = \{q : p \cdot q \in P\}$.*

Proof. By induction on the definition of orthogonal higher-order rewriting. If $\Lambda \in P$, then $p = \Lambda$ and the result holds. If $u \overset{P}{\underset{i}{\Longrightarrow}} v$, then the result follows from the definition parallel rewriting. Otherwise, let $u \overset{O\otimes_K Q}{\underset{i}{\otimes\!\!\Longrightarrow}} v$, hence $s = \underline{u}_K \overset{O}{\underset{i}{\otimes\!\!\Longrightarrow}} t$, $\sigma = \overline{u}^K \overset{Q}{\underset{i}{\otimes\!\!\Longrightarrow}} \tau$, $u = s\sigma$ and $v = t\tau$. There are two cases:

(1) $p = o \cdot q$ with $o \in K$, $u|_o = X(\overline{x})$ and $q \in Q_{min}$. By induction hypothesis, $\sigma(X)|_q \overset{Q'}{\underset{i}{\otimes\!\!\Longrightarrow}} \tau(X)|_q$. Since $\sigma(X)|_q = u|_{o\cdot q} = u|_p$, we are done.

(2) $p \in O_{min}$. By induction hypothesis, $s|_p \overset{P'}{\underset{i}{\otimes\!\!\Longrightarrow}} t|_p$. By Definition 3.2, $u|_p = s|_p\sigma \overset{P'\otimes_{s|_p} Q}{\underset{i}{\otimes\!\!\Longrightarrow}} t|_p\tau = v|_p$ and we are done.

In both cases, verifying the form of the resulting set of positions is a routine calculation. □

Lemma 3.9. *Orthogonal rewriting is monotonic: $s \overset{P}{\underset{i}{\otimes\!\!\Longrightarrow}} t$ implies $u[s]_p \overset{p\cdot P}{\underset{i}{\otimes\!\!\Longrightarrow}} u[t]_p$.*

Gilles Dowek, INRIA-Saclay, France
Gaspard Ferey, LSV, ENS de Paris-Saclay, France
Jean-Pierre Jouannaud, LSV, ENS de Paris-Saclay, France
Jiaxiang Liu, Shenzhen University, China

Proof. By splitting the term $u[s]_p$ along the set $p \cdot P_{min}$, we get $u[s]_p = u[\underline{s}_{P_{min}}]_p \overline{s}^{P_{min}}$. By Lemma 3.8, $s|_{P_{min}} \overset{P/P_{min}}{\underset{i}{\otimes\!\!\Longrightarrow}} t|_{P_{min}}$. We can then conclude easily with Lemma 3.7. □

Monotonicity generalizes easily to a set of parallel positions:

Lemma 3.10 (Monotonicity). *Orthogonal rewriting is monotonic: $\sigma \overset{Q}{\underset{i}{\otimes\!\!\Longrightarrow}} \tau$ implies $u\sigma \overset{\varnothing \otimes_u Q}{\underset{i}{\otimes\!\!\Longrightarrow}} u\tau$.*

Lemma 3.11 (Stability). *Let $s \overset{P}{\underset{i}{\otimes\!\!\Longrightarrow}} t$ and σ a substitution. Then $s\sigma \overset{P}{\underset{i}{\otimes\!\!\Longrightarrow}} t\sigma$.*

Proof. If P is a set of parallel positions, the property follows directly from Lemma 2.15. Otherwise, $P = O \otimes_K Q$, $\underline{s}_K \overset{O}{\underset{i}{\otimes\!\!\Longrightarrow}} u$, $\overline{s}^K \overset{Q}{\underset{i}{\otimes\!\!\Longrightarrow}} \theta$ and $t = u\theta$. Since K is a set of parallel positions in $\mathcal{P}os(s)$, splitting $s\sigma$ yields $\underline{s\sigma}_K = \underline{s}_K\sigma$ and $\overline{s\sigma}^K = \overline{s}^K\sigma$. By induction hypothesis, $\underline{s}_K\sigma \overset{O}{\underset{i}{\otimes\!\!\Longrightarrow}} u\sigma$ and $\overline{s}^K\sigma \overset{Q}{\underset{i}{\otimes\!\!\Longrightarrow}} \theta\sigma$. Since splitting uses fresh meta-variables, $\mathcal{D}om(\theta) \cap \mathcal{D}om(\sigma) = \varnothing$. Hence $(u\sigma)\theta\sigma = u\theta\sigma = t\sigma$. Definition of orthogonal rewriting yields the result. □

Lemma 3.12 (Linearization). *Let $u \overset{O}{\underset{i}{\otimes\!\!\Longrightarrow}} v$. Then $u \underset{i}{\longrightarrow\!\!\!\!\!\rightarrow} v$.*

Proof. By induction on the definition of orthogonal rewriting. If $u \overset{O}{\underset{i}{\Longrightarrow}} v$, the result is clear. Otherwise, $O = P \otimes_K Q$, $u = s\sigma$ with $s = \underline{u}_K$ and $\sigma = \overline{u}^K$, $s \overset{P}{\underset{i}{\otimes\!\!\Longrightarrow}} t$, $\sigma \overset{Q}{\underset{i}{\otimes\!\!\Longrightarrow}} \tau$, and $v = t\tau$. By stability, $u = s\sigma \overset{P}{\underset{i}{\otimes\!\!\Longrightarrow}} t\sigma$, and by monotonicity, $t\sigma \overset{\varnothing \otimes_t Q}{\underset{i}{\otimes\!\!\Longrightarrow}} t\tau = v$. We conclude by induction applied twice. □

This proof shows that redexes can be linearized using a top-down strategy, that is a redex at some position p is always reduced before anorher redex at a position $p \cdot q$. We could of course base the proof on the other reduction $u = s\sigma \overset{\varnothing \otimes_K Q}{\underset{i}{\otimes\!\!\Longrightarrow}} s\tau \overset{P}{\underset{i}{\Longrightarrow}} t\tau = v$, which would give us a bottom up strategy. Using any other strategy would be possible but require commutation properties that we do not intend to develop here. Next section will provide another way to construct an arbitrary linearization strategy.

3.3 Splitting

Definition 3.2 is very flexible in the way splitting the input term is possible, minimal rewriting positions taking place above and/or below the set of splitting positions. This design choice has an important consequence: our product construction is both horizontal and vertical in the way a set of orthogonal positions can be extended with another by making their product.

We show here that any orthogonal rewrite step $s \overset{P}{\underset{i}{\otimes\!\!\Longrightarrow}} t$ can actually be defined via a *canonical* splitting, for which the minimal rewriting positions are all (strictly) above the splitting set, whose all elements are rewrite positions themselves:

Definition 3.13. Let $P \subseteq \mathcal{P}os(s)$ be a set of orthogonal positions in s, and K a subset of P such that $P = O \otimes_K Q$. The set K of *splitting positions* is said to be *canonical* if $O = P_{min}$ and $K = (P \setminus O)_{min}$.

Assuming $O = P_{min}$ is not enough for uniqueness of the canonical splitting set. On the other hand, assuming $P = (P \setminus P_{min})_{min}$ would imply $O = P_{min}$, hence give an equivalent definition.

Lemma 3.14 (Canonical splitting). *Let P be a set of orthogonal positions such that $u \overset{P}{\underset{i}{\otimes\!\Longrightarrow}} u'$, and K its canonical splitting such that $P = P_{min} \otimes_K P'$. Then, $u \overset{P_{min}\otimes_K P'}{\underset{i}{\otimes\!\Longrightarrow}} u'$.*

Proof. By induction on $|u|$. The result holds if P is a set of parallel positions, hence $P = P_{min}$, taking $K = \emptyset$ and $P' = \emptyset$.

Otherwise, $P = O \otimes_{K'} Q$. Let $s = \underline{u}_{K'}$, $\sigma = \overline{u}^{K'}$, $s \overset{O}{\underset{i}{\otimes\!\Longrightarrow}} s'$ and $\sigma \overset{Q}{\underset{i}{\otimes\!\Longrightarrow}} \sigma'$ for some s', σ', and $u \overset{O\otimes_s Q}{\underset{i}{\otimes\!\Longrightarrow}} s'\sigma'$. Cases $O = \emptyset$ or $Q = \emptyset$ are left to the reader. Otherwise, the case is depicted at Figure 1 (left). Let $t = \underline{s}_{(O\setminus O_{min})_{min}}$, $\tau_1 = \overline{s}^{(O\setminus O_{min})_{min}}$ and $O = O_{min} \otimes_t O'$. By induction hypothesis, $s \overset{O_{min}\otimes_t O'}{\underset{i}{\otimes\!\Longrightarrow}} s'$.

Q may contain positions which are minimal in P. Let $Q = Q_1 \uplus Q_2 \uplus Q_3$, where $Q_1 >_{\mathcal{P}} (O\setminus O_{min})_{min}$, $Q_2 >_{\mathcal{P}} O_{min} \wedge Q_2 \# (O\setminus O_{min})_{min}$, and $Q_3 \# O_{min}$. Note that $P_{min} = O_{min} \cup (Q_3)_{min}$. Since meta-variables must ocur linearly in s, we split σ as its restrictions σ_1, σ_2 and σ_3 to the meta-variables of s which occur above $(Q_1)_{min}$, $(Q_2)_{min}$, and $(Q_3)_{min}$ respectively. Using now successively Lemma 3.8 for σ_2 and the induction hypothesis for σ_3, we get $\sigma_2 \overset{\emptyset\otimes_{\theta_2} Q'_2}{\underset{i}{\otimes\!\Longrightarrow}} \theta'_2\gamma'_2 = \sigma'_2$, with $\sigma_2 = \theta_2\gamma_2$ (note that $\theta'_2 = \theta_2$), and $\sigma_3 \overset{(Q_3)_{min}\otimes_{\theta_3} Q'_3}{\underset{i}{\otimes\!\Longrightarrow}} \theta'_3\gamma'_3 = \sigma'_3$, with $\sigma_3 = \theta_3\gamma_3$. We finally construct v and γ, hence defining v' and γ'. Let $v = t(\theta_2 \cup \theta_3)$, $v' = t'(\theta'_2 \cup \theta'_3)$, $\gamma = \tau_1\sigma_1 \cup \gamma_2 \cup \gamma_3$ and $\gamma' = \tau'_1\sigma'_1 \cup \gamma'_2 \cup \gamma'_3$. Let now $P' = O' \otimes_{\tau_1} Q_1 \cup Q'_2 \cup Q'_3$. Using associativity and stability, we get $u \overset{P_{min}\otimes_v P'}{\underset{i}{\otimes\!\Longrightarrow}} v'\gamma' = u'$. □

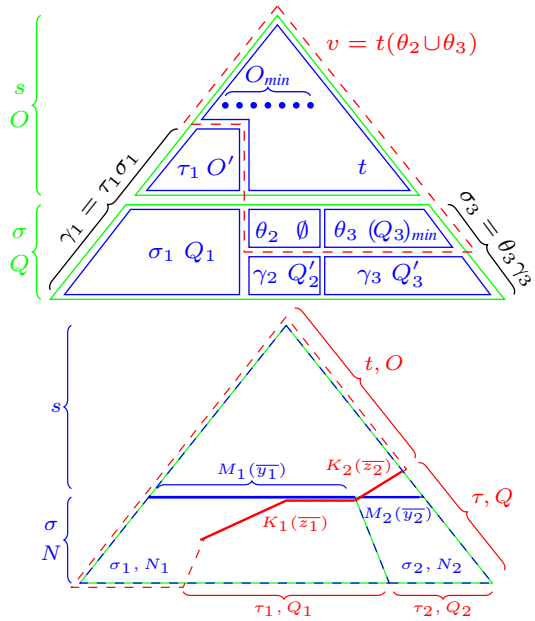


Fig. 1. Proof of Lemma 3.14 with $P' \neq \emptyset$. Proof of Lemma ??, Case 3.

An important direct consequence of canonical splitting is that the outcome of an orthogonal rewrite step is entirely determined by its input term and set of orthogonal positions:

Gilles Dowek, INRIA-Saclay, France
Gaspard Ferey, LSV, ENS de Paris-Saclay, France
Jean-Pierre Jouannaud, LSV, ENS de Paris-Saclay, France
Jiaxiang Liu, Shenzhen University, China

Lemma 3.15 (Functionality). *Let* $P \otimes_K Q = P' \otimes_{K'} Q'$, $u \overset{P\otimes_K Q}{\underset{i}{\otimes\Longrightarrow}} v$ *and* $u \overset{P'\otimes_{K'} Q'}{\underset{i}{\otimes\Longrightarrow}} v'$. *Then* $v = v'$.

The tensor notation has shown itself to be very convenient: we will use it systematically, in particular when P is empty, writing then $s\sigma \overset{\varnothing\otimes_s Q}{\underset{i}{\otimes\Longrightarrow}} s\tau$, or when Q is empty, writing $s\sigma \overset{P\otimes_s \varnothing}{\underset{i}{\otimes\Longrightarrow}} t\sigma$. It will serve as a type-checking device to control complex rewriting calculations.

3.4 Critical peaks

Our formulation of the definition of orthogonal rewriting has one main purpose: ease the definition of critical pairs and the proof of the associated critical peak property.

Generating the minimal *nested critical peaks* that characterize the confluence of orthogonal rewriting requires computing the overlaps of two orthogonal rewriting steps issuing from a term. Such peaks are defined by two different rules, each lefthand side overlapping alternatively on the other at a set of parallel positions, but not between themselves so that there are two different orthogonal steps issuing from the same term. These overlaps form both *horizontal* chains when one lefthand side overlaps the other at several parallel positions, and *vertical* chains when there is an alternation of overlaps between the two lefthand sides.

Definition 3.16 (Nested overlaps). Given two rules $k : L \to R$ and $l : G \to D$, a term u, a substitution σ, two sets $P = \{\wedge\} \cup \{p_i\}_{i\in I}$ and $Q = \{q_j\}_{j\in J}$ of positions in $\mathcal{FP}os(u)$, and a set $\{L_i, G_j\}_{i\in I, j\in J}$ of renamings of L, G that share no variables between themselves nor with L, then $\langle u, k, P, l, Q, \sigma\rangle$ (u, σ being possibly omitted) is a *nested overlap* of G onto L iff the following conditions hold:

(i) σ satisfies the equality $u = L\sigma \wedge \bigwedge_{i\in I} u|_{p_i} = L_i\sigma \wedge \bigwedge_{j\in J} u|_{q_j} = G_j\sigma$;

(ii) $\forall i\ \exists j\ (p_i \in q_j \cdot \mathcal{FP}os(G))$ and $\forall i \neq i'\ (p_{i'} \notin p_i \cdot \mathcal{FP}os(L))$;

(iii) $\forall j\ (q_j \in \mathcal{FP}os(L) \vee \exists i\ (q_j \in p_i \cdot \mathcal{FP}os(L)))$ and $\forall j \neq j'\ (q_{j'} \notin q_j \cdot \mathcal{FP}os(G))$.

The nested overlap is called *trivial* if $Q = \emptyset$ and *critical* if σ is minimal in the subsumption ordering modulo β^0. The set of critical nested overlaps of rule j onto rule i is denoted by $\mathcal{S}cno(l, k)$.

Condition (i) does not make visible the fact that matching is not syntactic, but modulo β^0 instead, since β^0-steps are buried inside the definition of substitution for meta-variables. It says that u is entirely defined by the tuple $\langle k, P, l, Q, \sigma\rangle$, and that the subterms of u at other positions in P are k-redexes, while those at positions in Q are l-redexes. Condition (ii) says that k-redexes but the topmost one overlap an above l-redex but no other k-redex. Condition (iii) for l-redexes is similar. When P and Q are singleton sets, u is then a usual higher-order overlap between the two rules.

One may wonder why we call these critical peaks nested rather than orthogonal. First, orthogonality refers explicitly to the absence of critical pairs, so an orthogonal critical pair would be kind of self-contradicting. Another reason is that there is a single rule lefthand side sitting at the top of a seed. Therefore, all redexes occurring in a seed are nested inside that lefthand side's instance, whether they extend the seed construction vertically or horizontally.

Non-trivial nested critical overlaps give rise to critical local peaks:

Lemma 3.17. *Given* $\langle u, k, P, l, Q, \sigma\rangle \in \mathcal{S}cno(k : L \to R, l : G \to D)$, *then* $v \overset{P}{\underset{k}{\otimes\Longleftarrow}} u = L\sigma \overset{Q}{\underset{l}{\otimes\Longrightarrow}} w$. *The pair* (v, w) *is called a* nested critical pair *of rule* l *onto rule* k *at positions* P, Q.

3.5 Calculation of nested critical pairs

The previous definition of a nested overlap does not allow us computing σ, hence the critical nested overlaps, since the positions p_k and q_l are positions in $L\sigma$, σ being yet unknown. An algorithm computing these overlaps must therefore proceed by successive unifications, possibly alternating between the two lefthand sides. Computing these overlaps requires then some bookkeeping, both

in terms of substitutions and overlapping positions, in order to avoid self-overlaps of L and G. This is achieved by the next definition:

Definition 3.18 (Seeds). Given two rules $k : L \to R, l : G \to D$ from $\mathcal{R}$, the set $p\mathcal{S}_l^k$ of (k,l)-*pre-seeds* is the smallest set of tuples (s, σ, P, Q), where P and Q are lists of positions in $\mathcal{FP}os(s\sigma)$ of L-redexes and G-redexes respectively, such that

(i) $p\mathcal{S}_l^k$ contains the *trivial pre-seed* $(L, \{\,\}, \{\wedge\}, \{\,\})$;

(ii) $p\mathcal{S}_l^k$ is closed under *nested overlapping*: given $(s, \sigma, P, Q) \in p\mathcal{S}_l^k$, two lists of parallel positions $\{p_i \in \mathcal{FP}os(s\sigma) : p_i \geq_{\mathcal{P}} P \cdot F_L\}_{i \in I}$ and $\{q_j \in \mathcal{FP}os(s\sigma) : q_j \geq_{\mathcal{P}} Q \cdot F_G\}_{j \in J}$ which are not both empty and whose elements are pairwise incomparable, renamings $\{L_i\}_{i \in I}$ of L and $\{G_j\}_{j \in J}$ of G such that $\forall i, j, \mathcal{V}ar(L_i), \mathcal{V}ar(G_j)$ and $\mathcal{V}ar(s\sigma)$ are pairwise disjoint sets, and τ a most general unifier of the equation $\bigwedge_{i \in I}(s\sigma)|_{p_i} = L_i \wedge \bigwedge_{j \in J}(s\sigma)|_{q_j} = G_j$, the *non-trivial pre-seed* $(s\sigma, \tau, P \cup \{p_i\}_{i \in I}, Q \cup \{q_j\}_{j \in J})$ belongs to $p\mathcal{S}_l^k$.

We call *seed* a triple $(u\tau\downarrow, P, Q)$ where (u, τ, P, Q) is a pre-seed. A seed is *trivial* if $Q = \emptyset$. The set of seeds is denoted by $\mathcal{S}_l^k$.

Note that unifying alternatively with L and G would complicate the definition.

We now show that the sets of seeds and of critical nested overlappings are one-to-one (up to variable renaming of bound variables). This statement includes trivial critical nested overlappings and trivial seeds in order to facilitate its proof.

Theorem 3.19. *Let R be a higher-order rewriting system such that $k, l \in R$. Then, $\langle s, k, P, l, Q, \sigma\rangle \in \mathcal{S}cno(l, k)$ iff $(s, P, Q) \in \mathcal{S}_l^k$.*

Proof. Note first that trivial critical nested overlappings and trivial seeds correspond.

- $\mathcal{S}_l^k \subseteq \mathcal{S}cno(l, k)$. It suffices to show that $\mathcal{S}cno(l, k)$ is "closed under nested overlapping". By definition of pre-seeds, let $(s, \sigma, P, Q) \in p\mathcal{S}_l^k$, $\{p_i\}_i$ and $\{q_j\}_j$ be sets of positions, $\{L_i\}_i$ and $\{G_j\}$ be renamings of L, R, and τ a substitution satisfying the condition (ii) of Definition 3.18. Using the induction hypothesis and the above conditions (ii), it is easy to verify that $\langle s\sigma, k, P, l, Q, \sigma\rangle \in \mathcal{S}cno(l, k)$.
- $\mathcal{S}cno(l, k) \subseteq \mathcal{S}_l^k$, the converse statement. Let $\langle s, \sigma, k, P, l, Q\rangle \in p\mathcal{S}cno(l, k)$, and consider the sets P', Q' of positions in P, Q which are maximal in $P \cup Q$. Let $P \setminus P' = \{p_i\}_i$ and $Q \setminus Q' = \{q_j\}_j$. By condition (i) and the fact that σ is minimal, $\sigma = \theta\tau$ and $s = t\tau$, where θ is the most general unifier of the equation $t = L\theta \wedge \bigwedge_i u|_{p_i} = L_i\theta \wedge \bigwedge_j u|_{q_j} = G_j\theta$. By conditions (ii,iii), $\langle t, \theta, k, P \setminus P', l, Q \setminus Q'\rangle \in p\mathcal{S}cno(l, k)$ is a critical nested overlapping. By induction hypothesis, $(t, \theta, P, Q) \in \mathcal{S}_l^k$. By condition (i) and closure under nested overlappings $(t, \tau, P, Q) \in p\mathcal{S}_l^k$, hence $(t\tau = s, P, Q) \in \mathcal{S}_l^k$ and we are done. □

Example 3.20 (Rules lu and ul of the theory of global states). These two rules, like their well-chosen names, overlap themselves *ad libitum* because the head function symbol of each lefthand side is heading a strict subterm of the other which will be part of the substitution when unifying the rules. We consider the case *ul* above *lu*, and index their free variables V and X by the number of runs in the computation of pre-seeds. The initial seed in $p\mathcal{S}_{lu}^{ul}$ is $(x, \sigma = \{x \mapsto ud(V_0, l_k(\lambda v.X_0[v]))\}, \{\wedge\}, \{\,\})$.

The only possible overlap with *lu* requires $Q_1 = \{2\}$, which is above the fringe of *ul*'s lefthand side. Unification yields $\tau_1 = \{X_0 \mapsto \lambda z.ud(z, X_1[z])\}$, hence $(ud(V_0, l_k(\lambda v.X_1[v])), \tau_1, \{\wedge\}, \{2\})$ is added to $p\mathcal{S}_{lu}^{ul}$. Because position $2{\cdot}1{\cdot}1$ in the overlap $ud(V_0, l_k(\lambda v.ud(v, X_1[v])))$ is at the fringe of *ul*'s lefthand side, we take $P_2 = \{2{\cdot}1{\cdot}1\}$ and unify the corresponding subterm with the renamed lefthand side of *ul*, yielding $\tau_2 = \{x_1 \mapsto \lambda z.lk(\lambda v.X_2[v])$. The seed $(ud(V_0, l_k(\lambda v.X_1[v])), \tau_2, \{2{\cdot}1{\cdot}1\}, \{2\})$ is added to $p\mathcal{S}_{lu}^{ul}$. We continue with $Q_3 = \{2{\cdot}1{\cdot}1{\cdot}2\}$, and so on. We get two infinite families whose seeds

Gilles Dowek, INRIA-Saclay, France
Gaspard Ferey, LSV, ENS de Paris-Saclay, France
Jean-Pierre Jouannaud, LSV, ENS de Paris-Saclay, France
Jiaxiang Liu, Shenzhen University, China

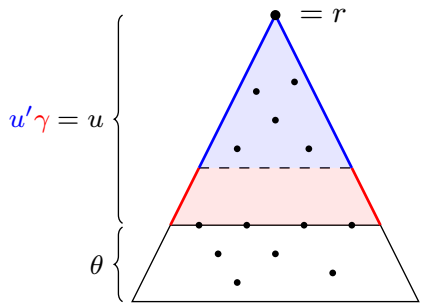


Fig. 2. Critical peak property

are $(ud(V_0, lk(\lambda v.ud(v, lk(..., lk(\lambda v.X_{2n}[v])...)))), \{2{\cdot}1{\cdot}1)^{2p}{\cdot}2 : 2p \leq n\}, \{2{\cdot}(1{\cdot}1{\cdot}2)^{2p+1} : 2p \leq n\})$, and $(ud(V_0, lk(\lambda v.ud(v, lk(..., lk(\lambda v.ud(v, X_{2n+1}[v])^2...)^4, \{2{\cdot}1{\cdot}1)^{2p+1}{\cdot}2 : 2p+1 \leq n\}, \{2{\cdot}(1{\cdot}1{\cdot}2)^{2p} : 2p \leq n\})$.

In the recursive definition of pre-seeds, the overlapping substitution σ obtained tells us where to overlap next, while the maximal positions in P and Q of these overlaps tell us where to not overlap L and G respectively. In particular, the initial overlap is impossible with L, unless $k=l$, but is possible with G. Subsequent overlaps may involve both L and G. Alternating overlaps with L and with G would eliminate some redundancies to the price of storing the run parity in the tuple.

Since L, G are left-linear, higher-order unification of G with some subterm of L (or vice-versa), does not instantiate these terms beyond their boundaries. It follows that each redex instance of L (resp., G) must overlap some lefthand side G (resp., L) obtained at the previous run. This remark is a property of the definition when the rules are left linear, building it in the definition is useless.

3.6 Critical peak property

We conclude this section with the nested critical peak property:

Theorem 3.21 (Nested Critical Peak). *Let* $s \underset{i:L\to R}{\overset{\{\Lambda\}\cup P}{\Longleftarrow\!\!\otimes}} r \underset{j:G\to D}{\overset{Q}{\otimes\!\!\Longrightarrow}} t$ *with* $Q \cap \mathcal{FP}os(L) \neq \emptyset$. *Then,* $\exists u, v, w, u', v', w', \theta, \sigma, \tau, \gamma, O, O', P', Q'$ *st:*

(i) $r = u\theta, s = v\sigma, t = w\tau, u = u'\gamma, v = v'\gamma, w = w'\gamma$,

(ii) $v' \underset{i}{\overset{O}{\Longleftarrow\!\!\otimes}} u' \underset{j}{\overset{O'}{\otimes\!\!\Longrightarrow}} w'$ *is a nested critical peak*,

(iii) θ *is a substitution st* $\sigma \underset{i}{\overset{P'}{\Longleftarrow\!\!\otimes}} \theta \underset{j}{\overset{Q'}{\otimes\!\!\Longrightarrow}} \tau$,

(iv) $P = O \otimes_u P'$ *and* $Q = O' \otimes_u Q'$.

This statement is pictured at Figure 2. The substitution θ is obtained by splitting r as $u\theta$ so that u contains a critical overlap. The substitution γ expresses the property that u is an instance of the most general critical peak (v', u', w'), hence $u = u'\gamma$. These substitutions play different roles, the substitution θ is rewritten while the substitution γ is not, that's why they are kept separate.

Proof. By assumption on Q, the two orthogonal rewrites from r overlap. Let O, O', where $O = \{O_k\}_{k\in I}, O' = \{O'_l\}_{l\in J}$, be the maximal subsets of P, Q, that satisfy conditions (ii, iii) of Definition 3.16. Then, it is easy to verify that the tuple $\langle r, i, \{\Lambda\}\cup O, j, O'\rangle$ is a nested overlap whose associated nested peak defined in Lemma 3.17 is $s' \underset{i}{\overset{\{\Lambda\}\cup O}{\Longleftarrow\!\!\otimes}} r \underset{j}{\overset{O'}{\otimes\!\!\Longrightarrow}} t'$ for some s', t'.

Let $N = ((P\cup Q)\setminus(O\cup O'))_{min}$, $u = \underline{r}_N$ and $\theta = \overline{r}^N$, hence $u\theta = r$. By Lemma 2.4, $P = O \otimes_N P'$ and $Q = O' \otimes_N Q'$. By definition of orthogonal rewriting and maximality of O, O', the positions $n \in N$ do

not belong to any set of the form $p \cdot \{o <_{\mathcal{P}} F_L \cup F_G\}$ unless $p = n$ or $q \cdot \{o <_{\mathcal{P}} F_L \cup F_G\}$ unless $q = n$. Therefore $s = v\sigma$ and $t = v\tau$ by Lemma 3.15.

We have got the peaks $v \underset{i}{\overset{\{\Lambda\}\cup O}{\Longleftarrow\!\!\otimes}} u \underset{j}{\overset{O'}{\otimes\!\!\Longrightarrow}} w$ and $\sigma \underset{i}{\overset{P'}{\Longleftarrow\!\!\otimes}} \theta \underset{j}{\overset{Q'}{\otimes\!\!\Longrightarrow}} \tau$. The first yields the equational formula $L\varphi = u \wedge \bigwedge_{i\in I, p\in O, j\in J, q\in O'} u|_p = L_i\varphi_i \wedge u|_q = G_j\psi_j$, where $\{L_i\}_{i\in I}$ and $\{G_i\}_{j\in J}$ are variable renamings of L, G sharing no variables among themselves nor with L (nor u). The corresponding unification problem is therefore unifiable. Hence $\varphi \cup \bigcup_i \varphi_i \cup \bigcup_j \psi_j = \delta\gamma$ for some substitutions δ, γ, such that δ of domain $\bigcup_{i\in I} \mathcal{D}om(\sigma_i) \cup \bigcup_{j\in J} \mathcal{D}om(\tau_j)$ is the most general unifier of the unification problem. Note that we use the fact that the substitutions from the set $\{\varphi_i, \psi_j\}_{i\in I, j\in J}$ have pairwise disjoint domains, and that $u = L\delta\gamma$.

Let $u' = L\delta$, hence $u = u'\gamma$. By Lemma 3.17, $v' \underset{i}{\overset{O}{\Longleftarrow\!\!\otimes}} u' \underset{j}{\overset{O'}{\otimes\!\!\Longrightarrow}} w'$. Instantiating u' by γ yields $v'\gamma \underset{i}{\overset{O}{\Longleftarrow\!\!\otimes}} u'\gamma \underset{j}{\overset{O'}{\otimes\!\!\Longrightarrow}} w'\gamma$ by Lemma 3.11. By Lemma 3.15, $v'\gamma = v$ and $w'\gamma = w$. □

3.7 Nested critical pairs of the theory of global states

We illustrate here the computation of nested critical peaks with our example of global states. First, we recall the rules:

$$\begin{array}{rrcl}
(ll) & lk(\lambda w.lk(\lambda v.X[v,w])) & \to & lk(\lambda v.X[v,v]) \\
(uu) & ud(V, ud(W,X)) & \to & ud[W,X] \\
(ul) & ud(V, lk(\lambda v.X[v])) & \to & ud(V, X[V]) \\
(lu) & lk(\lambda v.ud(v, X[v])) & \to & lk(\lambda v.X[v]) \\
(l) & lk(\lambda v.X) & \to & X
\end{array}$$

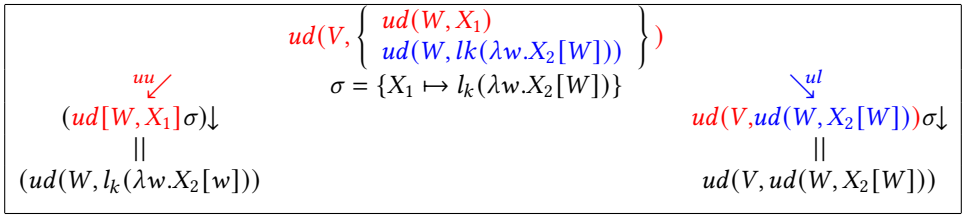
We now show the computation of an overlap via the calculation of pre-seeds and seeds: These two rules, like their well-chosen names, overlap *ad libitum* because the head function symbol of each lefthand side is heading a strict subterm of the other which will be part of the substitution when unifying the rules. We consider the case ul above lu, and index their free variables V and X by the number of runs in the computation of pre-seeds. The initial seed in $p\mathcal{S}^{ul}_{lu}$ is $(x, \sigma = \{x \mapsto ud(V_0, l_k(\lambda v.X_0[v]))\}, \{\wedge\}, \{\,\})$.

The only possible overlap with lu requires $Q_1 = \{2\}$, which is above the fringe of ul's lefthand side. Unification yields $\tau_1 = \{X_0 \mapsto \lambda z.ud(z, X_1[z])\}$, hence $(ud(V_0, l_k(\lambda v.X_1[v])), \tau_1, \{\wedge\}, \{2\})$ is added to $p\mathcal{S}^{ul}_{lu}$. Because position 2·1·1 in the overlap $ud(V_0, l_k(\lambda v.ud(v, X_1[v])))$ is at the fringe of ul's lefthand side, we take $P_2 = \{2\cdot 1\cdot 1\}$ and unify the corresponding subterm with the renamed lefthand side of ul, yielding $\tau_2 = \{x_1 \mapsto \lambda z.lk(\lambda v.X_2[v])$. The seed $(ud(V_0, l_k(\lambda v.X_1[v])), \tau_2, \{2\cdot 1\cdot 1\}, \{2\})$ is added to $p\mathcal{S}^{ul}_{lu}$. We continue with $Q_3 = \{2\cdot 1\cdot 1\cdot 2\}$, and so on. We get four infinite families whose seeds are $(ud(V_0, lk(\lambda v.ud(v, lk(\ldots, lk(\lambda v.X_{2n}[v])\ldots)))), \{2\cdot 1\cdot 1)^{2p}\cdot 2 : 2p \le n\}, \{2\cdot(1\cdot 1\cdot 2)^{2p+1} : 2p \le n\})$, and $(ud(V_0, lk(\lambda v.ud(v, lk(\ldots, lk(\lambda v.ud(v, X_{2n+1}[v])^2\ldots)^4, \{2\cdot 1\cdot 1)^{2p+1}\cdot 2 : 2p+1 \le n\}, \{2\cdot(1\cdot 1\cdot 2)^{2p} : 2p \le n\})$.

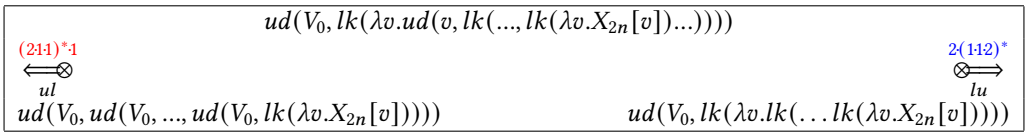
We now display the nested peaks before to explain their computation:

$$\begin{array}{ccc}
 & lk(\lambda w.\left\{\begin{array}{l} l_k(\lambda v.X_1[v,w]) \\ l_k(\lambda v.ud(v, X_2[v])) \end{array}\right\}) & \\
 & \sigma = \{X_1 \mapsto \lambda z_1 z_2.ud(z_1, X_2[z_1])\} & \\
\overset{ll}{\swarrow} & & \overset{lu}{\searrow} \\
(lk(\lambda v.X_1[v,v])\sigma)\downarrow & & (lk(\lambda w.l_k(\lambda v.X_2[v]))\sigma)\downarrow \\
\| & & \| \\
lk(\lambda v.ud(v, X_2[v])) & & lk(\lambda w.l_k(\lambda v.X_2[v]))
\end{array}$$

Gilles Dowek, INRIA-Saclay, France
Gaspard Ferey, LSV, ENS de Paris-Saclay, France
Jean-Pierre Jouannaud, LSV, ENS de Paris-Saclay, France
Jiaxiang Liu, Shenzhen University, China



For rule l, the fact that X does not depend on v in the lefthand side of l makes unification fail with lu. For all other three possibilities, one with ul and two with ll, the obtained critical pair is trivial, that is, the two rewrites yield identical result. The calculation details are left to the reader. The last two possible overlaps, of ul above with lu or vice versa, yield four infinite families of seeds, hence of critical overlaps. We consider the "even case" of the family of seeds described in Example 3.20:



In this last computation, a subterm like $lk(\lambda v.lk(...lk(\lambda v.X_{2n}[v])))$ matches $lk(\lambda v.X)$, where X does not depend on v, because $X_{2n}[v]$ is not in scope of the outside λv. We could have renamed all the bound v's by different variables to make it more apparent.

Checking the "odd case" results in no new ordering constraint. Checking then the other two infinite families obtained by overlapping uu at a subterm of ul is entirely left to the reader.

4 CONFLUENCE IN $\lambda\mathcal{F}$

Our goal here is to state and prove our main result, namely, the Church-Rosser property for a rewrite theory in $\lambda\mathcal{F}$, under the assumption that its nested critical pairs have decreasing diagrams.

Since beta-reductions do not terminate on untyped terms, we shall use van Oostrom's technique relying on the existence of a decreasing diagram for each local peak [20]. Since functional rewrites operate modulo variable renaming, we shall also use Jouannaud and Liu's extension of van Oostrom's decreasing diagram completeness property [12].

Labelled rewriting is a basic notion underlying decreasing diagrams. A labelled binary relation on an abstract set is denoted by $u \xrightarrow{m} v$, where m is an element of a set $\mathcal{L}$ of *labels* equipped with a partial quasi-order $\trianglerighteq$ which strict part $\triangleright$ is well-founded. We write $m = n$ (resp., $m\#n$) for equivalent (resp., incomparable) labels m, n, and $\alpha \triangleright l$ (resp., $l \triangleright \alpha$) if $m \triangleright l$ (resp., $l \triangleright m$) for all m in the multiset (or sequence) α of labels.

Rewrite arrows may therefore come along with two different upper indices, a position p and a label l, they will be written in this order separated by a comma. The lower index remains reserved for the rule name. The position or label may be omitted if no ambiguity arises.

The structure of this section is as follows: firstly, we recall the notion of decreasing diagram and its relationship to confluence; secondly, we describe the labelling schema used for $\lambda\mathcal{F}$; thirdly, we state the confluence theorem; fourthly, we apply the result to the theory of global states; lastly, comes the proof of the result.

4.1 Decreasing diagrams [22].

Definition 4.1 (Local diagram). Given a labelled relation $\longrightarrow$ on an abstract set, a *local diagram* D is a pair made of a *local peak* $D_{peak} = v \longleftarrow u \longrightarrow w$ and a *joining conversion* $D_{conv} = v \twoheadleftarrow\!\!\!\!\twoheadrightarrow w$.

Definition 4.2 (Decreasing local diagram). A local diagram with peak $v \xleftarrow{m} u \xrightarrow{n} w$ is *decreasing* if its joining conversion has the form $v \overset{\alpha}{\twoheadleftarrow\!\!\twoheadrightarrow} s \xrightarrow{n} s' \overset{\gamma}{\twoheadleftarrow\!\!\twoheadrightarrow} t' \xleftarrow{m} t \overset{\beta}{\twoheadleftarrow\!\!\twoheadrightarrow} w$, with labels in α (resp. β, γ) strictly smaller than m (resp. n, and m or n). $s \xrightarrow{n} s'$ and $t' \xleftarrow{m} t$ (resp., $v \overset{\alpha}{\twoheadleftarrow\!\!\twoheadrightarrow} s$, $t \overset{\beta}{\twoheadleftarrow\!\!\twoheadrightarrow} w$, $s' \overset{\gamma}{\twoheadleftarrow\!\!\twoheadrightarrow} t'$) are called the *facing* (resp. *side*, *side*, *middle*) steps of the conversion.

Decreasing diagrams are abbreviated as DDs. Note that the side and middle steps of a DD are conversions. In practice, at least the middle steps are usually directed as in a joinability diagram, but this is not necessarily so, as shown with a simple proof in [12]. Note also that a facing step of a decreasing diagram may be missing, its side steps are then absorbed by the middle ones. This is the case if $m \rhd n$ (or $n \rhd m$).

Theorem 4.3 ([22]). *A labelled relation is Church-Rosser if all its local peaks have decreasing diagrams. Conversely, any confluent relation on a countable set can be labelled so that all its local peaks have decreasing diagrams.*

Van Oostrom's theorem generalizes to rewrite relations modulo an equational theory, here $=_\alpha$. Its converse requires that rewriting commutes over the equational theory and that the set of labels is increased by a new minimum label reserved for the equational steps [12]. This generalization of van Oostrom's theorem is needed here for the functional rewriting relation $\longrightarrow_{\beta_\alpha}$.

4.2 Labelled rewrites in $\lambda\mathcal{F}$

We now consider the Church-Rosser property of the rewrite relation used in $\lambda\mathcal{F}$ on untyped terms. As usual, it is essential to choose carefully the relation to work with. For the method to be sound, it must contain rewriting and define the same convertibility relation as the one generated by the set of rules. In case of non-terminating rewrites, non-linearities make it difficult to get decreasing diagrams for ancestor peaks since there can only be one facing step on each side of the conversion. The usual way out is to impose left-linearity and use some form of parallel rewriting to handle non-right-linearities. Higher-order rewrite steps will require a label bigger than the functional steps, so that the latter can be neglected when needed. But parallel higher-order rewrites taking place below a beta-step may now become both duplicated and nested, making orthogonal higher-order rewriting necessary here to get decreasing diagrams. Functional steps having a label strictly smaller than higher-order steps won't need parallel rewriting. The steps to be considered in an arbitrary conversion, from which all local peaks must be replaced by decreasing diagrams, are therefore of the three following forms: $=_\alpha$, $\longrightarrow_{\beta_\alpha}$ and $\underset{\mathcal{R}}{\otimes\!\!\Longrightarrow}$. However, we sometimes allow ourselves to abbreviate a sequence $\xrightarrow[0]{p_1} \dots \xrightarrow[0]{p_n}$ by $\overset{P}{\underset{0}{\Longrightarrow}}$ when $P = \{p_i\}_i$ is a set of parallel positions.

For uniformity, we assign to β_α-steps the name 0, so that all rewrite steps are denoted by a natural number and let $\underset{i\geq 0}{\longrightarrow} = \underset{\beta_\alpha}{\longrightarrow} \cup \underset{\mathcal{R}}{\otimes\!\!\Longrightarrow}$. We further assign to $=_\alpha$-steps the name -1, which completes the set of natural numbers by the new smallest element -1, and use the writing $u \xrightarrow[-1]{p} v$ for an $=_\alpha$-step taking place in the subterm $u|_p$. Hence, $\underset{i\geq -1}{\longrightarrow} = \underset{-1}{\longrightarrow} \cup \underset{\beta_\alpha}{\longrightarrow} \cup \underset{\mathcal{R}}{\otimes\!\!\Longrightarrow}$.

We now label a rewrite step $\underset{i}{\longrightarrow}$ (or equational step $=_\alpha$) by a pair $\langle i, l\rangle$ whose second element l depends on the category of rewrite step, functional ($i = 0$) or higher-order ($i > 0$)). Equational steps ($i = -1$) don't need a second element, their label is the minimum of all labels as required the generalization of van Oostrom's theorem to rewriting modulo. Since the rule name appears already in lower position, we don't need to display the label in upper position unless the second

Gilles Dowek, INRIA-Saclay, France
Gaspard Ferey, LSV, ENS de Paris-Saclay, France
Jean-Pierre Jouannaud, LSV, ENS de Paris-Saclay, France
Jiaxiang Liu, Shenzhen University, China

element l of the pair is needed. Labels are compared lexicographically, using the natural order on the augmented set of natural numbers for their first element.

4.3 The confluence theorem

We have seen that decreasing diagrams can have a very general form. We shall however use a more convenient form for the nested critical pairs themselves:

Definition 4.4 (DRDs). Given a pair of rule indices (i, j), a *decreasing reduction (DR)* from u to v is a reduction of the form $u \underset{I}{\longrightarrow\!\!\!\!\!\rightarrow} s \underset{j}{\overset{P}{\otimes\!\!\!\!\!\Longrightarrow}} t \underset{K}{\longrightarrow\!\!\!\!\!\rightarrow} v$, where rule indices in I are strictly smaller than i and those in K are strictly smaller than either i or j. We also write $u \underset{<i}{\longrightarrow\!\!\!\!\!\rightarrow} \underset{j}{\overset{P}{\otimes\!\!\!\!\!\Longrightarrow}} \underset{<i,j}{\longrightarrow\!\!\!\!\!\rightarrow} v$.

Given a local peak $v \underset{i}{\overset{P}{\Longleftarrow\!\!\!\!\!\otimes}} u \underset{j}{\overset{Q}{\otimes\!\!\!\!\!\Longrightarrow}} w$, a *decreasing rewrite diagram (DRD)* is a pair of decreasing reductions from v to v' wrt (i, j) and from w to w' wrt (j, i), such that $v' =_\alpha w'$.

Our formulation of decreasing reductions includes α-steps in both sequences I and K. We could therefore identify v' and w' in the definition of a DRD, and will do it when convenient. Note also that a decreasing reduction reduces to a reduction of the form $u \underset{K}{\longrightarrow\!\!\!\!\!\rightarrow} v$ in case P is the empty set of orthogonal positions.

There is a single orthogonal step in a decreasing reduction. The reason is that any orthogonal step using a rule of index $k < j$ can be expanded into a derivation of the same kind by Lemma 3.12. On the other hand, it is not possible to expand the orthogonal j-step without violating the decreasing diagram condition: there may be at most one step labelled by the index j. Collecting many j-steps into a single orthogonal j-step is the very reason for introducing orthogonal rewriting.

DRDs have better properties than arbitrary decreasing diagrams which ease the confluence proof in many (but non-essential) ways. In practice, searching for DRDs is easier than searching for arbitrary decreasing diagrams, this is another reason for considering them.

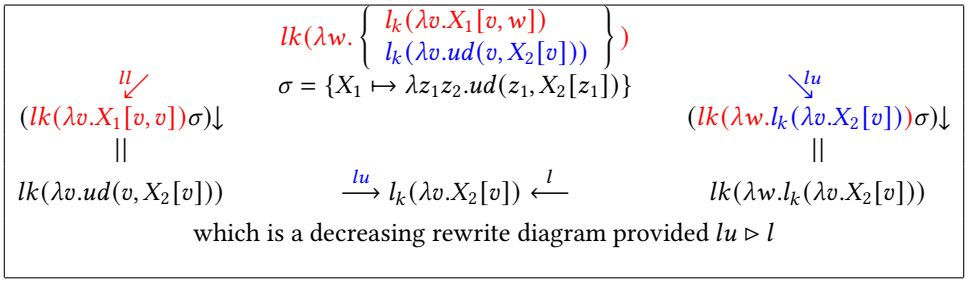
We can now state the first main result of the paper, whose proof spanns over Section 4.5:

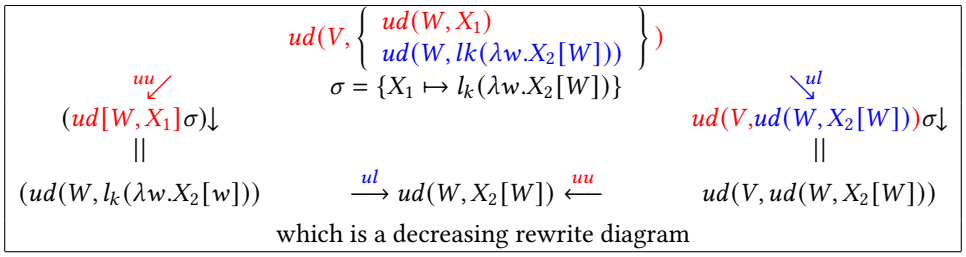
Theorem 4.5. *A rewrite theory $(\mathcal{F}, \mathcal{R})$ is confluent if the nested critical pairs of $\mathcal{R}$ have decreasing rewrite diagrams.*

4.4 Confluence of the theory of global states

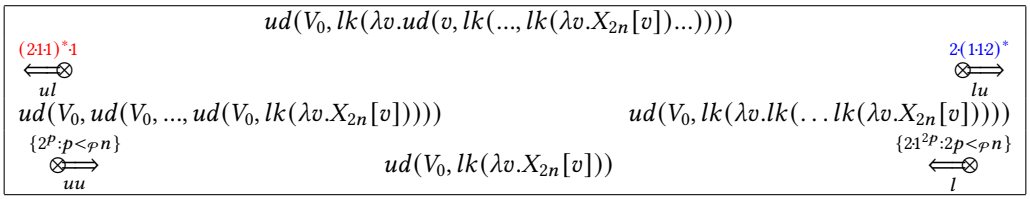
We illustrate here the confluence theorem with our example of global states, and show that all its nested critical pairs have decreasing diagrams. After recalling the rules, come the critical pairs computations presented inside individual boxes. In the upper middle of each box appear two rules whose superposition is inside braces. The upper rule is displayed in red, the lower one in blue. Next comes the unifier, then the coloured righthand sides, then the reduced righthand sides, and finally the decreasing diagram part itself. Coloured rule names label the arrows.

$$\begin{array}{rrcl}
(ll) & lk(\lambda w.lk(\lambda v.X[v,w])) & \to & lk(\lambda v.X[v,v]) \\
(uu) & ud(V,ud(W,X)) & \to & ud[W,X] \\
(ul) & ud(V,lk(\lambda v.X[v])) & \to & ud(V,X[V]) \\
(lu) & lk(\lambda v.ud(v,X[v])) & \to & lk(\lambda v.X[v]) \\
(l) & lk(\lambda v.X) & \to & X
\end{array}$$





For rule l, the fact that X does not depend on v in the lefthand side of l makes unification fail with lu. For all other three possibilities, one with ul and two with ll, the obtained critical pair is trivial, that is, the two rewrites yield identical result. The calculation details are left to the reader. The last two possible overlaps, of ul above with lu or vice versa, yield four infinite families of seeds, hence of critical overlaps. We consider the "even case" of the family of seeds described in Example 3.20:



In this last rewrite diagram, which is decreasing provided $\{ul, lu\} \rhd \{l, uu\}$, hence $\{ul, lu\} \rhd uu$ since we already need $lu \rhd l$, a subterm like $lk(\lambda v.lk(...lk(\lambda v.X_{2n}[v])))$ matches $lk(\lambda v.X)$, where X does not depend on v, because $X_{2n}[v]$ is not in scope of the outside λv. We could have renamed all the bound v's by different variables to make it more apparent.

Checking the "odd case" results in no new ordering constraint. Checking then the other two infinite families obtained by overlapping uu at a subterm of ul is entirely left to the reader.

4.5 The Confluence Proof

Using Theorem 4.3, we need to show the existence of decreasing diagrams for all local peaks in turn. Functional peaks come first. Their analysis makes an original use of the completeness property. Heterogeneous peaks between $\underset{0}{\longrightarrow}$ (that is, $\underset{\beta_\alpha}{\longrightarrow}$) and $\underset{i>0}{\otimes\!\!\Longrightarrow}$ come second. The case of higher-order local peaks is of course most difficult, their analysis comes last. Before starting these three analyses, we need to develop some commutation properties which are usual algebraic properties of reductions, although their proof here may sometimes use non-standard arguments.

4.5.1 Decreasing diagrams for free. Before to start building decreasing diagrams for all local peaks, we need to generalize some standard commutation properties of plain rewriting to the case of higher-order orthogonal reductions. These algebraic properties of reductions can be seen as *decreasing diagrams for free*. They will of course play an important role in the confluence proof.

Gilles Dowek, INRIA-Saclay, France
Gaspard Ferey, LSV, ENS de Paris-Saclay, France
Jean-Pierre Jouannaud, LSV, ENS de Paris-Saclay, France
Jiaxiang Liu, Shenzhen University, China

Plain first-order rewriting enjoys two properties implying that disjoint and ancestor local rewriting peaks are always joinable, called disjoint peak property (DP) and linear ancestor peak property (LAP) for left-linear rewrite rules [10]. (DP) is true of all monotonic relations, and a slightly modified form of (LAP) holds for higher-order rewriting as we have seen. It is important to realize that our definition of higher-order rewriting has been designed with this objective in mind: neither (DP) nor (LAP) are true of Nipkow's definition. As expected, these properties extend to orthogonal higher-order rewrites:

Lemma 4.6 (DP). *Let $Q\#P$. Then, rewriting steps at P and Q commute.*

Note that P (resp., Q) are singleton sets when rewriting takes place at a single position.

The reason why (DP) holds is that all rewriting relations considered here are *local*, that is, operate *below* the rewriting position(s). Nipkow's rewriting relation is non-local, because it also modifies terms above the rewriting position.

We now move to ancestor peak properties, which are given in turn. The first is straightforward:

Lemma 4.7 (LAPα). *Let $j \in \mathcal{R}$. Then, $\underset{-1}{\overset{p}{\longleftarrow}} \underset{j}{\overset{Q}{\otimes\!\!\Longrightarrow}} \subseteq \underset{j}{\overset{Q}{\otimes\!\!\Longrightarrow}} \underset{-1}{\overset{}{\longleftarrow\!\!\!\!\!\!\cdot}}$, where $\neg\, p\#Q$.*

The case where a functional reduction takes place *above* the higher-order one justifies the need for orthogonal higher-order reductions:

Lemma 4.8 (LAPβA$\mathcal{R}$). *Let $j \in \mathcal{R}$ and $Q >_{\mathcal{P}} p$. Then, $\underset{0}{\overset{p}{\longleftarrow}} \underset{j}{\overset{Q}{\otimes\!\!\Longrightarrow}} \subseteq \underset{j}{\overset{Q'}{\otimes\!\!\Longrightarrow}} \underset{0}{\overset{p}{\longleftarrow}}$ for some $Q' >_{\mathcal{P}} p$.*

Proof. Since functional reductions are monotonic, we may assume that $p = \Lambda$.

Let $s = (\lambda x\!:\!u.v\ w)$, hence $Q = 1\cdot 1\cdot Q_1 \cup 1\cdot 2\cdot Q_2 \cup 2\cdot Q_3$, $t = v\{x \mapsto w\}$, $u \underset{j}{\overset{Q_1}{\otimes\!\!\Longrightarrow}} u'$, $v \underset{j}{\overset{Q_1}{\otimes\!\!\Longrightarrow}} v'$, $w \underset{j}{\overset{Q_1}{\otimes\!\!\Longrightarrow}} w'$ and $t' = (\lambda x\!:\!u'.v'\ w')$. Let $s' = v'\{x \mapsto w'\}$. Then $t \underset{j}{\overset{Q_2 \otimes_v Q_3}{\otimes\!\!\Longrightarrow}} s' \underset{0}{\overset{\Lambda}{\longleftarrow}} t'$. □

The case where the functional step is *below* extends Lemma 2.19 to orthogonal reductions:

Lemma 4.9 (LAPβB$\mathcal{R}$). *Let $j \in \mathcal{R}$ and $p \geq_{\mathcal{P}} Q$. Then, $\underset{0}{\overset{p}{\longleftarrow}} \underset{j}{\overset{Q}{\otimes\!\!\Longrightarrow}} \subseteq \underset{j}{\overset{Q}{\otimes\!\!\Longrightarrow}} \underset{0}{\overset{P}{\Longleftarrow}}$ for some P.*

Proof. Let $v \underset{0}{\overset{p}{\longleftarrow}} u \underset{j}{\overset{Q}{\otimes\!\!\Longrightarrow}} w$. Since $p \geq_{\mathcal{P}} Q$, there exists $q \in Q_{max}$ such that $p \geq_{\mathcal{P}} q$. By splitting u at p, we get $u = s\sigma$ where $s = \underline{u}_p$ and $\sigma = \overline{u}^p = \{X \mapsto \lambda\overline{x}.u|_p\}$ and $u|_p \underset{\beta}{\overset{\Lambda}{\longrightarrow}} v|_p$, hence $v = s\tau$ and $\sigma \underset{\beta}{\longrightarrow} \tau$ where $\tau = \lambda\overline{x}.v|_p$. Since patterns are β-normal, $p \geq_{\mathcal{P}} q \cdot F_L$, hence Q is a set of orthogonal positions in s by Lemma 2.17. Let t such that $s \underset{i}{\overset{Q}{\otimes\!\!\Longrightarrow}} t$. Then $u \underset{j}{\overset{Q \otimes_s \varnothing}{\otimes\!\!\Longrightarrow}} t\sigma = w$ by Lemma 3.15.

The result now follows by rewriting both $s\tau$ and $t\sigma$ to $t\tau$ thanks to monotonicity of functional reductions and Lemma 3.11. □

We can now carry out the general case where the β-step is in the middle of an orthogonal step:

Lemma 4.10 (LAP$\beta\mathcal{R}$). *Let $j \in \mathcal{R}$, p a position, and P a set of orthogonal positions such that $\neg(p\#P)$. Then, $\underset{0}{\overset{p}{\longleftarrow}} \underset{i}{\overset{P}{\otimes\!\!\Longrightarrow}} \subseteq \underset{i}{\overset{Q}{\otimes\!\!\Longrightarrow}} \underset{0}{\overset{}{\longleftarrow\!\!\!\!\!\!\cdot}}$ for some Q.*

Proof. Let $v \underset{0}{\overset{p}{\longleftarrow}} u \underset{i}{\overset{P}{\otimes\!\!\Longrightarrow}} w$. Since patterns are β-normal, $p \notin P$. Let $K = mip\{k \in P : k >_{\mathcal{P}} p\}$, $P = O \otimes_K Q$, $u' = \overline{u}^K$, $\sigma = \underline{u}_K$ and $u = u'\sigma$. Note that $p \in \mathcal{P}os(u')$, hence $u' \underset{\beta}{\overset{p}{\longrightarrow}} v'$. By Lemma 3.6, O, Q

are (possibly empty) sets of orthogonal positions for u' and σ respectively, hence $u' \overset{O}{\underset{i}{\otimes\!\Longrightarrow}} w'$ and $\sigma \overset{Q}{\underset{i}{\otimes\!\Longrightarrow}} \tau$. Since $\neg(p\#P)$, p stands below positions in O and above those in Q unless they are empty.

By Lemma 2.15, $v = v'\sigma$. By Lemma 4.9, $v' \overset{O}{\underset{i}{\otimes\!\Longrightarrow}} s' \overset{P'}{\underset{0}{\Longleftarrow}} w'$ for some set P' of parallel positions and term s'. Therefore $v'\sigma \overset{O}{\underset{i}{\otimes\!\Longrightarrow}} s'\sigma \overset{P'}{\underset{0}{\Longleftarrow}} w'\sigma$ by monotonicity of higher-order reductions and Lemma 3.10.

By Lemma 3.15, $u = u'\sigma \overset{O\otimes_K Q}{\underset{i}{\otimes\!\Longrightarrow}} w'\tau = w$. We have therefore got the peak $s'\sigma \overset{P'}{\underset{0}{\Longleftarrow}} w'\sigma \overset{\varnothing\otimes_{w'} Q}{\underset{i}{\otimes\!\Longrightarrow}} w'\tau$. By applying Lemma 4.8 as many times as $|P'|$, we get $v'\sigma \overset{Q'}{\underset{i}{\otimes\!\Longrightarrow}} t\tau \overset{P'}{\underset{0}{\Longleftarrow}} w'\tau = w$ for some term t.

Finally, $v = v'\sigma \overset{O\otimes_{v'} Q'}{\underset{i}{\otimes\!\Longrightarrow}} t\tau$ by definition of orthogonal rewriting, and we are done. □

Lemma 4.11 (LAP$\mathcal{R}$). *Let $i : L \to R$, $j : G \to D \in \mathcal{R}$, u a term such that $u \overset{p}{\underset{i}{\longrightarrow}} v$ and σ a substitution such that $\sigma \overset{Q}{\underset{j}{\otimes\!\Longrightarrow}} \tau$. Then, $v\sigma \overset{p}{\underset{i}{\longleftarrow}} u\sigma \overset{\varnothing\otimes_u Q}{\underset{j}{\otimes\!\Longrightarrow}} u\tau$ and $v\sigma \overset{\varnothing\otimes_v Q}{\underset{j}{\otimes\!\Longrightarrow}} v\tau \overset{p}{\underset{i}{\longleftarrow}} u\tau$.*

Proof. By Lemma 2.15 and definition of orthogonal rewriting. □

We are now in the situation to carry out the search of decreasing diagrams for arbitrary local peaks.

4.5.2 *Decreasing diagrams for functional local peaks.*

Lemma 4.12. *Functional local peaks have decreasing rewrite diagrams.*

Proof. Functional rewrites are Church-Rosser, hence, by Theorem 4.3, a β_α-step can be labelled by some l belonging to a well-founded set so that its local peaks have decreasing diagrams. Functional steps can thus be labelled by the pair $\langle 0, l\rangle$, hence preserving the existence of decreasing diagrams. □

4.5.3 *Decreasing diagrams for heterogeneous functional/higher-order local peaks.*

Lemma 4.13. *Heterogeneous functional/higher-order local peaks have decreasing diagrams.*

Proof. Since patterns are β-normal, the result follows either from Lemma 4.6 or from Lemma 4.10. □

4.5.4 *Decreasing diagrams for higher-order local peaks.* We consider arbitrary local peaks:

Lemma 4.14. *Higher-order local peaks have decreasing diagrams provided higher-order nested critical peaks have decreasing rewrite diagrams.*

This is the difficult case of local peaks, whose proof is based on using Theorem 4.5. It also requires lifting decreasing reductions from critical peaks to overlapping peaks, as well as gluing together decreasing derivations obtained for a term and its substitution, two properties that we show first:

Lemma 4.15 (Stability). *Let $s \underset{<i}{\longrightarrow\!\!\!\!\!\rightarrow} \overset{P}{\underset{i}{\otimes\!\Longrightarrow}} \underset{<i,j}{\longrightarrow\!\!\!\!\!\rightarrow} t$ and σ arbitrary. Then $s\sigma \underset{<i}{\longrightarrow\!\!\!\!\!\rightarrow} \overset{}{\underset{i}{\otimes\!\Longrightarrow}} u\sigma \underset{<i,j}{\longrightarrow\!\!\!\!\!\rightarrow} t\sigma$.*

Proof. This is a direct consequence of stability of functional reductions, higher-order reductions (Lemma 2.15) and orthogonal reductions (Lemma 3.11). □

Gilles Dowek, INRIA-Saclay, France
Gaspard Ferey, LSV, ENS de Paris-Saclay, France
Jean-Pierre Jouannaud, LSV, ENS de Paris-Saclay, France
Jiaxiang Liu, Shenzhen University, China

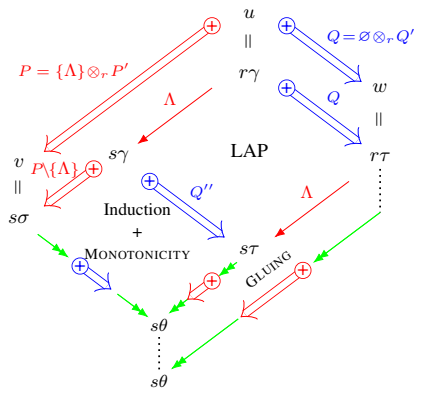


Fig. 3. Non-overlapping case.

Lemma 4.16 (Monotonicity). *Let* $\sigma \underset{<i}{\longrightarrow\!\!\!\!\!\!\rightarrow} \otimes\!\!\!\!\!\!\Longrightarrow^{P}_{i} \underset{<i,j}{\longrightarrow\!\!\!\!\!\!\rightarrow} \tau$ *and* u *arbitrary. Then* $u\sigma \underset{<i}{\longrightarrow\!\!\!\!\!\!\rightarrow} \otimes\!\!\!\!\!\!\Longrightarrow_{i} \underset{<i,j}{\longrightarrow\!\!\!\!\!\!\rightarrow} u\tau$.

Proof. This is a direct consequence of monotonicity of functional reductions, higher-order reductions (Lemma 2.14) and orthogonal reductions (Lemma 3.10). □

We now move to the general case where two decreasing reductions need be glued:

Lemma 4.17 (Gluing). *Let* $u \underset{<j}{\longrightarrow\!\!\!\!\!\!\rightarrow} u' \otimes\!\!\!\!\!\!\Longrightarrow^{P}_{j} v' \underset{<i,j}{\longrightarrow\!\!\!\!\!\!\rightarrow} v$ *and* $\sigma \underset{<j}{\longrightarrow\!\!\!\!\!\!\rightarrow} \sigma' \otimes\!\!\!\!\!\!\Longrightarrow^{Q}_{j} \tau' \underset{<i,j}{\longrightarrow\!\!\!\!\!\!\rightarrow} \tau$ *be two decreasing derivations originating from a term* u *and a substitution* σ*, respectively.*

Then, $u\sigma \underset{<j}{\longrightarrow\!\!\!\!\!\!\rightarrow} u'\sigma' \otimes\!\!\!\!\!\!\Longrightarrow^{P\otimes_{u'}Q}_{j} v'\tau' \underset{<i,j}{\longrightarrow\!\!\!\!\!\!\rightarrow} v\tau$ *is a decreasing derivation from* $u\sigma$ *to* $v\tau$.

Proof. Follows from stability properties of reductions as above, from their monotonicity properties, and from the definition of orthogonal reductions. □

We can now carry out the proof of Lemma 4.14:

Proof. Let $v \otimes\!\!\!\!\!\!\Longleftarrow^{P}_{i} u \otimes\!\!\!\!\!\!\Longrightarrow^{Q}_{j} w$ be an orthogonal higher-order local peak. The proof proceeds by induction on the size of u.

Assume first that $\Lambda \notin P \cup Q$. Then, we can cut u along $K = (P \cup Q)_{min}$, apply induction to $\overline{u}^K$ yielding some decreasing diagram, and compose back that diagram with $\underline{u}_K$ by Lemma 4.16, yielding the result.

Assume now that $\Lambda \in P \cup Q$ and wlog $\Lambda \in P$. Let $O \cup O'$ be the maximal subset of $P \cup Q$ s.t. (i, O, j, O') defines a nested critical overlap at the root. There are two cases depending upon the size of $O \cup O'$: the first, non-overlapping case, shown at Figure 3, and the second, overlapping case, shown at Figure 4.

JP: Jiaxiang: the figures need some changes. I assume you have the originals somewhere. Jiaxiang: Done.

(1) $|O \cup O'| = 0$. We then split u along $K = (P \setminus \{\Lambda\} \cup Q)_{min}$. Let therefore $r = \underline{u}_K$, $\gamma = \overline{u}^K$, and $r\gamma = u$. By Lemma 2.4, $P = \Lambda \otimes_K P'$ and $Q = \varnothing \otimes_K Q'$. By Lemma 3.15 applied twice, $v = s\sigma \otimes\!\!\!\!\!\!\Longleftarrow^{\{\Lambda\}\otimes_r P'}_{i} u \otimes\!\!\!\!\!\!\Longrightarrow^{\varnothing\otimes_r Q'}_{j} r\tau = w$.

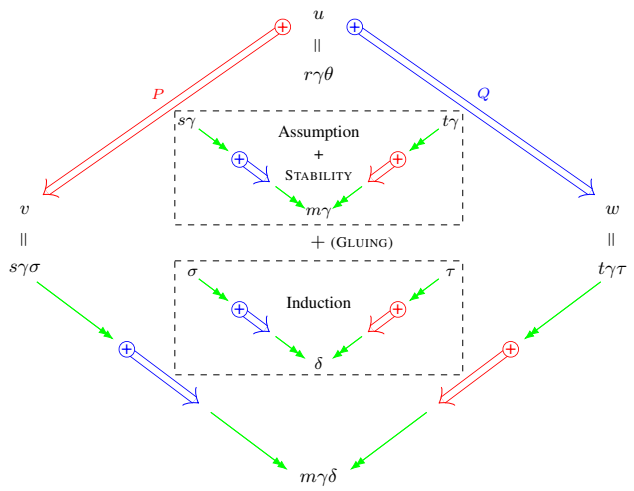


Fig. 4. Overlapping case.

We now decompose the step from u to v: by Definition 3.2, $r \underset{i}{\overset{\Lambda}{\longrightarrow}} s$ and $\gamma \underset{i}{\overset{P'}{\otimes\!\!\Longrightarrow}} \sigma$. By Lemma 3.11, $u = r\gamma \underset{i}{\overset{\Lambda}{\longrightarrow}} s\gamma \underset{i}{\overset{P\setminus\{\Lambda\}}{\otimes\!\!\Longrightarrow}} s\sigma = v$. Likewise, $u \underset{j}{\overset{\varnothing\otimes_K Q'}{\otimes\!\!\Longrightarrow}} r\tau$. By (LAP), $s\gamma \underset{j}{\overset{Q''}{\otimes\!\!\Longrightarrow}} s\tau \underset{i}{\overset{\Lambda}{\longleftarrow}} (r\tau)$. We are done if $P' = \varnothing$, otherwise we get smaller peaks $\sigma \underset{i}{\overset{P'}{\Longleftarrow\!\!\otimes}} \gamma \underset{j}{\overset{Q'}{\otimes\!\!\Longrightarrow}} \tau$. By induction hypothesis, $\sigma \underset{<i}{\longrightarrow\!\!\!\!\!\rightarrow} \otimes\!\!\Longrightarrow \underset{<i,j}{\longrightarrow\!\!\!\!\!\rightarrow} \theta$ and $\tau \underset{<j}{\longrightarrow\!\!\!\!\!\rightarrow} \otimes\!\!\Longrightarrow \underset{<i,j}{\longrightarrow\!\!\!\!\!\rightarrow} \theta$ for some θ. By Lemma 4.16, we get a decreasing derivation from $s\sigma$ to $s\theta$. By Lemma 4.17, we get a decreasing derivation from $r\tau$ to $s\theta$. We therefore have got a DRD for the peak $v = s\sigma \underset{i}{\Longleftarrow\!\!\otimes} u \underset{j}{\otimes\!\!\Longrightarrow} r\tau = w$.

(2) $|O \cup O'| \neq 0$, hence $\Lambda \in O$. We then split u according to Theorem 3.21, hence there exist $u', v', w', r, s, t, \theta, \gamma, \sigma, \tau, O, O', P', Q'$ such that (i) $u = u'\theta, v = v'\sigma, w = w'\tau$, $u' = r\gamma, v' = s\gamma, w' = t\gamma$; (ii) $s \underset{i}{\overset{O}{\Longleftarrow\!\!\otimes}} r \underset{j}{\overset{O'}{\otimes\!\!\Longrightarrow}} t$ is a nested critical peak; (iii) $\sigma \underset{i}{\overset{P'}{\Longleftarrow\!\!\otimes}} \theta \underset{j}{\overset{Q'}{\otimes\!\!\Longrightarrow}} \tau$; (iv) $P = O \otimes_{u'} P'$, $Q = O' \otimes_{u'} Q'$.
By assumption, there is a DRD for the nested critical pair $\langle s, t\rangle$, hence there exists some term m such that $s \underset{<i}{\longrightarrow\!\!\!\!\!\rightarrow} \otimes\!\!\Longrightarrow \underset{<i,j}{\longrightarrow\!\!\!\!\!\rightarrow} m$ and $t \underset{<j}{\longrightarrow\!\!\!\!\!\rightarrow} \otimes\!\!\Longrightarrow \underset{<i,j}{\longrightarrow\!\!\!\!\!\rightarrow} m$. It follows by Lemma 4.15 that $s\gamma \underset{<i}{\longrightarrow\!\!\!\!\!\rightarrow} \underset{i}{\otimes\!\!\Longrightarrow} \underset{<i,j}{\longrightarrow\!\!\!\!\!\rightarrow} m\gamma$ and $t\gamma \underset{<j}{\longrightarrow\!\!\!\!\!\rightarrow} \underset{j}{\otimes\!\!\Longrightarrow} \underset{<i,j}{\longrightarrow\!\!\!\!\!\rightarrow} m\gamma$.
By induction hypothesis, the peak $\sigma \underset{i}{\overset{P'}{\Longleftarrow\!\!\otimes}} \theta \underset{j}{\overset{Q'}{\otimes\!\!\Longrightarrow}} \tau$ has a DRD, hence $\sigma \underset{<i}{\longrightarrow\!\!\!\!\!\rightarrow} \underset{j}{\otimes\!\!\Longrightarrow} \underset{<i,j}{\longrightarrow\!\!\!\!\!\rightarrow} \delta$ and $\tau \underset{<j}{\longrightarrow\!\!\!\!\!\rightarrow} \underset{i}{\otimes\!\!\Longrightarrow} \underset{<i,j}{\longrightarrow\!\!\!\!\!\rightarrow} \delta$.
We can now glue these DRDs together and obtain a DRD for the original local peak by Lemma 4.17. □

4.5.5 Commuting diagrams for local cliffs. This straightforward property is required in case where a rewrite relation is modulo a theory, here modulo $=_\alpha$.

Lemma 4.18. *Local cliffs have commuting diagrams:* $u =_\alpha v \underset{i\neq 0}{\longrightarrow} w$ *implies that* $u \underset{i}{\longrightarrow} v' =_\alpha w$.

This terminates the proof of our main result.

5 CONCLUSION

Van Oostrom's decreasing diagrams technique characterizes confluence of rewriting on an abstract set. It is well-known that its application to term rewriting is difficult, although many techniques were elaborated during the last years that successfully solved many open problems [2–4, 12, 14, 15, 23]. For example, Felgenhauer proved that the existence of decreasing diagrams for parallel critical pairs ensures the confluence of non-terminating left-linear first-order rewriting systems [4].

Our main result, Theorem 4.5, shows that van Ostrom's method applies to a quite complex new situation, higher-order rewriting of untyped terms with rules having non-trivial higher-order critical pairs. Compared to Felgenhauer's, there are two new difficulties: rewrites are higher-order, and the presence of untyped β-reductions. To our knowledge, this is the first result which allows mixing higher-order rewrite rules having arbitrary critical pairs with untyped β-reductions, a problem known to be difficult. This extends quite substantially the toolkit of theorems that can be used to prove the confluence on untyped terms of λ-calculi augmented by higher-order rewrite rules.

A main technical tool used here is the theory of orthogonal rewriting, which appears as intimately related to van Oostrom's multiset rewriting [19]. A main novel aspect of our definition is the associated notion of a nested critical pair and the corresponding critical pair property which allows to check confluence of non-terminating higher-order definitions whose critical pairs are not development closed, as they are in [21].

Higher-order rewriting definitions have been studied extensively in the past years because they allow encoding program constructs in rather simple type theories allowing for user-defined higher-order rules, as in Agda, dedukti, and SOL. The example we have carried out here, Plotkin-Power's theory of global states, illustrates the use, strength and weaknesses of orthogonal rewriting. Our ambition is to study and implement these techniques in the context of Dedukti, a dependent type theory with user defined higher-order rewrite rules [7]. A more complex example that we have carried out in this setting is [**?**].

One may wonder whether it would be important to develop an abstract theory of orthogonal rewriting. This is indeed questionable. Orthogonal rewriting is needed in presence of β-reduction *and* higher-order rules for three concurrent reasons that do not occur together otherwise: first, β-reduction does not terminate on untyped terms ; second, higher-order rules generate β-redexes, which requires having maximal labels for the higher-order steps ; third, β-rewrites duplicate and stack their subexpressions, which requires using orthogonal higher-order rewriting steps in order to pack together many steps into one in order to meet the decreasing diagram condition for local peaks made of a β-redex sitting above a higher-order redex. The only other cases we can think of where these circumstances would be met, are obtained by relaxing the constraints on the rewrite system added to untyped β-reduction. This is what we shall do in Part II of this work, by allowing for non-left linear rules ranging over *confined first-order expressions*, as well as rewriting confined expressions modulo equations like associativity and commutativity. We do not define confinedness here, but want to point out that we shall be able to reuse without change in this new context the work on orthogonal rewriting carried out here.

REFERENCES

[1] Claus Appel, Vincent van Oostrom, and Jakob Grue Simonsen. Higher-order (non-)modularity. In Christopher Lynch, editor, *Proceedings of the 21st International Conference on Rewriting Techniques and Applications, RTA 2010, July 11-13, 2010, Edinburgh, Scottland, UK*, volume 6 of *LIPIcs*, pages 17–32. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2010.

[2] Bertram Felgenhauer. Rule labeling for confluence of left-linear term rewrite systems. In *IWC*, pages 23–27, 2013.

[3] Bertram Felgenhauer, Aart Middeldorp, Harald Zankl, and Vincent van Oostrom. Layer systems for proving confluence. *ACM Trans. Comput. Log.*, 16(2):14:1–14:32, 2015.
[4] Bertram Felgenhauer and Vincent van Oostrom. Proof orders for decreasing diagrams. In Femke van Raamsdonk, editor, *RTA*, volume 21 of *LIPIcs*, pages 174–189. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2013.
[5] Gaspard Ferey. *Higher-Order Confluence and Universe Embedding in the Logical Framework*. PhD thesis, 2021.
[6] Gaspard Ferey and Jean-Pierre Jouannaud. Confluence in (un)typed higher-order type theories i. draft. hal-, INRIA, march 2019. available from http://dedukti.gforge.inria.fr/.
[7] Gilles Dowek at all. The Dedukti system, 2016. Available from http://dedukti.gforge.inria.fr/.
[8] Healfdene Goguen. The metatheory of UTT. In Peter Dybjer, Bengt Nordström, and Jan M. Smith, editors, *Types for Proofs and Programs, International Workshop TYPES'94, Båstad, Sweden, June 6-10, 1994, Selected Papers*, volume 996 of *Lecture Notes in Computer Science*, pages 60–82. Springer, 1994.
[9] Makoto Hamana. How to prove your calculus is decidable: practical applications of second-order algebraic theories and computation. *PACMPL*, 1(ICFP):22:1–22:28, 2017.
[10] G. Huet. Confluent reductions: abstract properties and applications to term rewriting systems. *Journal of the ACM*, 27(4):797–821, October 1980.
[11] Gérard P. Huet and Jean-Jacques Lévy. Computations in orthogonal rewriting systems, I. In Jean-Louis Lassez and Gordon Plotkin, editors, *Computational Logic - Essays in Honor of Alan Robinson*, pages 395–414. MIT-Press, 1991.
[12] Jean-Pierre Jouannaud and Jiaxiang Liu. From diagrammatic confluence to modularity. *Theor. Comput. Sci.*, 464:20–34, 2012.
[13] Jan Willem Klop. *Combinatory reduction systems*. PhD thesis, CWI tracts, 1980.
[14] Jiaxiang Liu and Jean-Pierre Jouannaud. Confluence: The unifying, expressive power of locality. In Shusaku Iida, José Meseguer, and Kazuhiro Ogata, editors, *Specification, Algebra, and Software - Essays Dedicated to Kokichi Futatsugi*, volume 8373 of *Lecture Notes in Computer Science*, pages 337–358. Springer, 2014.
[15] Jiaxiang Liu, Jean-Pierre Jouannaud, and Mizuhito Ogawa. Confluence of layered rewrite systems. In Stephan Kreutzer, editor, *24th EACSL Annual Conference on Computer Science Logic, CSL 2015, September 7-10, 2015, Berlin, Germany*, volume 41 of *LIPIcs*, pages 423–440. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015.
[16] Richard Mayr and Tobias Nipkow. Higher-order rewrite systems and their confluence. *Theoretical Computer Science*, 192:3–29, 1998.
[17] Dale Miller. A logic programming language with lambda-abstraction, function variables, and simple unification. *Journal of Logic and Computation*, 1(4):497–536, 1991.
[18] Gordon D. Plotkin and John Power. Algebraic operations and generic effects. *Applied Categorical Structures*, 11(1):69–94, 2003.
[19] Terese. Term rewriting systems. In *Cambridge Tracts in Theoretical Computer Science, Marc Bezem, Jan Willem Klop, and Roel de Vrijer editors*. Cambridge University Press, 2003.
[20] Vincent van Oostrom. Confluence by decreasing diagrams. *Theor. Comput. Sci.*, 126(2):259–280, 1994.
[21] Vincent van Oostrom. Developing developments. *Theor. Comput. Sci.*, 175(1):159–181, 1997.
[22] Vincent van Oostrom. Confluence by decreasing diagrams converted. In Voronkov A., editor, *RTA*, volume 5117 of *Lecture Notes in Computer Science*, pages 306–320. Springer, 2008.
[23] Harald Zankl, Bertram Felgenhauer, and Aart Middeldorp. Labelings for decreasing diagrams. *J. Autom. Reasoning*, 54(2):101–133, 2015.