Confluence properties of rewrite rules by decreasing diagrams

Jiaxiang Liu

NNT : 2016SACLX044

Thèse de doctorat de Tsinghua University et de l'Université Paris-Saclay préparée à l'École Polytechnique

Ecole Doctorale n°580
Sciences et technologies de l'information et de la communication
Spécialité de doctorat : Informatique

Par

M. Jiaxiang Liu

Propriétés de Confluence des Règles de Réécriture par des Diagrammes Décroissants

Thèse présentée et soutenue à Palaiseau, le 10 octobre 2016.

Composition du Jury :

M.	Olivier Bournez	Professeur École Polytechnique	(Président du jury)
M.	José Meseguer	Professeur University of Illinois at Urbana-Champaign	(Rapporteur)
M.	Luke Ong	Professeur University of Oxford	(Rapporteur)
M.	Vincent van Oostrom	Docteur University of Innsbruck	(Examinateur)
M.	Gérard Huet	Directeur de recherche émérite INRIA	(Examinateur)
M.	Jean-Pierre Jouannaud	Professeur émérite Université Paris-Saclay	(Directeur de thèse)

Confluence Properties of Rewrite Rules by Decreasing Diagrams

Jiaxiang Liu

Supervisors

Prof. Jean-Pierre Jouannaud

Prof. Ming Gu

Abstract

Formal methods are increasingly used for developing critical software. Proof assistants based on type theories allow to formally prove properties of software, in particular partial or total correctness. In expressive type theories allowing for dependent types, computations based on rewriting play a fundamental role in identifying types up to computation, such as $even(2 + 2)$ and $even(4 + 0)$ which both compute to $even(4)$. This is possible thanks to two crucial properties of rewrite rules, termination and confluence. A third essential, more semantical property, is type preservation. Confluence is the property of rewriting-based computations expressing that the associated extensional relation is functional, implying uniqueness of normal forms, which exist thanks to termination. In this thesis, we are interested in confluence.

Note that this problem is already present in algebraic specification languages, such as OBJ or the functional kernel of Maude. In those simply typed languages without functional types, type preservation is an easy property of the rules, and proving termination can be done independently of confluence. The confluence proof can therefore use the termination property. This is not possible in typed theories, for which termination, confluence of typed terms, and type preservation, depend on each other. Proving confluence on untyped terms is the usual way out, and can then be done first. The difficulty is that computations do not terminate on untyped terms, hence confluence must be proved for non-terminating computations. Our interest in this thesis is therefore to develop confluence proof methods in the presence of non-terminating computations.

It is well-known that confluence of a set of rewrite rules is undecidable. In the sub-case where rewriting terminates, methods for showing confluence have been well developed, and are based on the computation of "minimal diverging computations" called critical peaks, made of a minimal middle term called "overlap" which computes in two different ways, resulting in a so-called "critical pair".

In the case of non-terminating computations, a main result is that left-linear rewrite rules that have no critical pairs are always confluent, where a rule is left-linear when each one of its free variables cannot occur more than once in the left-hand side. This suggests that the notion of critical pairs plays a key role there too, but a general understanding of the confluence of non-terminating computations in terms of critical pairs is still missing.

Recently, van Oostrom proposed a framework based on decreasing diagrams, a notion that can capture the two main methods used in the literature for analyzing confluence, no matter whether the rewrite system is terminating or not. Based on that, Felgenhauer obtained a general result to solve the confluence problem of left-linear non-terminating systems via critical pairs, leaving the non-left-linear non-terminating case open.

This thesis is therefore devoted to the development of techniques that reduce confluence to the checking of critical pairs for rewrite systems that are possibly non-terminating and non-left-linear. To this end, we carry out a thorough investigation of the notion of decreasing diagrams, from the notion itself up to its applications.

The first part of this thesis focuses on the decreasing diagrams method itself, which is known to be complete: a relation on an abstract set is confluent if and only if it can be equipped with a (well-founded) set of labels such that every diverging computation, called peak, has a decreasing diagram, that is, its extremities can be joined by steps whose direction and labels satisfy some constraints with respect to the peak's rewrites and labels. The proof of completeness is based on Klop's notion of cofinal derivations, which is an infinite derivation playing the role of a normal form when computations do not terminate.

By giving an alternative simpler proof of the decreasing diagrams method, we succeed in extending the method and its completeness result to the modulo case, in which computations mix rewrite steps and equational steps which are strongly coherent, a notion used by Jouannaud and Muñoz to study termination of computations mixing rewrite steps and equational steps. A direct consequence is a new and concise proof of Toyama's celebrated modularity result of confluence for rewrite systems that are built from disjoint signatures and its modulo extension by Jouannaud and Toyama.

A second achievement of the thesis lifts up the abstract decreasing diagrams method to a slightly more concrete level. By generalizing the method on abstract positional rewriting introduced by Jouannaud and Li, and by extending it by a multi-labelled version, we propose a general framework for proving confluence of term rewrite systems in an axiomatic way which captures all results from the literature that we know of, in particular those relying on a notion introduced by Huet and further developed under the name of parallel closedness, which all appear as particular cases of decreasing diagrams.

The rest of the thesis deals with confluence of syntactic classes of concrete rewrite systems that are possibly non-terminating and non-left-linear.

A first idea is to split a rewrite system into a terminating part R_T and a left-linear, possibly non-terminating one R_{NT}. Again, we assume two disjoint signatures, $\mathcal{F}_T$ and $\mathcal{F}_{NT}$. R_T is built from symbols in $\mathcal{F}_T$. R_{NT} is built from arbitrary symbols, but assumed to be rank non-increasing, where the rank of a term is its maximal number of layers alternations. Then, the confluence of $R_T \cup R_{NT}$ can be reduced to the joinability of the critical pairs of R_T and the existence of decreasing diagrams for the critical pairs of R_T inside R_{NT}, as well as for some parallel critical pairs of R_{NT} with itself called rigid. The results, that are a strict generalization of Knuth–Bendix critical pair criterion for terminating computations, rely on a new rewrite relation, called "sub-rewriting", which allows to apply an R_T-rewrite provided the various possible instantiations of a non-linear variable can be (recursively) joined. This notion appears therefore as a restriction of conditional rewriting with left-linear conditional rewrite rules, in case the conditions are conjunctions of joinability predicates between variables.

The second idea investigated is a novel notion of rank, which is defined independently of any signature split: in essence, the maximum number of "linearized redexes" traversed from the root to a leaf in a term, where linearized redexes are instances of the linearized left-hand sides of rules. The main result here relies on two notions: sub-rewriting again, and "cyclic-unification", in other words, unification "à la PROLOG" without occurs-check. We then prove that a rank non-increasing rewrite system is confluent provided all its "cyclic critical pairs" have decreasing diagrams in which the cyclic equations obtained by unification can be used via their congruence closure. This result explains a variety of confluent and non-confluent examples due to Newman for its abstract version, Klop for its concrete version, and others for variations. We also show that our result is sharp, by showing that another more complex non-confluent rewrite system, due again to Klop, that happens to have no cyclic critical pair is indeed rank increasing.

We are currently investigating non-terminating higher-order computations as those we may find in Dedukti. This part of our work is still preliminary, hence will not be included in this thesis, despite the fact that it can be seen as a major practical application of these techniques.

Résumé

Cette thèse étudie la confluence des systèmes de récriture en l'absence de propriété de terminaison, pour des applications aux langages fonctionnels de premier ordre comme Maude, ou aux langages d'ordre supérieur comportant des types dépendants, comme Dedukti. Dans le premier cas, les calculs opérant sur des structures de données infinies ne terminent pas. Dans le second, les calculs non typés ne terminent pas à cause de la beta-réduction. Dans le cas où les calculs terminent, la confluence se réduit à celle des pics critiques, divergences minimales du calcul, obtenues à partir d'un terme médian appellé superposition qui se récrit de deux manière différentes en une paire de termes appellée critique. Dans le cas où les calculs terminent, le résultat de Knuth et Bendix dit que les calculs sont confluents si et seulement si les paires critiques sont joignables. Dans le cas où les calculs ne terminent pas, le résultat majeur est que les calculs définis par des règles linéaires à gauche et sans paires critiques confluent. Il s'agit donc d'étendre ce résultat aux systèmes dont les règles peuvent être non-linéaires à gauche et avoir des paires critiques.

L'étude la confluence est faite à partir de la méthode des diagrammes décroissants de van Oostrom, qui généralise les techniques utilisées antérieurement aussi bien pour des calculs qui terminent que pour des calculs qui ne terminent pas. Cette technique est abstraite, en ce sens qu'elle s'applique à des relations arbitraires opérant sur un ensemble abstrait. Elle consiste à équiper chaque étape de calcul d'un label pris dans un ensemble bien fondé. Un pic de calcul, composé d'un terme se récrivant de deux manières différentes, possède un diagramme décroissant lorsque ses extémités peuvent se récrire en un terme commun avec des étapes de calcul dont les labels sont plus petits, en un certain sens, que les labels du pic. La force de cette technique est sa complétude, c'est-à-dire que toute relation confluente peut-être équipée d'un système de labels (par des entiers) pour lequel tous ses pics possèdent des diagrammes décroissants. Ce résultat est basé sur un théorème assez ancien de Klop, qui définit pour les systèmes non-terminant, une espèce de forme normale sous la forme

d'une suite infinie de récritures élémentaires, appellée "dérivation cofinale".

Dans une première partie, nous révisitons les résultats de van Oostrom, et en proposons une preuve différente simple dans le but de les généraliser au cas des calculs dits "modulo", c'est-à-dire dans des quotients, qui mèlent des règles et des équations. Cette généralisation inclue la complétude, en faisant intervenir une généralisation de la notion de dérivation cofinale dans le cas des calculs fortement cohérents au sens de Jouannaud et Muñoz. Nous révisitons ensuite, et généralisons parfois, un grand nombre nombre de résultats fondamentaux de confluence qui ne nécessitent pas d'hypothèse de terminaison. C'est le cas des réductions parallèles-closes de Huet, au prix d'une généralisation mineure de la méthode de van Oostrom. C'est aussi le cas du théorème de modularité de Toyama et de sa généralisation aux quotients, due à Jouannaud et Toyama. Ces deux dernière généralisations sont intéressantes, car elles sont l'aboutissement d'une succession de travaux qui tous ont simplifié la preuve initiale de Toyama. Elles le sont pour une autre raison: elles montrent que la construction d'une dérivation cofinale au sens de Klop est elle-même modulaire.

La second partie de la thèse applique le théorème de van Oostrom et sa généralisation à des systèmes (concrets) de récriture de termes, ainsi qu'à plusieurs problèmes ouverts du domaine. Dans un premier temps, la technique de van Oostrom est appliquée aux systèmes positionels, qui constituent un intermédiaire entre les récritures abstraites et concrètes. Dans un second, elle est appliquée à deux problèmes importants. Le premier est la généralisation du résultat de Knuth et Bendix à des systèmes union d'un système arbitraire qui termine, et d'un système linéaire gauche gauche qui ne termine pas mais dont les paires critiques possèdent des diagrammes décroissants. Ce résultat s'avère être la première généralisation importante de celui de Knuth et Bendix, dans le sens où les calculs opérés sur les paires critiques du système qui termine sont exactement ceux produits par le résultat de Knuth et Bendix. La preuve de ce résultat utilise une stratification des termes obtenue par une condition portant sur la signature, ainsi que l'utilisation d'une nouvelle notion de récriture, la sous-récriture, qui permet de joindre des instances différentes d'une même variable pour déclencher le remplacement d'une instance de membre gauche de règle par l'instance du membre droit correspondant. Le second résultat s'affranchit des conditions de signature en proposant une nouvelle méthode de stratification, le décompte des redex amalgamés traversés en parcourant un terme de sa racine vers ses feuilles, un redex amalgamé étant défini comme une instance de membre gauche de règle ou d'un terme médian. La sous-récriture dans ce contexte introduit alors le calcul de paires-critiques par unification cyclique, une nouvelle interprétation de l'unification dans les arbres infinis rationels qui opère directement sur les arbres finis. Le résultat obtenu dans ce cadre a permis de résoudre une enigme ancienne: l'existence de système de règles n'ayant aucune paire critique, mais ne terminant pas. De fait, ces sytèmes avaient des paires critiques obtenues par unification cyclique.

L'application récente de ces techniques à des problèmes concrets d'ordre supérieur tirés de la théorie des types dépendants ne fait pas partie de la thèse bien que faisant partie des objectifs que nous nous étions fixés.

Acknowledgements

First and foremost, I would like to express my sincere gratitude toward Prof. Jean-Pierre Jouannaud, my supervisor, for his guidance and kind support. Jean-Pierre is a patient supervisor. He led me to this interesting rewriting world, taught me how to think, how to write and how to share ideas. He is also a wise mentor, inspiring me greatly during work as well as during life. Every discussion we had and the nights we worked together are meaningful moments for me.

I am deeply grateful to Prof. Ming Gu, my co-supervisor in Tsinghua University. She gave me such an opportunity to start this thesis, which has been changing my life. It is her strong support encouraging me to get over most difficulties during the thesis.

I would like to seize this opportunity to thank Tsinghua University and Prof. Jiaguang Sun for supporting me to study in École Polytechnique, and as well to thank École Polytechnique for providing me good environment and so much convenience making my stay in France wonderful.

I also wish to give many thanks to my thesis reviewers Prof. José Meseguer, Prof. Luke Ong and Dr. Vincent van Oostrom for their patient reading, constructive and detailed suggestions, and to all the other jury members Prof. Gérard Huet and Prof. Olivier Bournez, who kindly accepted to take part in the jury.

I would like to thank Prof. Yoshihito Toyama and Prof. Takahito Aoto for hosting me in Tohoku University, and Prof. Aart Middeldorp for inviting me to University of Innsbruck. Special thanks to Bertram Felgenhauer for the invaluable discussion with him during my stay in Innsbruck and during my whole thesis. I would also like to thank my co-authors Prof. Nachum

Dershowitz, Prof. Mizuhito Ogawa, Ali Assaf and Prof. Gilles Dowek. I am deeply impressed and influenced by their passions for knowledge and their great ability to solve problems.

Thanks to my friends Qian Wang, Jiazi Yi, Jie Yang, Shiguang Li, Guangyang Wen, Xinzi Rao, Dan Yu, Ling Qin, Han Zheng, Feng Xu, Jianyang Pan, Jing Yang, Ruxi Shi and Yaowu Zhang for the help in my daily life during my stay in France.

Last but not least, I am grateful to my parents and my sister. I could not have done this without your endless support.

* This thesis is supported in part by the National Natural Science Foundation of China under Grant 61272002.

Contents

List of Figures

List of Tables

One

Introduction

While software systems invade our life, embedded in most equipment of everyday use, at the office, in the house, in the garden, in the car, in our pockets, in our environment, and sometimes in ourselves, their correct functioning raises new challenges to the industry. Traditional techniques such as testing and static analysis have difficulties to eliminate all bugs in a system, let alone to ensure its correctness. This increases the need for formal methods to develop these sorts of software, especially those whose functioning is critical, such as in aeronautics, transportation, finance and medicine. There are three main trends in formal methods: *abstract interpretation* [CC77], targeting bugs, *model checking* [CGP01], targeting safety properties, and *formal proofs* (see, for instance, [BC04, Pau94, ORS92]), targeting total correctness of programs with respect to their specification. Formal proofs need being carried out with a proof assistant which checks that all proofs elaborated by the user are correct.

The core of a proof assistant that is based on type theory is a proof checker for the logical system on which it is based. These proofs contain logical steps, described by inference rules, and computational steps described by *rewrite rules*. Both are integrated in modern type theories which become more and more sophisticated in order to meet the needs for user-friendly proof assistants. In particular, rewrite rules may be user-defined. As a consequence, studying the meta-theory of these type theories is becoming too complex to be carried out entirely by hand, requiring computer support to do, at least, the error-prone calculations.

Rewriting is a non-deterministic mechanism for describing intensional computations, which is at the heart of algebraic specification languages as well as functional languages. Three properties of rewriting are fundamental, from which the most important properties of the logical system, soundness and decidability of type checking, can be derived: type preservation, confluence, and termination. This thesis is devoted to the investigation of the confluence property.

1.1 Confluence

Confluence is the property of rewriting expressing that the associated extensional relation is functional (if non-empty). It is a major property of functional programming languages and proof systems as well, since proofs are indeed functional programs by the Curry–Howard isomorphism. Confluence implies uniqueness of normal forms, and is therefore a key property to decide the congruence defined by computations, which is itself an essential ingredient of the type checking device of modern type theories.

Let $\to$ be a rewrite relation on a set. We denote by $\to^=$ its reflexive closure, by $\to^*$ its reflexive, transitive closure called *derivation*, and by $\leftrightarrow^*$ its reflexive, symmetric, transitive closure called *conversion* or *convertibility*. A triple $\langle u, s, v\rangle$ is called a *local peak* if $u \leftarrow s \to v$, a *peak* if $u \mathrel{{}^*{\leftarrow}} s \to^* v$. A conversion $u \leftrightarrow^* v$ or a pair $\langle u, v\rangle$ is *joinable* if $u \to^* t \mathrel{{}^*{\leftarrow}} v$ for some t and *strongly joinable* if $u \to^= t \mathrel{{}^={\leftarrow}} v$, where the specific form $\to^* \circ \mathrel{{}^*{\leftarrow}}$ of a conversion is called *joinability*. The rewrite relation $\to$ is *Church-Rosser* (resp., confluent, *locally confluent*) if every conversion (resp., peak, local peak) is joinable. It is *strongly confluent* if every local peak is strongly joinable.

It is well-known that confluence of a set of *rewrite rules* is undecidable in general [Hue80]. There are traditionally two main methods for showing confluence of a rewrite relation, in terminating and non-terminating cases, respectively. In both cases, there are abstract results at the level of relations on a set, and concrete results elaborating upon the abstract ones in the case of rewrite relations operating on a concrete structure, in general a term structure.

When rewrite relations are terminating, Newman proved that confluence of an abstract rewrite system is reducible to local confluence [New42]. Then Knuth and Bendix, followed by Huet, showed that local confluence of a rewrite relation on *terms*, called a *term rewrite relation*, is reducible to the joinability of pairs corresponding to specific local peaks called *critical pairs* [KB70, Hue80], which are finitely many. Knuth–Bendix's Lemma makes the confluence test of terminating term rewrite relations decidable.

As for the non-terminating case, Hindley and Rosen proved that confluence of an abstract rewrite relation is implied by its strong confluence [Hin64, Ros73], while Tait showed that *parallel rewriting* in pure λ-calculus is strongly confluent, which therefore implies confluence. Reduction of confluence to joinability of critical pairs is possible as well under strong linearity assumptions [Hue80], although practice favours the case of *orthogonal systems* where there are no such pairs.

Many efforts have been made for investigating non-terminating rewrite relations on terms, which can be viewed as labelled ordered trees, based on different assumptions, such as: *left-linearity* [Hue80, Toy88, Gra96, vO97, Oku98], a property stating that all left-hand sides of rewrite rules are linear, where a term is linear if each of its free variables occurs at most once; *simple-right-linearity* [TO94, OOT95], an assumption that for any rewrite rule, the right-hand side is linear and no variables occurring more than once in the left-hand side occur in the right-hand side; *strongly depth-preservation* [GOO96, GOO98], a characteristic that for any rewrite rule and any variable appearing in its both sides, the minimal depth of the variable occurrences in the left-hand side is greater than or equal to the maximal depth of the variable occurrences in the right-hand side; and *non-collapsingness* [SO10, SOO15], meaning that right-hand sides of no rewrite rules are variables. However, no general criterion based on critical pair computations is known when rewrite relations do not terminate.

1.2 Decreasing Diagrams

Based on de Bruijn's Lemma [dB78], in van Oostrom's seminal paper [vO94a], he succeeded in capturing both abstract confluence methods – Newman's Lemma and Hindley–Rosen's Lemma – within a single framework thanks to the notion of *decreasing diagrams* of a *labelled abstract relation*. He then improved it in [vO08a] to obtain a more flexible notion of decreasing diagrams for practical use.

In this setting, each *rewrite step* underlying a rewrite relation is decorated by an element belonging to an abstract set of *labels*, which is equipped with a well-founded order $\rhd$. A decreasing diagram for a local peak $u \;{}_{l}{\leftarrow}\; s \rightarrow_m v$ is defined as a conversion of the form $u \leftrightarrow^*_\alpha \circ \rightarrow^=_m \circ \leftrightarrow^*_\delta \circ {}^{=}_{l}{\leftarrow} \circ \leftrightarrow^*_\beta v$, where the labels in the sequence α (resp., β) are strictly smaller than l (resp., m), and the labels in the sequence δ are strictly smaller than l or m with respect to $\rhd$. Van Oostrom's result says that a rewrite relation is confluent if every local peak has a decreasing diagram. It is easy to see that decreasing diagrams are a generalization of the familiar notions of joinability: joinability is required by Newman's Lemma for terminating relations; strong joinability is required by Hindley–Rosen's Lemma for non-terminating relations.

The decreasing diagrams method has a remarkable property: it is proved to be *complete*, in the sense that, given any confluent rewrite relation on a *countable* set, there always exists a way to label the relation making it satisfy the decreasing diagram condition [vO94b]. This is still open for non-countable sets.

The notion of decreasing diagrams appears to be a conceptual breakthrough. In [JvO09], the method is applied to concrete term rewrite relations that are both left-linear and right-linear, opening the way to an analysis of non-terminating rewrite relations in terms of the existence of decreasing diagrams for their critical peaks. Since then, many confluence results based on decreasing diagrams have been obtained. We only cite a few here.

Hirokawa and Middeldorp showed that a left-linear and locally confluent term rewrite relation $\rightarrow$ is confluent if the *critical pair steps* are *relatively terminating* with respect to $\rightarrow$ [HM11], while Klein and Hirokawa obtained an extension of Knuth–Bendix's Lemma on relatively terminating term rewrite relations, by checking joinability of *extended critical pairs* [KH12]. As for a more directly applicable result, Felgenhauer proved that confluence of left-linear term rewrite relations can be reduced to the existence of decreasing diagrams for their *parallel critical pairs* [Fel13b]. Further, he and van Oostrom presented a new result of decreasing diagrams for a generalization of confluence in the presence of equations, called the *Church-Rosser modulo* property [FvO13]. On the other hand, Aoto et al. investigated the confluence of non-left-linear term rewrite relations by combining the decreasing diagrams technique with *persistency* of confluence [ATU14], where persistency of confluence says that if a rewrite relation on *sorted* terms is confluent then it is confluent on all terms when eliminating sorts [AT97].

1.3 This Thesis

The ambition of this thesis is to develop techniques that reduce confluence of non-terminating rewrite relations on a term structure to the computation and checking of critical pairs, specifically in the case of term rewrite relations which are generated by non-left-linear rewrite rules.

To this end, we thoroughly investigate the notion of decreasing diagrams and its applications. We address three different kinds of issues:

1. The proof of the decreasing diagrams method is revised, which allows us to investigate its generalization in the presence of equations, and give a *new proof* of well-known existing modularity results.

2. The decreasing diagrams technique is applied to *abstract positional rewrite relations*, which builds a bridge between abstract rewriting and term rewriting.

3. A new rewrite relation is introduced, *sub-rewriting*, whose role is to linearize the non-left-linear variables of the rewrite rules and recursively check when used that their different instances can be joined. Under different assumptions on the rules, confluence of new classes of non-

terminating, non-left-linear term rewrite systems can then be reduced to the checking of (some variant of) their critical pairs by using the decreasing diagrams method.

1.3.1 Decreasing Diagrams and Modularity

In Chapter 3, we revise the proof of van Oostrom's decreasing diagrams method following the work by Jouannaud and van Oostrom [JvO09], via a technique called *diagram rewriting*. The diagram rewriting technique replaces a local peak in a conversion by its associated decreasing diagram to obtain a new conversion. When diagram rewriting terminates on all conversions of a rewrite relation, then the rewrite relation must be confluent. We give a new, simple order on conversions that establishes the confluence of rewriting under the assumption that every local peak has a decreasing diagram.

A generalization of decreasing diagrams is then proposed for *rewrite modulo* relations $\langle S, E\rangle$, made of a rewrite relation $\rightarrow_S$ and a symmetric relation $\leftrightarrow_E$. When considering rewriting modulo, confluence should be generalized to the *Church-Rosser modulo* property: a rewrite modulo relation $\langle S, E\rangle$ is Church-Rosser modulo E if every $(S \cup E)$*-conversion* $u \leftrightarrow^*_{S\cup E} v$ is *(S-)joinable modulo* E (or say *up to* E), that is, $u \rightarrow^*_S \circ \leftrightarrow^*_E \circ {}_S^*\!\!\leftarrow v$. We show that the decreasing diagrams method scales to the modulo case, thanks to a generalization of our order on conversions.

This chapter builds as well on a fundamental notion that characterizes confluence of possibly non-terminating relations, Klop's *cofinal derivations* [Klo80]. A cofinal derivation of a *convertibility class* is a possibly infinite derivation that each element of the convertibility class can rewrite to some element in the derivation. It plays the role of a normal form when the relation is non-terminating. Cofinal derivations were used by van Oostrom to obtain the completeness of his decreasing diagrams method, by labelling each rewrite step $u \rightarrow v$ with the minimum number of steps from v to the cofinal derivation of its convertibility class [vO94b]. We show that cofinal derivations can be used to give a new, concise proof of Toyama's celebrated modularity theorem [Toy87] and its recent extensions to rewriting modulo [JT08] in the case of *strongly-coherent systems*, an assumption discussed in depth within the chapter. This is done by generalizing cofinal derivations to *cofinal streams*, allowing us in turn to generalize van Oostrom's completeness result to the modulo case.

1.3.2 Decreasing Diagrams on Abstract Positional Rewriting

Shown to be complete via Klop's notion of cofinal derivations [Klo80], the decreasing diagrams method becomes a hammer for tackling confluence problems. When applying the method to show the confluence of a particular rewrite relation, the key is now to find a labelling that makes the relation satisfy the decreasing diagrams condition. Since cofinal derivations are non-constructive, the completeness result indeed gives us little information about how to construct a *local* labelling, which is a function from rewrite steps to labels. Common labellings such as *self-labelling* and *rule-labelling* [vO08a] have no relationship whatsoever with the completeness result. Indeed, finding good labellings in practice has shown to be a hard task.

Another problem pops up when applying the abstract decreasing diagrams technique to a concrete rewrite relation on a term structure. Our experience is that difficulties come essentially from *ancestor (local) peaks*, which are joinable in various ways depending on linearity assumptions of the relation. The technicalities to make them decreasing get much more complex in the absence of linearity assumptions.

In Chapter 4, inspired by the work of Jouannaud and Li [JL12a], we lift the notion of decreasing diagrams to abstract positional rewriting, a level intermediate between abstract rewriting and term rewriting. Positional rewriting carries information about an abstract notion of *positions*, while remaining a relation on an abstract set whose elements have no structure. We further give different ways to define decreasing diagrams for abstract positional rewriting, which are guidelines on how to label a relation and to check its confluence.

In Chapter 4, motivated by Huet's *parallel closedness* criterion [Hue80, Lemma 3.3], we investigate the *coloured* (or *commutation*) version of decreasing diagrams [vO94a, vO08a]. A simple extension, *multi-labelled* decreasing diagram, is proposed to capture Huet's parallel closedness criterion as well as its generalization [Toy88].

1.3.3 Confluence of Rewrite Unions

Knuth and Bendix showed that confluence of a terminating term rewrite system can be reduced to the joinability of its finitely many critical pairs [KB70]. In Chapter 5, a novel notion of rewriting based on a signature split, *sub-rewriting*, is proposed. We show that Knuth–Bendix's Lemma is still true of a term rewrite system $R_T \cup R_{NT}$ such that R_T is terminating and R_{NT} is a left-linear, *rank non-increasing*, possibly non-terminating term rewrite system. Confluence can then be reduced to the joinability of the critical pairs of R_T and to the existence of decreasing diagrams for the critical pairs of R_T inside R_{NT} as well as for the *rigid parallel critical pairs* of R_{NT}. Our notion of rigid parallel critical pairs is computed by *unifying* several copies of a *single* left-hand side of rewrite rule, hence the name "rigid", with another left-hand side of a rule at *disjoint* positions, which is a restriction of the notion of *parallel critical pairs* [Gra96] used in [Fel13b, ZFM15] that requires unifying several – possibly different – left-hand sides of rules with another left-hand side of rule at disjoint positions.

1.3.4 Confluence of Layered Rewrite Systems

Consider a famous term rewrite system NKH $= \{f(x,x) \to a,\ f(x,c(x)) \to b,\ g \to c(g)\}$, which is inspired by an abstract example of Newman, algebraized by Klop and publicized by Huet [Hue80]. It is critical pair free but non-confluent. Indeed, it enjoys non-joinable non-local peaks such as $a \leftarrow f(g,g) \to f(g,c(g)) \to b$. Inspired by the example, its confluent and as well non-confluent variations, in Chapter 6, we investigate the new, Turing-complete class of *layered* systems, whose left-hand sides of rules can only be *overlapped* at a multiset of disjoint or equal positions. Layered systems define a natural notion of *rank* for terms: the maximal number of non-overlapping redexes along a path from the root to a leaf. Overlappings are allowed in finite or infinite trees. Rules may be non-terminating, non-left-linear, or non-right-linear. Using a more general notion of sub-rewriting and a novel unification technique called *cyclic unification*, we show that rank non-increasing layered systems are confluent provided their *cyclic critical pairs* have *cyclic-joinable decreasing diagrams*.

1.3.5 Confluence in Dependent Type Theories

This work is not part of the thesis. We mention it for two reasons. First, it is announced in the introduction as a major motivation for this thesis. Second, while it was not completely finished at the time when the thesis was defended, it is now ready when this final version of the thesis is completed. It is quite clear that we would not have been successful without all the work presented in this thesis and the experience we have got with the arcana of the decreasing diagrams technique, in particular the work done on the confluence of rewrite unions.

1.4 Contributions and Organization of This Thesis

This thesis provides a thorough investigation of the notion of decreasing diagrams, from its basis to its applications, showing its theoretical importance as well as its applicability to confluence test of concrete term rewrite systems. The most significant contributions of this thesis can be summarized as follows:

1. We give an alternative proof of the decreasing diagrams method, and extend it to rewriting modulo, by defining a simple well-founded partial order that contains diagram rewriting (in Chapter 3).

2. We propose a notion of cofinal streams, generalizing cofinal derivations to the modulo case, which allows to generalize the completeness result of decreasing diagrams to the modulo case (in Chapter 3).

3. We obtain a new and simple proof of Toyama's modularity result of confluence, based on the use of cofinal derivations, and of cofinal streams in the modulo case (in Chapter 3).

4. We propose a general framework based on abstract positional rewriting for proving confluence of term rewrite systems, by using multi-labelled decreasing diagrams, a simple extension of decreasing diagrams (in Chapter 4).

5. By introducing a novel notion of sub-rewriting, we deliver a true generalization of Knuth–Bendix's confluence check, to rewrite systems made of two subsets, R_T of terminating rules and R_{NT} of possibly non-terminating, rank non-increasing, left-linear rules (in Chapter 5).

6. We propose a notion of *cyclic unifiers*, shown to be a powerful tool to handle unification problems with cyclic equations in the same way as we deal with unification problems without cyclic equations, thanks to the existence of most general cyclic unifiers which generalize the usual notion of most general unifiers (in Chapter 6). This notion is used to explain the non-confluence of certain non-left-linear, non-terminating, non-confluent systems that have no *apparent* critical pairs.

7. We prove that rank non-increasing layered systems are confluent provided their cyclic critical pairs have cyclic-joinable decreasing diagrams (in Chapter 6). This new class of rewrite systems possesses an intrinsic notion of term ranks, which does not invoke any signature split.

Basic notions and properties of abstract rewriting, term rewriting and decreasing diagrams are first recalled in Chapter 2. The results and contributions of this thesis that we just sketched are then presented in detail in Chapters 3, 4, 5 and 6, respectively. Conclusion comes last, in Chapter 7.

1.5 Publications

The results of this thesis have already appeared in the scientific literature:

- Chapter 3 is based on the paper "From Diagrammatic Confluence to Modularity" [JL12b] that was published in *Theoretical Computer Science*.

- Chapter 4 is based on the paper "Confluence: The Unifying, Expressive Power of Locality" [LJ14], which appeared in *Specification, Algebra, and Software - Essays Dedicated to Kokichi Futatsugi*.

- Chapter 5 is based on the paper "Confluence by Critical Pair Analysis" [LDJ14] that appeared in the *Rewriting and Typed Lambda Calculi - Joint International Conference (RTA-TLCA 2014)*.

- Chapter 6 is based on the paper "Confluence of Layered Rewrite Systems" [LJO15], which was published in the proceedings of *24th EACSL Annual Conference on Computer Science Logic (CSL 2015)*.

Two

Preliminaries

In this chapter, we recall some important notions of rewriting and decreasing diagrams, which will be used throughout this thesis. For more about rewriting, see [DJ90, BN98, Ter03], and for decreasing diagrams, see [vO94a, vO94b, vO08a]. Notions specific to each chapter will be introduced on the fly.

2.1 Abstract Rewriting

We first consider rewrite relations at an abstract level.

Definition 2.1.1. Given a set $\mathcal{O}$ of *objects*, an *(abstract) rewrite step* is a pair $\langle s, t \rangle$ for $s, t \in \mathcal{O}$, denoted by $s \to t$. An *(abstract) rewrite system* is composed of a set $\mathcal{O}$ and a set of rewrite steps, while an *(abstract) rewrite relation* is the relation corresponding to a rewrite system.

Note that a rewrite relation is just a binary relation on a set $\mathcal{O}$. We use R or $\to$ to denote a rewrite system[1] as well as its corresponding rewrite relation, and sometimes mention them without differences. We may also omit s, t to use only $\to$ representing a rewrite step $s \to t$ when no ambiguity can arise.

[1] The set $\mathcal{O}$ is usually omitted when it is clear from the context.

Given an arbitrary rewrite relation $\rightarrow$, we denote[2] its inverse by $\leftarrow$, its reflexive closure by $\rightarrowtriangle$, its symmetric closure by $\leftrightarrow$, its reflexive, transitive closure, called *reachability*, by $\twoheadrightarrow$, its transitive closure by $\rightarrow^+$, and its reflexive, symmetric, transitive closure called *convertibility*, by $\twoheadleftarrow\!\!\twoheadrightarrow$. The sequence $u_0 \rightarrow u_1 \ldots u_{n-1} \rightarrow u_n$ (resp., $u_0 \leftrightarrow u_1 \ldots u_{n-1} \leftrightarrow u_n$) of $\rightarrow$-steps (resp., $\leftrightarrow$-steps), where $u_0 = u$ and $u_n = v$, witnessing the membership of a given pair $\langle u, v\rangle$ to $\twoheadrightarrow$ (resp., $\twoheadleftarrow\!\!\twoheadrightarrow$) is called a *derivation* (resp., *conversion*). We use "$\circ$", which is sometimes omitted, to denote the composition of two conversions $u_0 \twoheadleftarrow\!\!\twoheadrightarrow u_n$ and $v_0 \twoheadleftarrow\!\!\twoheadrightarrow v_m$, writing $u_0 \twoheadleftarrow\!\!\twoheadrightarrow u_n \circ v_0 \twoheadleftarrow\!\!\twoheadrightarrow v_m$, requiring $u_n = v_0$. Given u, $\{v \mid u \twoheadrightarrow v\}$ is the set of *reducts* of u. We say that a reduct of u is *reachable* from u.

A conversion is called a *local peak* if it has the form $v \leftarrow u \rightarrow w$, a *peak* if it has the form $v \twoheadleftarrow u \twoheadrightarrow w$, a *joinability* if it is of the form $v \twoheadrightarrow u \twoheadleftarrow w$. A pair $\langle v, w\rangle$ is *convertible* if $v \twoheadleftarrow\!\!\twoheadrightarrow w$, *divergent* if $v \twoheadleftarrow u \twoheadrightarrow w$ for some u, *joinable* if $v \twoheadrightarrow t \twoheadleftarrow w$ for some t, and *strongly joinable* if $v \rightarrowtriangle t \leftarrowtriangle w$ for some t. A conversion $v \twoheadleftarrow\!\!\twoheadrightarrow w$ is (strongly) joinable if its corresponding pair $\langle v, w\rangle$ is so.

Now we can define confluence of a rewrite relation.

Definition 2.1.2. A rewrite relation $\rightarrow$ is *Church-Rosser* (resp., *confluent*, *locally confluent*) if every conversion (resp., peak, local peak) is joinable. It is *strongly confluent* if every local peak is strongly joinable.

Another important property of rewriting is termination.

Definition 2.1.3. A rewrite relation $\rightarrow$ on a set $\mathcal{O}$ is *terminating* if there exists no infinite sequence $u_1 \rightarrow u_2 \rightarrow \ldots$ of $\rightarrow$-steps in $\mathcal{O}$.

Two famous methods exist in the literature for checking confluence at the abstract level in the terminating case and possibly non-terminating case, respectively:

[2]Note that we define different notations from the superscript-style ones used in Chapter 1, which are standard in the literature (for example in [DJ90]), because in the following chapters, superscripts are preserved for other information.

Lemma 2.1.4 (Newman's Lemma [New42])**.** *A terminating rewrite relation is confluent if and only if it is locally confluent.*

Lemma 2.1.5 (Hindley–Rosen's Lemma [Hin64, Ros73])**.** *A rewrite relation is confluent if it is strongly confluent.*

2.2 Decreasing Diagrams

In [vO94a], van Oostrom proposed a novel technique, called *decreasing diagrams* for showing confluence of abstract rewrite relations. In his framework, rewrite systems should be extended by *labels*.

2.2.1 Labelled Rewriting

We now assume a set $\mathcal{L}$ of labels, equipped with a quasi-order $\trianglerighteq$ whose strict part $\triangleright$ is well-founded. We write $l = m$ (resp., $l \# m$) for equivalent (resp., incomparable) labels $l, m \in \mathcal{L}$. Given $l \in \mathcal{L}$, we also write $\alpha \triangleright l$ (resp., $l \triangleright \alpha$) if $m \triangleright l$ (resp., $l \triangleright m$) for all m in the multiset (or sequence) α of labels.

Definition 2.2.1. Given a set $\mathcal{O}$ of objects and a set $\mathcal{L}$ of labels, a *labelled rewrite step* is a triple $\langle s, t, l \rangle$ for $s, t \in \mathcal{O}$ and $l \in \mathcal{L}$, denoted by $s \to^{l} t$, where we may omit s, t or l. A *labelled rewrite system* is composed of a set $\mathcal{O}$ and a set of labelled rewrite steps, while a *labelled rewrite relation* is the corresponding relation.

The word "labelled" can be omitted when the context makes it clear that a relation is labelled.

The *underlying* rewrite system of a labelled rewrite system is obtained by projecting all its labelled rewrite steps on $\mathcal{O} \times \mathcal{O}$. On the other hand, a rewrite system can be lifted to a labelled one by defining a labelling function that maps each rewrite step to a label in $\mathcal{L}$.

Properties of rewrite systems are extended to its labelled version via the underlying rewrite system. All notions used for rewrite systems, such as peaks and joinability, can be extended naturally to labelled rewrite systems by equipping each rewrite step with a label. Notations are also extended as expected. In particular, reachability (resp., convertibility) is denoted by $\twoheadrightarrow^{\alpha}$ (resp., $\twoheadleftarrow\!\!\twoheadrightarrow^{\alpha}$), where α is a sequence of labels. When needed, we consider the sequence α to be a multiset of labels.

2.2.2 Local Diagrams

Given a labelled rewrite relation $\rightarrow$, we first consider specific structures made of a local peak and an associated conversion called *local diagrams*, and recall the important subclass of van Oostrom's decreasing (local) diagrams and their main property: a relation whose all local peaks have decreasing diagrams enjoys the Church-Rosser property, hence confluence.

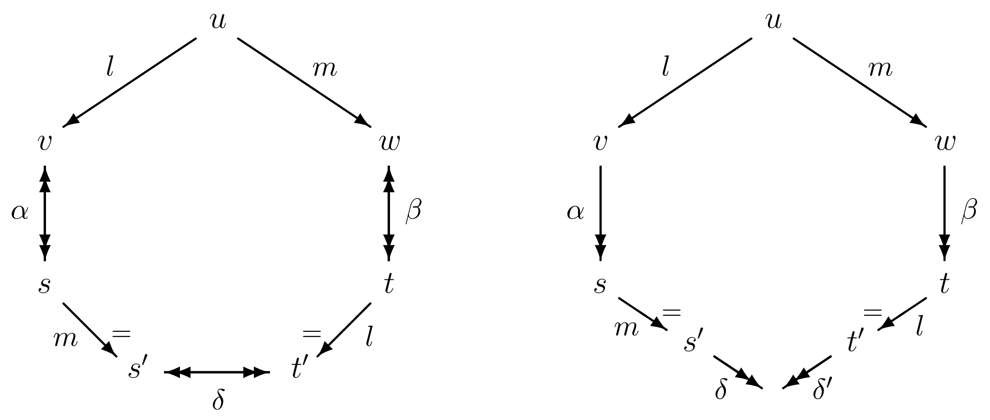
Decreasing diagrams were introduced in [vO94a], where it is shown that they imply confluence, and then further developed in [vO08a]. We will mostly use here the latter version, but present both.

Definition 2.2.2. A *diagram* D is a pair made of a peak $D_{peak} := v \twoheadleftarrow u \twoheadrightarrow w$ and a conversion $D_{conv} := v \twoheadleftarrow\!\!\twoheadrightarrow w$, where $u, v, w \in \mathcal{O}$.

Definition 2.2.3 (Local Diagrams)**.** A *local diagram* D is a diagram made of a local peak $D_{peak} := v \leftarrow u \rightarrow w$ and a conversion $D_{conv} := v \twoheadleftarrow\!\!\twoheadrightarrow w$, where $u, v, w \in \mathcal{O}$.

Definition 2.2.4 (Decreasing Diagrams [vO08a])**.** A local diagram D with peak $v \;{}^{l}\!\!\leftarrow u \rightarrow^{m} w$ is *decreasing* if its conversion D_{conv} has the form $v \twoheadleftarrow\!\!\twoheadrightarrow^{\alpha} s \twoheadrightarrow^{=m} s' \twoheadleftarrow\!\!\twoheadrightarrow^{\delta} t' \;{}^{l}\!\!\twoheadleftarrow^{=} t \twoheadleftarrow\!\!\twoheadrightarrow^{\beta} w$, satisfying the *decreasingness condition*: labels in α (resp., β) are strictly smaller than l (resp., m), and labels in δ are strictly smaller than l or m. See Figure 2.1 (i). The steps $s \twoheadrightarrow^{=m} s'$ and $t' \;{}^{l}\!\!\twoheadleftarrow^{=} t$ (resp., $v \twoheadleftarrow\!\!\twoheadrightarrow^{\alpha} s$ and $t \twoheadleftarrow\!\!\twoheadrightarrow^{\beta} w$, $s' \twoheadleftarrow\!\!\twoheadrightarrow^{\delta} t'$) are called the *facing steps* (resp., *side steps*, *middle steps*) of the diagram. We usually talk of decreasing diagrams, omitting the word "local".

It is worth noting that any local diagram decreasing for $\rhd$ is again decreasing for $\rhd' \supseteq \rhd$. Since a partial well-founded order can be embedded into a total one by the axiom of choice, partial well-founded orders have practical value only.



(i) Decreasing Diagram (ii) Joinably Decreasing Diagram

Decreasingness condition: labels in α (resp., β) are strictly smaller than l (resp., m), and labels in δ, δ' are strictly smaller than l or m.

Figure 2.1: Decreasing (Local) Diagrams

We refer to the first version of decreasing diagrams as *joinably decreasing diagrams*. It suffices for our needs in some cases.

Definition 2.2.5 (Joinably Decreasing Diagrams [vO94a])**.** A local diagram D with peak $v \,{}^{l}\!\leftarrow u \rightarrow^{m} w$ is *joinably decreasing* if its conversion D_{conv} is of the form $v \twoheadrightarrow^{\alpha} s \rightarrow^{m}_{=} s' \twoheadrightarrow^{\delta} \circ \,{}^{\delta'}\!\twoheadleftarrow t' \,{}^{l}_{=}\!\leftarrow t \,{}^{\beta}\!\twoheadleftarrow w$, satisfying the *decreasingness condition*: labels in α (resp., β) are strictly smaller than l (resp., m), and labels in δ, δ' are strictly smaller than l or m. See Figure 2.1 (ii).

Here comes the main result of the decreasing diagrams method:

Theorem 2.2.6 ([vO08a])**.** *A labelled rewrite relation is Church-Rosser (hence confluent) if all its local peaks have a decreasing diagram.*

Corollary 2.2.7 ([vO94a])**.** *A labelled rewrite relation is Church-Rosser (hence confluent) if all its local peaks have a joinably decreasing diagram.*

Remark 2.2.8. Newman's Lemma (Lemma 2.1.4) appears to be a particular case of Theorem 2.2.6, more precisely of Corollary 2.2.7, when using *self-labelling* [vO08a]: each rewrite step $u \rightarrow v$ is labelled by its source u (or target v), and labels are compared in the considered relation $\rightarrow$ which is well-founded.

Remark 2.2.9. Hindley–Rosen's Lemma (Lemma 2.1.5) is a particular case of Corollary 2.2.7, by *rule-labelling* [vO08a]: all rewrite steps $u \rightarrow v$ are labelled by the same label, for instance 0, and the labels are (strictly) compared in the empty relation.

2.2.3 Diagram Rewriting

Definition 2.2.10. *Diagram rewriting* is the rewrite relation $\Rightarrow_{\mathcal{D}}$ on conversions associated with a set $\mathcal{D}$ of local diagrams, in which a local peak is replaced by one of its associated conversions:

$$\pi \circ D_{peak} \circ \psi \;\Rightarrow_{\mathcal{D}}\; \pi \circ D_{conv} \circ \psi \quad \text{for some } D \in \mathcal{D}$$

where π, ψ are conversions.

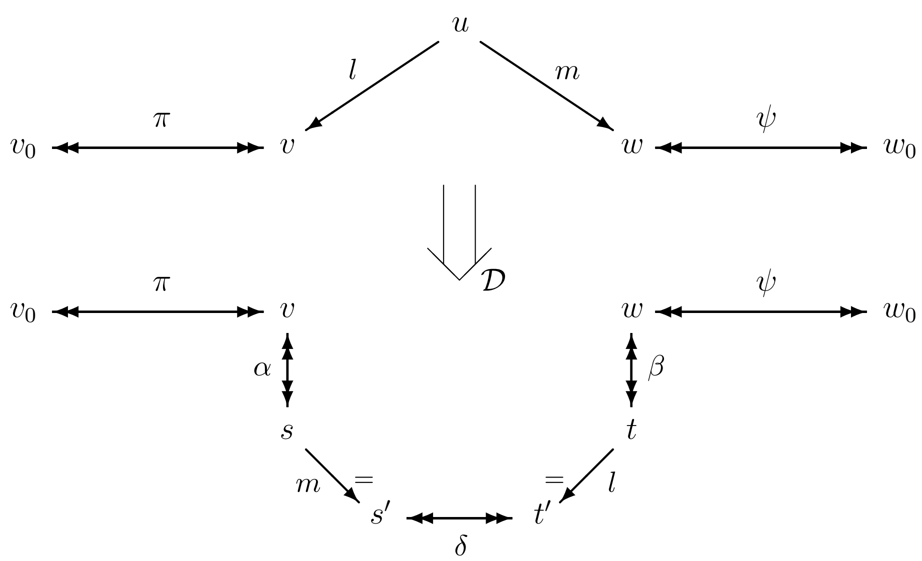


Figure 2.2: Diagram Rewriting with a Set $\mathcal{D}$ of Decreasing Diagrams

The replacement performed by diagram rewriting with a set $\mathcal{D}$ of decreasing diagrams is depicted in Figure 2.2. In [JvO09], Jouannaud and van

Oostrom revised the proof of Theorem 2.2.6 by using diagram rewriting. They proved the following result implying the Church-Rosser property, thus confluence, as a corollary:

Theorem 2.2.11 ([JvO09]). *The rewrite relation $\Rightarrow_{\mathcal{D}}$ terminates for any set $\mathcal{D}$ of decreasing diagrams.*

Corollary 2.2.12. *Assume that $T \subseteq \mathcal{O}$ and $\mathcal{D}$ is a set of decreasing diagrams in T such that the set of T-conversions, that is conversions only consisting of objects in T, is closed under $\Rightarrow_{\mathcal{D}}$. Then, the restriction of $\rightarrow$ to T is Church-Rosser if every local peak in T has a decreasing diagram in $\mathcal{D}$.*

Note that this simple corollary of Theorem 2.2.11 is a reformulation of Theorem 2.2.6.

2.3 Term Rewriting

In this section, we consider concrete rewrite relations on a set of terms, called *term rewrite relations*.

2.3.1 Term Algebras

Given a *signature* $\mathcal{F}$ of *function symbols*, and a denumerable set $\mathcal{X}$ of *variables*, $\mathcal{T}(\mathcal{F},\mathcal{X})$ denotes the set of *terms* built up from $\mathcal{F}$ and $\mathcal{X}$, which is the smallest set containing $\mathcal{X}$ such that $f(t_1,\ldots,t_n) \in \mathcal{T}(\mathcal{F},\mathcal{X})$ whenever $f \in \mathcal{F}$ with arity n and $t_i \in \mathcal{T}(\mathcal{F},\mathcal{X})$ for $i \in [1,n]$. We reserve letters x,y,z for variables, f,g,h for function symbols, and s,t,u,v,w for terms. Sometimes we write f^n to indicate the arity n of $f \in \mathcal{F}$. Terms can be viewed as finite labelled ordered trees.

Positions are finite strings of positive integers. We use o,p,q for arbitrary positions, the empty string Λ for the root position, and "$\cdot$" for concatenation of positions or sets thereof. We denote by $\mathcal{P}os(t)$ the set of positions of the term t, and by $\mathcal{FP}os(t)$ the set of positions of function symbols in t. Given a position $p \in \mathcal{P}os(t)$, we use $t(p)$ to denote the function symbol at position

p in t, $t|_p$ for the *subterm* of t at p, and $t[u]_p$ for the result of replacing $t|_p$ with u at p in t. We may omit the position p, writing $t[u]$ for simplicity. We call $t[\cdot]_p$ a *context*, which is a term where $t|_p$ is replaced by a fresh nullary symbol in t. Given a term t, $t(\Lambda)$ is called t's *head (symbol)*, $\#_x(t)$ is the number of occurrences of the variable x in t, and $|t|$ is the size of t, which is defined as $|x| = 0$ with $x \in \mathcal{X}$ and $|f^n(t_1, \ldots, t_n)| = 1 + \Sigma_1^n |t_i|$ with $f^n \in \mathcal{F}$. We use $\mathcal{V}ar(t_1, \ldots, t_n)$ for the set of variables occurring in $\{t_i\}_i$. A term t is *linear* if no variable of $\mathcal{V}ar(t)$ occurs more than once in t, *ground* if $\mathcal{V}ar(t) = \varnothing$.

We use $\geq_{\mathcal{P}}$ for the partial prefix order on positions (further from the root is bigger), $p\#q$ for incomparable positions p, q, called *disjoint*. Given sets P, Q of positions, we use the following abbreviations: $P \geq_{\mathcal{P}} Q$ (resp., $P >_{\mathcal{P}} Q$) if $(\forall p \in P)(\exists q \in max(Q))\, p \geq_{\mathcal{P}} q$ (resp., $p >_{\mathcal{P}} q$), where $max(Q)$ is the set of maximal positions in Q. We use p for the singleton set $\{p\}$. Given a term t and positions $p_i \in \mathcal{P}os(t)$ for $i \in [1, n]$ satisfying $p_i \# p_j$ if $i \neq j$, the notation $t[u_1, \ldots, u_n]_{p_1, \ldots, p_n}$ is an abbreviation for the term $t[u_1]_{p_1} \ldots [u_n]_{p_n}$, which is also written as $t[u_1, \ldots, u_n]_P$ when $P = \{p_1, \ldots, p_n\}$.

Substitutions are mappings from variables to terms, extended to homomorphisms from terms to terms. A substitution is called a *variable substitution* when it maps variables onto variables, and a *variable renaming* when also bijective. The *domain* of a substitution σ is the set $\mathcal{D}om(\sigma) := \{x \in \mathcal{X} \mid \sigma(x) \neq x\}$. Its *variable range* is $\mathcal{VR}an(\sigma) := \bigcup_{x \in \mathcal{D}om(\sigma)} \mathcal{V}ar(\sigma(x))$. A substitution of finite domain $\{x_1, \ldots, x_n\}$ is written as in $\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ or $\{x_i \mapsto t_i\}_{i \in [1..n]}$. We define $\sigma_{|X}$ as the restriction of σ to a subset X of variables, by $\sigma_{|X}(x) = \sigma(x)$ if $x \in X$ and $\sigma_{|X}(y) = y$ otherwise. And we denote by $\sigma_{|\neg X}$ for the restriction of σ to $\mathcal{D}om(\sigma) \setminus X$. A substitution σ is *ground* if for each $x \in \mathcal{X}$, $\sigma(x)$ is ground. We use Greek letters for substitutions and postfix notation for their application.

The strict *subsumption order* $\gtrdot$ on terms (resp., substitutions) associated with the quasi-order $s \mathrel{\underline{\gtrdot}} t$ (resp., $\sigma \mathrel{\underline{\gtrdot}} \tau$) iff $s = t\theta$ (resp., $\sigma = \tau\theta$) for some substitution θ, is well-founded[3]. t (resp., τ) is then said to be *more general*

[3]Note that $\gtrdot$ is well-founded on substitutions provided that the domains are finite, which is the case we discuss in the thesis.

than s (resp., σ). Given two terms s, t, computing the substitution σ whenever it exists such that $s = t\sigma$ (resp., $s\sigma = t\sigma$) is called *(pattern) matching* (resp., *unification*) and σ is called a *match* (resp., *unifier*). Two unifiable terms s, t have a unique (up to variable renaming) *most general unifier* $mgu(s, t)$, which is the smallest with respect to subsumption. The result remains true when unifying terms $s, t_1, \ldots, t_n$ at a set of disjoint positions $\{p_i\}_1^n$ such that $s|_{p_1}\sigma = t_1\sigma \wedge \ldots \wedge s|_{p_n}\sigma = t_n\sigma$, of which the previous result is a particular case when $n = 1$ and $p_1 = \Lambda$.

2.3.2 Term Rewrite Systems

In a term rewrite relation, rewrite steps are generated by *rewrite rules*.

Definition 2.3.1. Given a signature $\mathcal{F}$ and a set $\mathcal{X}$ of variables. A *rewrite rule* is a pair of terms in $\mathcal{T}(\mathcal{F}, \mathcal{X})$, written $l \to r$, whose *left-hand side* l is not a variable and whose *right-hand side* r satisfies $\mathcal{V}ar(r) \subseteq \mathcal{V}ar(l)$. A *(term) rewrite system* is composed of a signature $\mathcal{F}$, a set $\mathcal{X}$ of variables and a set R of rewrite rules. A rewrite rule $l \to r$ is *left-linear* (resp., *right-linear*, *linear*, *collapsing*) if l is a linear term (resp., r is a linear term, l and r are linear terms, r is a variable). A rewrite system is *left-linear* (resp., *right-linear*, *linear*) if all its rules are so.

The signature $\mathcal{F}$ and the set $\mathcal{X}$ of variables are often omitted when they are clear. The rewrite system is then represented by its set R of rewrite rules.

Definition 2.3.2. A term u *rewrites* to a term v at position $p \in \mathcal{P}os(u)$ with the rule $l \to r \in R$, written as $u \to^p_{l \to r \in R} v$, if $u|_p = l\sigma$ and $v = u[r\sigma]_p$ for some substitution σ. The term $l\sigma$ is a *redex*. We may omit p, R as well as $l \to r$, writing for example $u \to_R v$.

Rewriting extends naturally to lists of terms of the same length, hence to substitutions of the same domain.

Consider a local peak in a term rewrite system, we distinguish three cases following Huet [Hue80]:

Definition 2.3.3. Given a term rewrite system R, a local peak $v \;{}_{l \to r}^{\;\;p}\!\!\leftarrow u \to_{g \to d}^{q} w$ is:

- a *disjoint peak*, if $p \# q$;
- an *ancestor peak*, if $q >_{\mathcal{P}} p \cdot \mathcal{FP}os(l)$;
- a *critical peak*, if $q \in p \cdot \mathcal{FP}os(l)$.

The notion of *critical pairs* lies at the heart of most results showing confluence of term rewrite systems. It is of course the basis of the well-known Knuth–Bendix's Lemma.

Definition 2.3.4 (Critical Pairs)**.** Given two different rules $l \to r, g \to d$, being possibly two copies of the same rule, and a position $p \in \mathcal{FP}os(l)$. Variables are renamed such that $\mathcal{V}ar(l) \cap \mathcal{V}ar(g) = \varnothing$. Assuming σ is a most general unifier between $l|_p$ and g, then $l\sigma$ is the *overlap* and $\langle r\sigma, l\sigma[d\sigma]_p \rangle$ is the *critical pair* of $g \to d$ on $l \to r$ at p. Critical pairs of a term rewrite system R are all critical pairs computed between any two rules in R at any possible positions.

We end up this section with the most celebrated results for checking confluence of terminating term rewrite systems.

Lemma 2.3.5 ([Hue80])**.** *A terminating term rewrite system is locally confluent if and only if all its critical pairs are joinable.*

Lemma 2.3.6 (Knuth–Bendix's Lemma [KB70])**.** *A terminating term rewrite system is confluent if and only if all its critical pairs are joinable.*

Three

Decreasing Diagrams and Modularity

In 1987, Toyama proved a famous, major result stating that confluence is a *modular* property of term rewrite systems: given two confluent term rewrite systems sharing absolutely no function symbols, their union is as well a confluent term rewrite system [Toy87]. Toyama's original proof was rather intricate, but an improved proof was later given by Klop, Middeldorp, Toyama and de Vrijer [KMTdV94]. Toyama's theorem was then extended in three different directions. In 1994, Ohlebusch proved that modularity was preserved for term rewrite systems sharing *constructor* symbols, provided finitely many constructors only could pop up from a given term [Ohl94]. In 2006, Jouannaud gave a new, simple proof of Toyama's modularity theorem [Jou06] which was further improved by Jouannaud and Toyama who showed that it indeed scales to all known notions of *rewriting modulo* [JT08]. Finally, van Oostrom proved in 2008 that *constructive* confluence is modular, defining constructive confluence as the ability to recursively transform a convertibility proof into a joinability proof [vO08b].

At the root of van Oostrom's proof is the notion of decreasing diagrams. Note that decreasing diagrams associate specific conversions to local peaks, whose labels are smaller in some sense than those of the local peak they aim at replacing. Any convertibility proof can then be converted into a joinability proof by diagram rewriting: recursively replacing its local peaks by their associated decreasing diagrams. Using a subtle characterization of confluence for arbitrary (possibly non-terminating) relations by *cofinal derivations* due to Klop [Klo80], van Oostrom showed that his decreasing diagrams method is complete: any confluent relation whose convertibility classes are countable, can be labelled in a way that makes it a labelled relation satisfying the decreasing diagrams condition. The constructive version of Toyama's theorem appears to be a side benefit of proving the result by means of decreasing diagrams.

Our first contribution in this chapter is an elegant proof that replacing local peaks by their associated decreasing diagrams terminates, which is the key technical result behind van Oostrom's decreasing diagrams method [vO94a, vO08a]. This proof simplifies further [JvO09], where this result appeared first, and is generalized here to rewriting modulo. The second is the notion of *cofinal streams*, a natural extension of cofinal derivations under a *strong coherence* assumption (and countability of convertibility classes), which allows us to prove completeness of decreasing diagrams for characterizing the Church-Rosser modulo property under these two assumptions. The last is a new, concise proof of Toyama's modularity theorem based on cofinal derivations which scales to rewriting modulo via cofinal streams.

The organization of this chapter follows this description. The decreasing diagrams method on abstract labelled relations is discussed in Section 3.1, followed by cofinal derivations and streams in Section 3.2. Completeness and Modularity are considered in Sections 3.3 and 3.4, respectively. We conclude this chapter in Section 3.5.

3.1 Diagrammatic Church-Rosser Property

3.1.1 Plain Labelled Rewriting

Labelled rewriting is also called *plain* labelled rewriting, when we need to distinguish it with the *modulo* case.

Given a labelled rewrite relation $\rightarrow$ on a set $\mathcal{O}$, we call *convertibility class* of an object s the set $\overline{s}$ of objects that are convertible to s. In this chapter, we sometimes need closing conversions $u \twoheadleftarrow\!\!\twoheadrightarrow v$ by juxtaposition, yielding sequences of the form $u = u_1 \leftrightarrow^{l_1} v_1 \ldots u_n \leftrightarrow^{l_n} v_n = v$, called *conversations*, in which v_i and u_{i+1} cannot be identified as in conversions, since possibly different. To decompress notation, "$\circ$" is also used to denote the composition of two conversations.

3.1.2 Diagram Rewriting

In [JvO09], Jouannaud and van Oostrom proved Theorem 2.2.11 that diagram rewriting terminates for any set of decreasing diagrams, implying the Church-Rosser property, thus confluence, as a corollary.

The difficulty in the proof is to define a measure on conversions that decreases when replacing a local peak by its associated conversion. Our new measure below is based on two notions: that of a visible step in a conversation introduced in [JvO09], that makes invisible all rewrite steps of a smaller label located ahead of them; and that of *shadow* of a conversation. It is defined on conversations, because conversions are not closed under replacement of steps by arbitrary smaller conversions, an operation used in the proof. On the other hand, $\Rightarrow_{\mathcal{D}}$ preserves conversions, since the peak and its associated smaller conversion relate the same pair of objects.

Definition 3.1.1 (Visible Steps [JvO09])**.** Given conversations π, ψ, a rewrite step $\leftrightarrow^l$ is *visible* in a conversation $\pi \circ \leftrightarrow^l \circ \psi$ if there is no visible step $\rightarrow^m$ in π or ${}^m\!\!\leftarrow$ in ψ with $m \rhd l$ (the base case corresponding to empty π and ψ). Otherwise, $\leftrightarrow^l$ is *hidden* by some visible step *aiming* at it. We denote by $\textsc{vs}(\pi)$ (resp., $\textsc{vl}(\pi)$) the multiset of *visible steps* (resp., *visible labels*) in π.

Consider the conversation $\pi = \rightarrow^a \circ {}^b\!\!\leftarrow \circ \rightarrow^c \circ \rightarrow^b \circ {}^a\!\!\leftarrow$, with the ordered set of labels $c \rhd b \rhd a$. The step $\rightarrow^a$ is hidden because of ${}^b\!\!\leftarrow$ to its right, while $\rightarrow^b$ and ${}^a\!\!\leftarrow$ are hidden with $\rightarrow^c$ to their left. Hence $\textsc{vl}(\pi) = \{b, c\}$.

The relationship between the set of visible labels of a conversation and van Oostrom's lexicographic maximum measure [vO94a] is explained in [JvO09], it generalizing the idea of lexicographic maximum measure.

Definition 3.1.2. The *shadow* of a conversation π is the multiset of *shadows* of its visible steps, that is:

$$\begin{aligned} \mathrm{SH}(\pi) := \{&\langle\psi,\kappa\rangle \mid \pi = \psi \circ \to^l \circ \kappa \text{ with } \to^l \in \mathrm{VS}(\pi)\} \\ \cup\, \{&\langle\psi,\kappa\rangle \mid \pi = \kappa \circ {}^l\!\leftarrow \circ\, \psi \text{ with } {}^l\!\leftarrow \in \mathrm{VS}(\pi)\} \end{aligned}$$

We are ready for defining the interpretation of a conversation:

Definition 3.1.3. We interpret a conversation π by the pair $[\![\pi]\!] := \langle \mathrm{VL}(\pi), \mathrm{SH}(\pi)\rangle$ and define the partial order between conversations π, ψ as the smallest partial order such that

$$\pi \succ\!\!\succ \psi \quad \text{if} \quad [\![\pi]\!]\ (\rhd_{mul}, ((\succ\!\!\succ, \succ\!\!\succ)_{lex})_{mul})_{lex}\ [\![\psi]\!]\ .$$

We now need to show that our definition has indeed a least fixpoint, that is, that the underlying functional is monotonic. This follows from the coming observation, showing that the inductive comparisons by $\succ\!\!\succ$ are applied on strictly smaller conversations.

Lemma 3.1.4. *Let conversation $\pi := \psi \leftrightarrow^l \kappa$, with $\leftrightarrow^l \in \mathrm{VS}(\pi)$. Then, $\mathrm{VL}(\pi) \rhd_{mul} \mathrm{VL}(\psi)$ and $\mathrm{VL}(\pi) \rhd_{mul} \mathrm{VL}(\kappa)$.*

Proof. Since $\leftrightarrow^l \in \mathrm{VS}(\pi)$, the labels in $\mathrm{VL}(\psi \circ \kappa)$ are either already in $\mathrm{VL}(\pi)$ or strictly smaller than l. Hence $\mathrm{VL}(\pi) \rhd_{mul} \mathrm{VL}(\psi\circ\kappa)$. Further, $\mathrm{VL}(\psi\circ\kappa) \unrhd_{mul} \mathrm{VL}(\psi)$ and $\mathrm{VL}(\psi\circ\kappa) \unrhd_{mul} \mathrm{VL}(\kappa)$. The result follows by transitivity and irreflexivity. $\square$

In the rest of this section, π and ψ denote arbitrary conversations. We use the notations

$D_{peak} := {}^m\!\leftarrow \circ \to^n$,

$D_{conv} := \twoheadleftarrow\!\!\twoheadrightarrow^\alpha \circ \to^n \circ \twoheadleftarrow\!\!\twoheadrightarrow^\delta \circ {}^m\!\leftarrow \circ \twoheadleftarrow\!\!\twoheadrightarrow^\beta$ and

$D'_{conv} := \twoheadleftarrow\!\!\twoheadrightarrow^\alpha \circ \to^n \circ \twoheadleftarrow\!\!\twoheadrightarrow^\delta \circ {}^m\!\leftarrow \circ \twoheadleftarrow\!\!\twoheadrightarrow^\beta$,

with labels in α (resp., β) strictly smaller than m (resp., n), and labels in δ strictly smaller than m or n.

Our aim is to prove that our (well-founded) partial order contains diagram rewriting, hence implying that diagram rewriting terminates. A technical difficulty is that our order is *not* monotonic in general. Consider the steps $\rightarrow^a$ and ${}^a\!\leftarrow$, which have the same interpretation. Consider now the conversations $\rightarrow^b \circ \rightarrow^a$ and $\rightarrow^b \circ {}^a\!\leftarrow$ with $b \lhd a$, the first being bigger than the second in our order. Taking $\psi = \rightarrow^b$ and $\pi = \rightarrow^c$ with $a \rhd b \rhd c$, ψ being bigger than π, the conversation $\pi \rightarrow^a \psi$ is now smaller than $\pi\ {}^a\!\leftarrow \psi$. The next two (weak) monotonicity properties will however suffice.

Lemma 3.1.5. *If $l \rhd \alpha$, then $\pi \leftrightarrow^l \psi \ \ggcurly\ \pi \twoheadleftrightarrow^\alpha \psi$.*

Proof. By induction on the number of steps in $\pi \leftrightarrow^l \psi$. Note that the base case corresponds to empty conversations π and ψ, hence is a particular case of the first case of the induction step, which has two cases:

1. $\leftrightarrow^l$ is visible in $\pi \leftrightarrow^l \psi$. Then, $\mathrm{VL}(\pi \leftrightarrow^l \psi) \rhd_{mul} \mathrm{VL}(\pi \twoheadleftrightarrow^\alpha \psi)$, which concludes this case.

2. $\leftrightarrow^l$ is hidden in $\pi \leftrightarrow^l \psi$. Then, there is a visible step $\leftrightarrow^k$ in the conversation $\pi \leftrightarrow^l \psi$ aiming at $\leftrightarrow^l$ such that $k \rhd l$. By transitivity, $k \rhd \alpha$, hence $\mathrm{VL}(\pi \leftrightarrow^l \psi) = \mathrm{VL}(\pi \twoheadleftrightarrow^\alpha \psi)$. We therefore need to compare the shadows of both conversations, which are multisets of pairs of conversations. We pairwise compare the shadows of the same visible step. They are of the form: $\langle \pi', \pi'' \leftrightarrow^l \psi \rangle$ and $\langle \pi', \pi'' \twoheadleftrightarrow^\alpha \psi \rangle$ if the visible step $\rightarrow^m$ is in π; $\langle \pi \leftrightarrow^l \psi', \psi'' \rangle$ and $\langle \pi \twoheadleftrightarrow^\alpha \psi', \psi'' \rangle$ if the visible step $\rightarrow^m$ is in ψ; for the other two cases, the pairs must be flipped over. We conclude all four cases by induction, which finishes the proof. □

Lemma 3.1.6. $\pi D_{peak} \psi \ \ggcurly\ \pi D'_{conv} \psi$.

Proof. By induction on the number of steps in $\pi D_{peak} \psi$. As before, the base case corresponds to empty conversations π and ψ, hence is a particular case of the two cases of the induction step:

1. Both steps from D_{peak} are visible in $\pi D_{peak} \psi$, with $m \rhd n$ (resp., $n \rhd m$). Clearly, the step labelled by n (resp., m) is now hidden in $\pi D'_{conv} \psi$, hence there may be new visible steps from ψ (resp.,

π) whose all labels are strictly smaller than n (resp., m). On the other hand, visible steps from π, ψ remain unchanged, and therefore $\mathrm{VL}(\pi D_{peak}\psi) \rhd_{mul} \mathrm{VL}(\pi D'_{conv}\psi)$, which concludes this case.

2. Otherwise, the visibility status of the steps labelled by m, n of the local peak is entirely determined by π, ψ (in case π, ψ are both empty, then both steps of the local peak are visible), hence all steps in D'_{conv} which are not labelled by m, n are not visible in $\pi D'_{conv}\psi$. It follows that $\mathrm{VL}(\pi D_{peak}\psi) = \mathrm{VL}(\pi D'_{conv}\psi)$, and visible steps in $\pi D_{peak}\psi$ and $\pi D'_{conv}\psi$ are in one-to-one correspondence (facing steps from D_{peak} and D'_{conv} being associated with each other when visible). We now compare the shadows of the corresponding visible steps. By induction hypothesis, the shadow associated with a visible step from π, ψ is strictly smaller in $\pi D'_{conv}\psi$ than in $\pi D_{peak}\psi$. By Lemma 3.1.5, the shadows associated with the steps labelled by m and n (when visible) are strictly smaller as well in $\pi D'_{conv}\psi$ than in $\pi D_{peak}\psi$. Hence, $\pi D_{peak}\psi \ \rightarrowtail\!\!\!\!\succ \ \pi D'_{conv}\psi$. □

It is now time to prove that $\rightarrowtail\!\!\!\!\succ$ is indeed a well-founded partial order:

Lemma 3.1.7. *$\rightarrowtail\!\!\!\!\succ$ is a well-founded partial order on conversations satisfying $\pi D_{peak}\psi \ \rightarrowtail\!\!\!\!\succ \ \pi D_{conv}\psi$ for any decreasing diagram D and conversations π, ψ.*

Proof. We first prove well-foundedness: no conversation π is the origin of an infinite descending sequence in $\rightarrowtail\!\!\!\!\succ$. The proof is by induction on the definition of $\rightarrowtail\!\!\!\!\succ$. Since $\rhd$ is well-founded on labels, hence on multisets thereof, it suffices to show that $\mathrm{SH}(\pi)$ is not the origin of an infinite descending sequence for $((\rightarrowtail\!\!\!\!\succ, \rightarrowtail\!\!\!\!\succ)_{lex})_{mul}$. This follows from Lemma 3.1.4, the induction hypothesis and preservation of well-founded partial orders by multiset and lexicographic extensions.

Transitivity is by induction on the definition again.

Now comes the monotonicity property for local peaks. If both steps labelled m, n of D_{peak} occur in D_{conv}, then $\pi D_{peak}\psi \ \rightarrowtail\!\!\!\!\succ \ \pi D_{conv}\psi$ by Lemma 3.1.6. If not, adding them back to D_{conv} results in a new conversation D'_{conv}.

By Lemmas 3.1.6 and 3.1.5, $\pi D_{peak}\psi \twoheadrightarrow \pi D'_{conv}\psi \twoheadrightarrow \pi D_{conv}\psi$ and we are done. $\square$

Corollary 3.1.8 ([vO08a, vO08b]). *Assume that $\rightarrow$ is a labelled binary relation which all local peaks have a given decreasing diagram. Then $\rightarrow$ is* constructively confluent*: an arbitrary conversion can be recursively transformed into a joinability proof.*

Already mentioned in [vO08b], proofs based on Newman's Lemma or on Hindley–Rosen's Lemma yield constructive confluence in the very same sense. Van Oostrom used this fact to show a stronger version of Toyama's modularity theorem stating modularity of constructive confluence under the standard assumption of disjoint signatures.

Another important benefit of a proof based on a well-founded order on conversions is that it is a necessary building block for the design of a completion procedure. To this end, the ordering needs two monotonicity properties, with respect to elementary step replacement (Lemma 3.1.5) and with respect to local peak replacement (Lemma 3.1.7), see [BD07]. A preliminary completion procedure for the simple case of constant terms is given in [JvO09]. The general case of non-terminating rewrite rules built from an arbitrary graded signature needs much more work since there is no known technique yet to generate labels in this case.

Felgenhauer and van Oostrom presented another two different but novel well-founded orders on conversions in [FvO13]. The *iterative lexicographic path order* used in [FvO13] is more lightweight in the sense that it is equipped with simple interpretations on conversions, whose sizes are only linear in the number of steps in the conversions, while our order needs an exponential number of comparisons. The other one in [FvO13] is monotonic, resulting simpler proofs of Lemmas 3.1.5 and 3.1.6, while both our order and the one in [JvO09] are not.

3.1.3 Labelled rewriting modulo

We now turn our attention to a *labelled rewrite system modulo* (a *labelled rewrite system* for short) $\langle S, E\rangle$, made of a labelled rewrite relation $\rightarrow_S$ as before (S for short), and a symmetric labelled relation $\leftrightarrow_E$ (E for short). Note that E and S need not be disjoint. In this section, we are interested in the Church-Rosser property of their union $S \cup E$.

At this point, it is important to understand that $\rightarrow_S$ is not meant to be generated by a set of rules. Both $\rightarrow_S$ and $\leftrightarrow_E$ denote relations. It turns out that $\leftrightarrow_E$ will later denote the one-step equality relation generated by a set E of equations, but in general, $\rightarrow_S$ will not denote the rewrite relation generated by a set R of rules, but rewriting with R modulo E defined later. We need not refer to R in this section.

We shall now need several convertibility relations that will be distinguished by indexing the labelled relation in use: we use $\twoheadleftarrow\!\!\twoheadrightarrow_E$ for E-*conversion* and $\twoheadleftarrow\!\!\twoheadrightarrow_{S\cup E}$ for $(S \cup E)$-*conversion*. We reserve the notation $\overline{s}$ for the E-convertibility class of the element s. Conversations are as expected. We use $\twoheadrightarrow_{S\cup E}$ for the derivation relation of $\rightarrow_S \cup \leftrightarrow_E$, while *reachability* is now defined as $\twoheadrightarrow_S \circ \twoheadleftarrow\!\!\twoheadrightarrow_E$. Similarly, *joinability* modulo E of the pair $\langle v, w\rangle$ is now defined as $v \twoheadrightarrow_S s \twoheadleftarrow\!\!\twoheadrightarrow_E t \;{}_S\!\twoheadleftarrow w$ for some s, t, expressing the existence of a *joinability proof* modulo E.

Definition 3.1.9. A labelled rewrite system $\langle S, E\rangle$ is *Church-Rosser* modulo E if and only if any two $(S \cup E)$-convertible terms are joinable modulo E.

When E is the empty relation, the Church-Rosser property of S is characterized by the possibility of eliminating all local peaks from a given conversion. This is the essence of Theorem 2.2.11. In the case where E is non-empty, not only peaks, but also *cliffs* must be eliminated to get joinability proofs:

Definition 3.1.10 (Cliffs)**.** A *local cliff* (*cliff* for short) of S with E is a triple $\langle v, u, w\rangle$ such that $v \;{}^{m}_{S}\!\!\leftarrow u \leftrightarrow^{n}_{E} w$.

3.1.4 Diagram rewriting modulo

To extend our results to the modulo case, we make the following assumption:

Assumption 3.1. *The set of labels is completed with a minimum, labelling all E-steps and only them.*

This may look like a restrictive assumption, but it will however be enough to obtain completeness under a strong coherence assumption introduced later. We now need tuning our definitions and lemmas so as to fit with the modulo case.

The notion of visible step is unchanged. Since equality steps have a minimum label, they cannot hide any step and will be visible if and only if no rewrite step aims at them.

We define the *shadow* of a conversation in the modulo case as the heterogeneous multiset of pairs or two-element multisets, using $\cup$ for multiset union:

$$\begin{aligned}\mathrm{SH}(\pi) := {} & \{\langle\psi,\kappa\rangle \mid \pi = \psi \rightarrow^l_S \kappa \text{ with } \rightarrow^l_S \in \mathrm{VS}(\pi)\} \\ & \cup \{\langle\psi,\kappa\rangle \mid \pi = \kappa \ {}_S^l\!\!\leftarrow \psi \text{ with } {}_S^l\!\!\leftarrow \in \mathrm{VS}(\pi)\} \\ & \cup \{\{\psi,\kappa\} \mid \pi = \psi \leftrightarrow^l_E \kappa \text{ with } \leftrightarrow^l_E \in \mathrm{VS}(\pi)\}\end{aligned}$$

We shall of course make the assumption that pairs do not compare with the two-element multisets, and compare the whole multiset with a union of two orders, one for the pairs and the other for the two-element multisets.

The interpretation of a conversation is as before the pair made of its multiset of visible labels and its shadow, hence conversations are now compared in the smallest order such that

$$\pi \succ\!\!\succ \psi \quad \text{if} \quad [\![\pi]\!] \ (\rhd_{mul}, ((\succ\!\!\succ, \succ\!\!\succ)_{lex} \cup \succ\!\!\succ_{mul})_{mul})_{lex} \ [\![\psi]\!] \ .$$

Definition 3.1.11 (Decreasing Diagrams Modulo)**.** A *local diagram modulo* is a pair made of a local peak or cliff $\langle v, u, w\rangle$ and an associated conversion $v \twoheadleftarrow\!\!\twoheadrightarrow_{S\cup E} w$.

A local peak diagram $v \ {}_S^m\!\!\leftarrow \ u \rightarrow^n_S \ w$ is *decreasing* if the associated conversion has the form $v \twoheadleftarrow\!\!\twoheadrightarrow^{\alpha}_{S\cup E} \ s \rightarrow^n_S \ s' \twoheadleftarrow\!\!\twoheadrightarrow^{\delta}_{S\cup E} \ t' \ {}_S^m\!\!\leftarrow \ t \twoheadleftarrow\!\!\twoheadrightarrow^{\beta}_{S\cup E} \ w$, with labels in α (resp., β) strictly smaller than m (resp., n), and labels in

δ strictly smaller than m or n. $s \twoheadrightarrow^n_S s'$ and $t' \,{}^m_S\!\twoheadleftarrow t$ are called the *facing steps* of the conversion.

A local cliff diagram $v \;{}^m_S\!\leftarrow u \leftrightarrow^n_E w$ is *decreasing* if the associated conversion has the form $v \twoheadleftarrow\!\twoheadrightarrow^{\delta}_{S\cup E} t \;{}^m_S\!\twoheadleftarrow w$, with labels in δ strictly smaller than m (hence than m or n), $t \;{}^m_S\!\twoheadleftarrow w$ being the only *facing step* of the conversion.

In all coming lemmas and proofs, we use the following notations:
$D_{peak} := \;{}^m_S\!\leftarrow \circ \rightarrow^n_S$,
$D_{cliff} := \;{}^m_S\!\leftarrow \circ \leftrightarrow^n_E$,
$D_{convp} := \twoheadleftarrow\!\twoheadrightarrow^{\alpha}_{S\cup E} \circ \twoheadrightarrow^n_S \circ \twoheadleftarrow\!\twoheadrightarrow^{\delta}_{S\cup E} \circ \;{}^m_S\!\twoheadleftarrow \circ \twoheadleftarrow\!\twoheadrightarrow^{\beta}_{S\cup E}$,
$D'_{convp} := \twoheadleftarrow\!\twoheadrightarrow^{\alpha}_{S\cup E} \circ \rightarrow^n_S \circ \twoheadleftarrow\!\twoheadrightarrow^{\delta}_{S\cup E} \circ \;{}^m_S\!\leftarrow \circ \twoheadleftarrow\!\twoheadrightarrow^{\beta}_{S\cup E}$,
$D_{convc} := \twoheadleftarrow\!\twoheadrightarrow^{\delta}_{S\cup E} \circ \;{}^m_S\!\twoheadleftarrow$,
$D'_{convc} := \twoheadleftarrow\!\twoheadrightarrow^{\delta}_{S\cup E} \circ \;{}^m_S\!\leftarrow$,
with labels in α (resp., β) strictly smaller than m (resp., n), and labels in δ strictly smaller than m or n. Moreover, π, ψ will denote arbitrary conversations.

The proof that diagram rewriting terminates follows the same steps as before, with some additional lemmas for the E-steps.

Lemma 3.1.12. *If $l \rhd \alpha$, then $\pi \leftrightarrow^l_S \psi \;\;\ggcurly\;\; \pi \twoheadleftarrow\!\twoheadrightarrow^{\alpha}_{S\cup E} \psi$.*

Proof. The proof is the same as Lemma 3.1.5, except in the second case of the induction, where $\leftrightarrow^l_S$ is hidden in $\pi \leftrightarrow^l_S \psi$. Since $\mathrm{VL}(\pi \leftrightarrow^l_S \psi) = \mathrm{VL}(\pi \twoheadleftarrow\!\twoheadrightarrow^{\alpha}_{S\cup E} \psi)$, we need to compare the shadows of both conversations. As before, we pairwise compare pairs associated to the same visible S-step and two-element multisets associated to the same visible E-step. In both cases, we conclude by induction. $\square$

Lemma 3.1.13. $\pi \leftrightarrow^l_E \psi \;\;\ggcurly\;\; \pi \circ \psi$.

Proof. By induction on the number of steps in $\pi \circ \psi$. The base case where $\pi \circ \psi$ is empty is trivial. Otherwise, there are two cases:

1. $\leftrightarrow^l_E$ is visible in $\pi \leftrightarrow^l_E \psi$. Since l is minimum, $\mathrm{VL}(\pi \leftrightarrow^l_E \psi) = \mathrm{VL}(\pi \circ \psi) \cup \{l\}$, and we are done.

2. $\leftrightarrow^l_E$ is hidden in $\pi \leftrightarrow^l_E \psi$. By the same token, $\textsc{vl}(\pi \leftrightarrow^l_E \psi) = \textsc{vl}(\pi \circ \psi)$ and we easily conclude by induction. □

We can now show our main lemma for local peaks:

Lemma 3.1.14. $\pi D_{peak}\psi \ \ggcurly\ \pi D'_{convp}\psi$.

Proof. The proof is the same as Lemma 3.1.6, except the comparison of shadows for the second case. As in Lemma 3.1.12, we need to compare the two-element multisets of conversations for the same visible E-steps from π, ψ, as well as the pairs of conversations for the same visible S-steps from π, ψ, before to conclude by induction hypothesis. Then we use Lemma 3.1.12, instead of Lemma 3.1.5, to compare the conversation pairs of m and n when they are visible. □

Lemma 3.1.15. $\pi D_{peak}\psi \ \ggcurly\ \pi D_{convp}\psi$.

Proof. By Lemmas 3.1.14, 3.1.12 and transitivity. □

We now move to corresponding lemmas for cliffs:

Lemma 3.1.16. $\pi D_{cliff}\psi \ \ggcurly\ \pi D'_{convc}\psi$.

Proof. By induction on the number of steps in $\pi D_{cliff}\psi$. There are several cases depending on the visibility of the steps labelled m, n from D_{cliff} in $\pi D_{cliff}\psi$.

- Both steps are visible. Since $\delta \lhd m$, $\textsc{vl}(\pi D_{cliff}\psi) = \textsc{vl}(\pi D'_{convc}\psi) \cup \{n\}$ and we are done.

- In the other two cases (the step labelled m is visible while the one labelled n is hidden, or both are hidden), we first show that $\textsc{vl}(\pi D_{cliff}\psi) = \textsc{vl}(\pi D'_{convc}\psi)$, and then compare the shadows associated with the corresponding visible steps. For the pairs (resp., two-element multisets) associated with visible S-steps (resp., E-steps) from π and ψ, we use the induction hypothesis. And for the step m, when visible, the associated pairs are of the form $\langle \leftrightarrow^n_E \circ \psi, \pi\rangle$ and $\langle \psi, \pi \circ \twoheadleftarrow\!\!\twoheadrightarrow^{\delta}_{S\cup E}\rangle$. We conclude thanks to Lemma 3.1.13. □

Lemma 3.1.17. $\pi D_{\mathit{cliff}} \psi \succ\!\succ \pi D_{\mathit{convc}} \psi$.

Proof. By Lemmas 3.1.16, 3.1.12 and transitivity. □

Using Lemmas 3.1.15 and 3.1.17, we now get:

Corollary 3.1.18 (Decreasing Diagrams Modulo)**.** *Given a labelled rewrite system $\langle S, E \rangle$, rewriting modulo is Church-Rosser modulo E if all local peaks and cliffs have decreasing diagrams.*

Decreasing diagrams for cliffs have also already been considered by Ohlebusch [Ohl98] and by Aoto and Toyama [AT12]. Ohlebusch's diagram is indeed a particular (incomplete) instance of ours. Aoto and Toyama allow arbitrary labels for equality steps, but forbid facing steps in the diagrams for cliffs. Capturing their result requires allowing arbitrary labels for equality steps, and modifying the notion of visibility as expected. The monotonic order proposed in [FvO13] is able to capture [AT12], but it is open whether the idea of visibility could work.

3.2 Cofinal Derivations and Streams

Van Oostrom showed the following completeness result: every confluent rewrite relation on a countable set can be labelled in such a way that every peak enjoys a decreasing diagram. The major insight is the use of Klop's notion of cofinal derivation [Klo80], which we recall before generalizing to the modulo case.

In this section, we shall use sets indexed by any non-zero ordinal $\alpha \leq \omega$, the first limit ordinal. We will write $i \in \alpha \leq \omega$ for $i \in \alpha$ and $\alpha \leq \omega$.

3.2.1 Cofinal Derivations

When every object has a unique normal form for a given rewrite relation, all objects in a convertibility class reduce to that normal form. This property is stronger than confluence: β-reduction in λ-calculus is an example of a confluent relation for which some objects have no normal form. It however enjoys an interesting property: objects in an equivalence class can be rewritten to objects in a sequence converging towards some kind of limit, hence this sequence can be regarded as a sort of "normal form" for the class, in the sense that it forms a complete set of witnesses for joinability.

Definition 3.2.1. Given a rewrite relation $\rightarrow$ on a non-empty set $\mathcal{O}$, a *cofinal derivation* is a non-empty α-indexed subset $D = \{s_i\}_{i \in \alpha}$ of $\mathcal{O}$ such that

(i) for all $i \in \alpha \setminus \{0\}$, $s_{i-1} \rightarrow s_i$;

(ii) every object $s \in \mathcal{O}$ reaches some element in D.

Being a set, the sequence $\{s_i\}_i$ is cycle-free: $\forall i \neq j,\ s_i \neq s_j$. A cofinal derivation D is indeed viewed as a sub-relation of $\rightarrow$ restricted to the set D, and containing no more than the pairs of condition (i) : the rewrite steps $s_i \rightarrow s_j$ belong to the cofinal derivation if and only if $j = i + 1$.

Note also that chopping off an initial segment from a cofinal derivation yields another cofinal derivation. In particular, if a cofinal derivation is finite, then its last element is itself cofinal (hence is a normal form in the usual sense unless it is part of a cycle for $\rightarrow$).

Theorem 3.2.2 ([Klo80])**.** *A rewrite relation on a countable set is confluent if and only if every convertibility class has a cofinal derivation.*

It actually suffices that each convertibility class is countable, but we shall use the simpler assumption that the underlying set itself is. Let us mention that Klop gave a counter-example showing the necessity of the cardinality assumption.

3.2.2 Cofinal Streams

We could think of reusing the same notion of cofinal derivation for a rewrite system $\langle S, E\rangle$, but it would then contain E-steps as well as S-steps. Instead, we build derivations in which the E-steps are crowded together after the S-steps.

Definition 3.2.3. A derivation $u \twoheadrightarrow_{S \cup E} v$ is said to be *cycle-free* if it does not contain a (necessarily non-empty) sub-derivation $s\,(\twoheadrightarrow_{S \cup E} \setminus \twoheadleftarrow\!\!\twoheadrightarrow_E)\,t$ such that $\overline{s} = \overline{t}$.

Definition 3.2.4. Given a rewrite system $\langle S, E \rangle$ on a non-empty set $\mathcal{O}$, a *cofinal* E*-stream* (*cofinal stream* for short) is a non-empty α-indexed set of E-convertibility classes $\{\overline{s_i}\}_{i \in \alpha}$ of *representative* s_i, of *support* $D = \bigcup_{i \in \alpha} \overline{s_i}$, such that

(i) for all $i \in \alpha \setminus \{0\}$ and $s \in \overline{s_{i-1}}$, there exists $t \in \overline{s_i}$ such that $s \to_S t$;

(ii) every object $s \in \mathcal{O}$ reaches some element in D by S-steps only.

Note that a cofinal stream being a set, $(\forall i \neq j)\ \overline{s_i} \neq \overline{s_j}$ (cycle-freeness). As before, rewrite steps between non-consecutive classes do not belong to the stream (viewed as a sub-rewrite system of $\langle S, E \rangle$ on its support), including those between elements of a same E-class: only the S-steps defined in (i) and the E-steps in each convertibility class $\overline{s_i}$ belong to the stream. Building cofinal streams will require a compatibility property between S-steps and E-steps:

Definition 3.2.5. A rewrite system $\langle S, E \rangle$ is *strongly-coherent*, if for all u, v, w such that $u \leftrightarrow_E v \to_S w$ and $\overline{v} \neq \overline{w}$, there exists t such that $u \to_S t$ and $t \twoheadleftarrow\!\!\twoheadrightarrow_E w$ (note that $\overline{t} \neq \overline{u}$).

The notion of strong coherence is a particular case of the notion of E*-commuting relations* $>$ *with a rewrite relation* S used by Jouannaud and Muñoz [JM84], by taking S to be the considered relation $>$.

Lemma 3.2.6. *Let $\langle S, E \rangle$ be a strongly-coherent system. Then, any finite sequence d of the form $u \twoheadrightarrow_{S \cup E} v$ can be transformed into another sequence d' of the form $u \twoheadrightarrow_S w \twoheadleftarrow\!\!\twoheadrightarrow_E v$ for some w such that $u \twoheadrightarrow_S w$ is cycle-free, and the number of S-steps in d' is smaller or equal to that in d.*

Proof. By induction on the number n of S-steps in d. If $n = 0$, we are done. Otherwise, cycles are replaced by their corresponding E-convertibility steps, allowing us to conclude by induction hypothesis. If we have a cycle-free sequence $u \twoheadleftarrow\!\!\twoheadrightarrow_E s \to_S t \twoheadrightarrow_{S \cup E} v$, repeated applications of strong coherence yield a sequence $u \rightarrow_S w \twoheadleftarrow\!\!\twoheadrightarrow_E t \twoheadrightarrow_{S\cup E} v$ for some w. We apply the induction hypothesis to $w \twoheadrightarrow_{S\cup E} v$. If new cycles pop up, they are replaced, resulting in a sequence with number n' of S-steps such that $n' < n$. We conclude by induction hypothesis again. □

We can now state and prove our generalization of Klop's theorem:

Theorem 3.2.7. *A strongly-coherent rewrite system $\langle S, E\rangle$ on a countable set is Church-Rosser modulo E if and only if every convertibility class has a cofinal stream.*

Proof. First note that any two objects belonging to the cofinal stream are joinable by rewrites belonging to the stream. The if direction therefore follows from the fact that an arbitrary object reaches some object in the cofinal stream of its convertibility class by definition of a cofinal stream.

We are left with the only if direction of the claim, for which the basic idea is similar to van Oostrom's [vO94b]: construct a sequence with cycles, and then, eliminate the cycles.

The first construction is by induction on the natural number n. Let $\{a_i\}_{i\in\alpha}$ be an enumeration of the (countable) class A. We denote by D_n the support of the sequence $C_n = \{\overline{s_i}\}_{i\leq q_n<\omega}$ constructed at step n, and by A_n the subset of A whose terms can reach D_n by S-steps only. Note that $D_n \subseteq A_n$.

Base case: $n = 0$, $q_0 = 0$, $s_0 = a_0$ and $D_0 = \overline{a_0}$.

Induction case: if $A_n = A$, we are done, otherwise let a be the first element of A not reaching D_n. Since a is convertible to s_{q_n}, by Church-Rosser assumption, there exist $u, v \in A$ such that $s_{q_n} \twoheadrightarrow_S u \twoheadleftarrow\!\!\twoheadrightarrow_E v\ {}_S\!\twoheadleftarrow a$. Assuming the chosen derivation $s_{q_n} \twoheadrightarrow_S u$ has k steps, we write it as $s_{q_n} \rightarrow_S s_{q_n+1} \rightarrow_S \ldots \rightarrow_S s_{q_n+k} = u$. Let $C_{n+1} = \{\overline{s_i}\}_{i\leq q_n} \cup \{\overline{s_{q_n+i}}\}_{1\leq i\leq k}$. It follows that the new sequence is reachable from a subset A_{n+1} of A such that $A_n \subset A_{n+1}$, and satisfies property (ii) of a cofinal stream. By strong coherence assumption, it also satisfies (i). We now have an infinite increasing sequence $\{C_n\}_n$ which limit $C := \bigcup_{j\geq 0} C_j$ satisfies (i) and (ii), with possibly cycles. If the sequence C is finite, then its last element is cofinal. If there is an E-class $\overline{s}$ occurring infinitely often in C, then $\{\overline{s}\}$ is a cofinal stream of A. Otherwise, every E-class in C occurs finitely often. We construct by induction on n an infinite sequence $\{C'_n\}_n$ of increasing, finite sub-sequences of C which limit C' is our cofinal stream.

Let $C'_0 := \{\overline{s_0}\}$, and let us assume by induction hypothesis that $C'_n := \{\overline{s'_j}\}_{j \leq n}$ is cycle-free and satisfies (i,ii). Let j be the largest index such that $\overline{s_j} = \overline{s'_n}$. Then $\overline{s'_{n+1}} = \overline{s_{j+1}}$ and $C'_{n+1} := C'_n \cup \{\overline{s'_{n+1}}\}$. It is easy to see that C'_{n+1} is cycle-free and satisfies properties (i,ii). The limit of this increasing sequence is our cofinal stream. $\square$

We shall now show two consequences of Klop's theorem and its generalization. The first, as shown by van Oostrom, is that the existence of decreasing diagrams is a characterization of completeness. The second is that it yields a new, simple proof of Toyama's modularity theorem. Both results require the countability assumption and scale to rewriting modulo.

3.3 Completeness

We successively consider van Oostrom's result and its generalization.

3.3.1 Plain Rewriting

Van Oostrom remarked in [vO94b, Theorem 3.3.3] that the cofinal derivation in a convertibility class allows to define a notion of distance from a term to the cofinal derivation seen as a normal form for the elements in the convertibility class:

Definition 3.3.1. Given a cofinal derivation $D = \{s_i\}_{i \in \alpha}$ in a convertibility class A, the *distance* $d(a, D)$ of $a \in A$ to D is defined as the minimum number of S-steps to reach an element of D from a.

Definition 3.3.2. Given a confluent relation $\rightarrow$, a cofinal derivation D_a for the convertibility class of the element a, and two objects s, t in the convertibility class of a such that $s \rightarrow t$, we call *canonical labelling* of $s \rightarrow t$

the natural number 1 if $s \to t$ belongs to D_a, and the natural number $d(t, D) + 2$ otherwise.

The numbers 2 instead of 1 (for steps hitting D_a but not in D_a) and 1 instead of 0 (for steps in D_a) are non-important here, but will help with the modulo case. As noted in [vO08a], we can prove that:

Theorem 3.3.3. *Given a confluent relation $\to$ on a countable set, equipped with a canonical labelling, all its local peaks enjoy decreasing diagrams.*

3.3.2 Strongly-Coherent Rewriting Modulo

We may now think of applying van Oostrom's completeness result to an arbitrary labelled rewrite system $\langle S, E\rangle$. This does not work, however: to conclude the Church-Rosser property from the existence of a cofinal derivation, we would need that the shortest path from an element of the convertibility class to the cofinal derivation contains S-steps only, which is not true in general. We shall therefore restrict our attention to strongly-coherent systems, and use cofinal streams.

We define the distance of an object to the cofinal stream of its convertibility class to be the minimum number of S-steps to reach an element of its support. The canonical labelling of S-steps is then kept unchanged, and the canonical labelling of E-steps is taken to be 0. We then get:

Theorem 3.3.4. *Given a strongly-coherent, Church-Rosser system $\langle S, E\rangle$ on a countable set equipped with a canonical labelling, all its local peaks and cliffs enjoy decreasing diagrams.*

Proof. By Theorem 3.2.7, every convertibility class has a cycle-free cofinal stream. Given a convertibility class, its cycle-free cofinal stream $\{\overline{s_i}\}_{i\in\alpha}$ and the support D, we consider all local peaks and cliffs $u \;{}_{S\cup E}\!\overset{m}{\leftarrow}\; s \to^{n}_{S\cup E} v$. There are several cases:

1. $m = n = 0$, hence $s \to u$ and $s \to v$ are both E-steps, then we are done with the conversion $u \leftrightarrow^{0}_{E} s \leftrightarrow^{0}_{E} v$.

2. $m = 0, n = 1$. Then $s \leftrightarrow u$ is an E-step and $s \to v$ is an S-step. According to the definition of a cofinal stream, there exists $t \in \overline{v}$ such that $u \to_S^1 t$. The derivation $u \to_S^1 t \twoheadleftarrow\!\!\twoheadrightarrow_E^0 v$ satisfies the decreasing diagram property.

3. $m = 0, n \geq 2$, hence $s \leftrightarrow u$ is an E-step and $s \to v$ is an S-step which does not belong to $\{\overline{s_i}\}_{i \in \alpha}$. If v is E-convertible to s, then it is E-convertible to u, resulting in a decreasing diagram. Otherwise, by strong coherence assumption, there exists $t \in \overline{v}$ such that $u \to_S^{n'} t$. We get the decreasing diagram $u \to_S^{n'} t \twoheadleftarrow\!\!\twoheadrightarrow_E^0 v$ by showing $n' \leq n$. Note that $n' \neq 1$, otherwise n would be 1 as well. Consider the shortest derivation from v to D. By Lemma 3.2.6, $d(t, D) \leq d(v, D)$, and similarly $d(v, D) \leq d(t, D)$. Therefore $n' = n$ and we are done.

4. $m = n = 1$, hence $s \to u$ and $s \to v$ are both S-steps belonging to $\{\overline{s_i}\}_{i \in \alpha}$ and u, v are in the same E-class, resulting in a decreasing diagram again.

5. $m \geq 1, n \geq 2$, hence both are S-steps. Taking the shortest (possibly empty if $m = 1$) derivations to D from both extremities and joining these derivations in $\{\overline{s_i}\}_{i \in \alpha}$ yields a conversion which all steps have labels smaller or equal to $max(m, n) - 1$, which concludes the proof. □

3.3.3 Need for Strong Coherence

One may wonder whether strong coherence is a necessary requirement for the above theorem, and the notion of decreasing diagram for cliffs is general enough.

It is possible to relax the definition of a cofinal stream, and replace condition (i) by (i'): any two elements $s \in \overline{s_i}$ and $t \in \overline{s_j}$ are E-joinable *below*, that is, at some E-convertibility class $\overline{s_k}$ with $k \geq i$ and $k \geq j$. Assuming the rewrite system $\langle S, E \rangle$ is Church-Rosser modulo E, then such cofinal streams can be obtained with a slightly more involved construction. The problem is that we were not able to prove completeness of decreasing diagrams under condition (i'), even when allowing arbitrary labels for the E-steps.

Indeed, we give at Figure 3.1 an example of Church-Rosser rewrite system $\langle S, E\rangle$ which shows the incompleteness of a relaxed decreasing diagrams condition for cliffs, but leaves the question of completeness open for a more general notion. We conjecture that a general definition of decreasing diagrams for a cliff ${}_{S}^{m}\!\!\leftarrow \circ \leftrightarrow_{E}^{n}$ is obtained by taking $D_{convc} := \twoheadleftarrow\!\!\twoheadrightarrow_{S\cup E}^{\alpha} \circ \Leftrightarrow_{E}^{n} \circ \twoheadleftarrow\!\!\twoheadrightarrow_{S\cup E}^{\delta} \circ {}_{S}^{m}\!\!\leftarrow \circ \twoheadleftarrow\!\!\twoheadrightarrow_{S\cup E}^{\beta}$, with labels in β strictly smaller than n, and labels in α, δ strictly smaller than m or n, where $\Leftrightarrow_{E}^{n}$ denotes the reflexive closure of $\leftrightarrow_{E}^{n}$. We only assume here that facing steps (of the rewrite step or the equality step) belong to the same category. We restrict here this general notion of decreasing diagram by assuming that (i) all E-steps have the same label, or (ii) the labels of the E-steps are not bigger than the labels of the S-steps. Since both these restrictions capture our previous definition of decreasing diagrams for cliffs, we shall refer to them as the *relaxed labelling schema.*

Lemma 3.3.5. *There is no labelling ensuring that every cliff of Figure 3.1 (a) has a decreasing diagram satisfying the relaxed labelling schema.*

Proof. We reason by contradiction, assuming that all cliffs have decreasing diagrams. We then show that $(\forall i \geq 1)(\exists j \geq 1)\, l_i \rhd l_j$. This implies that the order on labels cannot be well-founded, resulting in a contradiction.

Let us consider all possible cycle-free conversions for the cliff $u\ {}_{S}^{l_i}\!\!\leftarrow s \leftrightarrow_{E}^{m_i} v$, since eliminating a cycle from the conversion of a decreasing diagram yields a decreasing diagram with a conversion of a reduced length. Let max and min be respectively the largest and the smallest indexes of the E-steps occurring in such a conversion. There are two cases only depicted at Figure 3.1, the cliff $u\ {}_{S}^{l_i}\!\!\leftarrow s \leftrightarrow_{E}^{m_i} v$ being labelled in black for facilitating its localization:

1. $min < i$, named (b) on Figure 3.1, with rewrite steps going opposite directions from $\leftrightarrow^{m_{min}}$. We then let $j = min$ (max is not needed here, which has allowed us to shorten the figure by taking $max = i + 1$).

2. $min = i$, named (c) on Figure 3.1, with rewrite steps going opposite directions from $\leftrightarrow^{m_{max}}$. We then let $j = max - 1$.

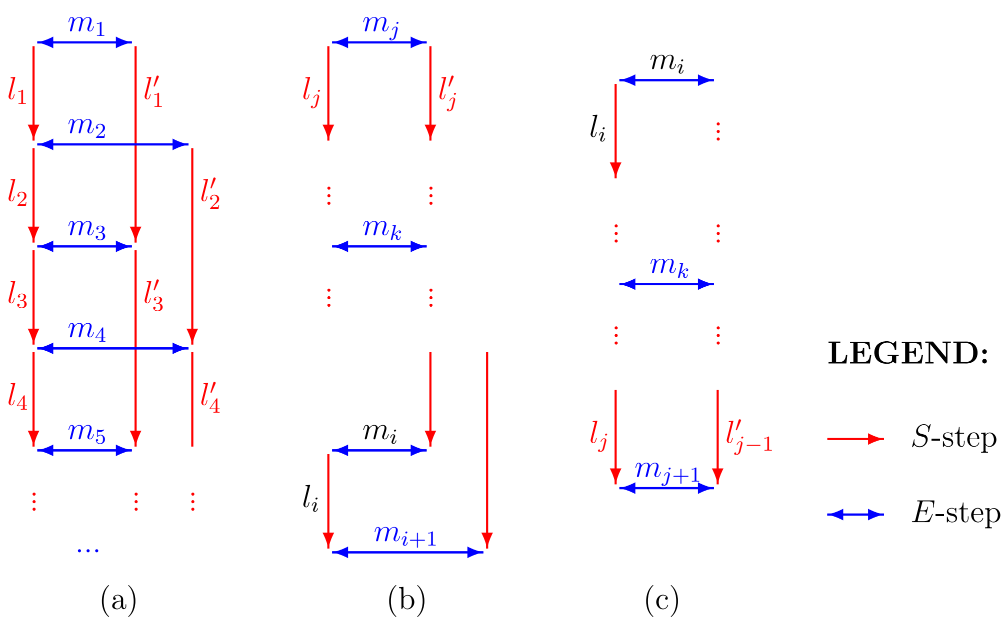


Figure 3.1: A Non-Strongly-Coherent Church-Rosser Rewrite System

In both cases, we show that the step $\to_S^{l_j}$ cannot be facing the step $\to_S^{l_i}$. We carry out the proof for case (b) only, using either assumption (i): $(\forall i \geq 1)\, m_i = m$, or (ii): $(\forall i, j \geq 1)\, m_i \ntriangleright l_j$. There are two cases:

1. The conversion has the form $u \twoheadleftrightarrow_{S\cup E} \circ {}_S^{l'_j}\!\!\leftarrow \circ \leftrightarrow_E^{m_j} \circ \to_S^{l_j} \circ \twoheadleftrightarrow_{S\cup E} \circ \leftrightarrow_E^{m_k} \circ \twoheadleftrightarrow_{S\cup E} v$. Going the wrong direction, $\to_S^{l_j}$ cannot be the facing step, thus either $l_i \triangleright l_j$ and we are done, or $m_i \triangleright l_j$ which contradicts assumption (ii). With (i), $m_k = m$ and l_j must be smaller than either l_i or $m_i = m$, hence $l_i \triangleright m$ implying $l_i \triangleright l_j$.

2. The conversion has the form $u \twoheadleftrightarrow_{S\cup E} \circ {}_S^{l_j}\!\!\leftarrow \circ \leftrightarrow_E^{m_j} \circ \to_S^{l'_j} \circ \twoheadleftrightarrow_{S\cup E} v$. Since $m_j = m = m_i$ with assumption (i), or $m_i \ntriangleright l'_j$ with assumption (ii), ${}_S^{l_j}\!\!\leftarrow$ cannot be the facing step, and the reasoning proceeds as previously.

It is then easy to build an infinite decreasing sequence of labels, a contradiction. $\square$

Our lemma implies that strong coherence is a necessary condition for completeness not only when labelling equality steps with a minimum (extra) label, but even for the relaxed labelling schema. Aoto and Toyama use a different restriction of the general decreasing diagram condition by forbidding facing steps [AT12]. Whether this other restriction is complete is also open: the rewrite system of Figure 3.1 (a) does not allow to show incompleteness for their notion.

Finding a notion of decreasing diagrams for cliffs which characterizes confluence is therefore still open.

3.4 Modularity

We give here a new, simpler proof of Toyama's modularity theorem under the countability assumption, based on cofinal derivations.

3.4.1 Plain Term Rewriting

Basic notions of term rewriting have been introduced in Chapter 2. We assume in this section that the set $\mathcal{F}$ of signature and the set $\mathcal{X}$ of variables are both countable.

Note that the term rewrite systems introduced in Chapter 2 are also called *plain* term rewrite systems, since they use *(plain)* pattern matching for firing rules. Note also that in Definition 2.3.1 we impose the condition $\mathcal{V}ar(r) \subseteq \mathcal{V}ar(l)$ for all rewrite rules $l \to r$, thus term rewriting is *variable non-increasing*, that is, $\mathcal{V}ar(t) \subseteq \mathcal{V}ar(s)$ if $s \to t$ for terms s, t. Examples are given in [JT08] showing that rules which do not satisfy the above property on variables do not, in general, define a non-trivial confluent rewrite relation.

An *equation* is a pair of terms written $l = r$. Unlike rules, equations are not directed. We use $\leftrightarrow_E$ for rewriting with a set E of equations. An equation $u = v$ is *linear* if both u, v are linear, *regular* if $\mathcal{V}ar(u) = \mathcal{V}ar(v)$, and *collapsing* if u or v is a variable.

Given a set of equations (or rules), the associated convertibility classes are of course countable sets as subsets of a countable set.

3.4.2 Plain Modularity

In this section, S, T denote two confluent plain rewrite systems built from disjoint signatures $\mathcal{G}$ and $\mathcal{H}$. It is important to note that two different variables cannot be convertible (in S or T) since they are in normal form by our definition of a rule. We denote by $\mathcal{T}(\mathcal{G} \cup \mathcal{H}, \mathcal{X})$ the set of terms built on the union signature $\mathcal{G} \cup \mathcal{H}$ and the set of variables $\mathcal{X}$. Terms are called *homogeneous* when they belong to $\mathcal{T}(\mathcal{G}, \mathcal{X}) \cup \mathcal{T}(\mathcal{H}, \mathcal{X})$, *heterogeneous* when they belong to $\mathcal{T}(\mathcal{G} \cup \mathcal{H}, \mathcal{X}) \setminus (\mathcal{T}(\mathcal{G}, \mathcal{X}) \cup \mathcal{T}(\mathcal{H}, \mathcal{X}))$.

Definition 3.4.1. The *cap* $\hat{s}$ of a term $s \in \mathcal{T}(\mathcal{G} \cup \mathcal{H}, \mathcal{X})$ is the largest homogeneous term with respect to subsumption such that $s = \hat{s}\sigma$ for some *alien substitution* σ, while $A_s = \{\sigma(x) \mid x \in \mathcal{D}om(\sigma) = \mathcal{V}ar(\hat{s}) \setminus \mathcal{V}ar(s)\}$ is its set of *aliens*.

The *rank* of a term $s = \hat{s}\sigma$ is equal to $1 + max(\{\text{rank}(u) \mid u \in A_s\})$, where $max(\varnothing) = 0$.

A homogeneous term s is *compact* if and only if it is a variable, or it is not convertible to a variable and $\mathcal{V}ar(s) \subseteq \mathcal{V}ar(t)$ for any term t convertible to s. A heterogeneous term is *compact* if and only if its cap and aliens are compact, and any two convertible aliens are equal. A substitution is *compact* if it maps variables to compact terms.

Example 3.4.2. Take $\mathcal{G} = \{a, b, c, f^2\}$, $\mathcal{H} = \{g^3\}$, $S = \{a \to b\}$, and $T = \varnothing$. Then $g(g(x, a, b), a, b)$ has cap $g(g(x, y, z), y, z)$ and alien substitution $\{y \mapsto a,\ z \mapsto b\}$. The homogeneous term $f(b, b)$ is compact. Similarly, $g(a, a, a)$ is a compact heterogeneous term, while $g(b, a, b)$ is not. If $T = \{g(x, y, x) \to y\}$, then neither one is compact, but a is a compact term reachable from both. In both cases, $g(c, b, b)$ is a compact heterogeneous term.

The definition of cap ensures three important properties: (i) it is the identity for homogeneous terms; (ii) the cap of a heterogeneous term is not a variable; and (iii) any rewrite in the cap of a heterogeneous term can be lifted to a rewrite in its homogeneous cap. The idea of slicing terms into a homogeneous cap and an alien substitution was already used by

Shostak [Sho82]. To our knowledge, the particular definition used here originates from [JO91].

Compact terms are exactly the *stable equalizers* introduced in [JT08], defined there as being both stable and equalizers. The above more abstract definition is new, and allows us to dispense with many technicalities of collapsing and erasing rules present in [JT08]. It is important noting that the cap of a compact heterogeneous term cannot be a variable (by definition of cap), hence cannot be convertible to a variable since otherwise it would not be compact as a homogeneous term. Note also that variables are compact and reachable from any homogeneous convertible term under our assumption that S and T are confluent, since they are in normal form.

Lemma 3.4.3. *Given a homogeneous term $s \in \mathcal{T}(\mathcal{G}, \mathcal{X})$ (resp., $\mathcal{T}(\mathcal{H}, \mathcal{X})$), the cofinal derivation of its S- (resp., T-) convertibility class can be assumed to contain compact terms only.*

Proof. If s is convertible to a variable x, then $\{x\}$ is a cofinal derivation satisfying the claim. Otherwise, if $\{u_i\}_i$ is a cofinal derivation for its convertibility class, then $\mathcal{V}ar(u_{i+1}) \subseteq \mathcal{V}ar(u_i)$ by definition of a rewrite rule and property (i) of a cofinal derivation (Definition 3.2.1). Chopping off an initial segment of a cofinal derivation yields a new cofinal derivation whose all terms have the same minimum set X of variables. By property (ii) of a cofinal derivation, $X \subseteq \mathcal{V}ar(s)$ for all s in the class, hence u_i is compact. □

In the sequel, we associate to each convertibility class of homogeneous terms a *canonical* cofinal derivation made of compact terms only.

We now recall a handy technical tool: a confluent plain rewrite system for $S \cup T$. By an appropriate use of ordered completion [HR87], any plain rewrite system S can be transformed into a possibly infinite plain rewrite system S^∞ defining the same convertibility relation, such that ordered rewriting is confluent and terminating, variable non-increasing and variables are in normal form for S^∞. See [Jou06, JT08] for the definition of ordered rewriting and the detailed (easy) construction of S^∞. Let S^∞ and T^∞ be so obtained from S, T. Since $\mathcal{G} \cap \mathcal{H} = \varnothing$, $S^\infty \cup T^\infty$ is the confluent plain rewrite system obtained from $S \cup T$ by the same construction. We denote by $s{\downarrow}$ the normal form of s with respect to $S^\infty \cup T^\infty$ (for S^∞ or T^∞ for homogeneous terms).

Lemma 3.4.4. *Assume that $s = \hat{s}\sigma$ and $t = \hat{t}\tau$ are two different convertible compact terms. Then, s, t have the same rank, $\hat{s}$ and $\hat{t}$ are convertible homogeneous terms (up to some variable renaming) such that $\mathcal{V}ar(\hat{s}) = \mathcal{V}ar(\hat{t})$, and for all $x \in \mathcal{D}om(\sigma) = \mathcal{D}om(\tau)$, $\sigma(x)$ and $\tau(x)$ are convertible terms.*

Proof. Similar to that of [JT08]. Note that s and t cannot be variables, since variables are in normal form for $S^\infty \cup T^\infty$, hence two different variables cannot be convertible.

We prove by induction on the rank the following *Claim*: normal forms of different convertible compact terms are compact terms of the same rank. Since $\mathcal{G} \cap \mathcal{H} = \varnothing$, then $(\hat{s}\sigma){\downarrow} = (\hat{s}{\downarrow})\sigma{\downarrow}$, and therefore $\hat{s}$ and $\hat{s}{\downarrow}$ are convertible. Since $\hat{s}$ is compact and rewriting is variable non-increasing, $\mathcal{V}ar(\hat{s}) = \mathcal{V}ar(\hat{s}{\downarrow})$, hence $\hat{s}{\downarrow}$ is a compact homogeneous term. By induction hypothesis, $\sigma{\downarrow}$ is a compact substitution, and since $S^\infty \cup T^\infty$ is confluent, $\sigma(x){\downarrow} = \sigma(y){\downarrow}$ iff $\sigma(x) = \sigma(y)$ iff $x = y$ for any $x, y \in \mathcal{D}om(\sigma)$, hence $(\hat{s}{\downarrow})\sigma{\downarrow}$ is a compact term of the same rank.

We now normalize s, t with $S^\infty \cup T^\infty$, yielding two equal normal compact terms $(\hat{s}{\downarrow})\sigma{\downarrow}$ and $(\hat{t}{\downarrow})\tau{\downarrow}$ by confluence of $S^\infty \cup T^\infty$. The result follows. $\square$

We now prove Toyama's theorem by lifting cofinal derivations of classes of homogeneous terms to classes of heterogeneous terms. Remember that the signature $\mathcal{F}$ and the set $\mathcal{X}$ of variables are assumed to be countable sets, in order to have a countable term algebra $\mathcal{T}(\mathcal{F}, \mathcal{X})$ and apply Klop's theorem.

Theorem 3.4.5 ([Toy87]). *$S \cup T$ is confluent if and only if S and T are both confluent.*

Proof. The only if part of the proof of Toyama's theorem is straightforward. For the if case, we build a cofinal derivation for every $(S \cup T)$-convertibility class and apply Theorem 3.2.2.

Not all heterogeneous terms in an infinite cofinal derivation can be compact, since two equal aliens may need to be rewritten one after the other along the derivation, hence become temporarily unequal. We shall however construct (eventually cofinal) *dense* derivations on heterogeneous terms: any term in the derivation reaches a compact term further in the sequence.

We now prove by induction on the rank of terms the following properties:

(i) every term reaches a compact term in its convertibility class;

(ii) every compact term reaches a dense derivation in its convertibility class;

(iii) any two convertible compact terms define the same dense derivation.

Proof of (i). Let $u = \hat{u}\sigma$ be a term of rank k. For any $x \in \mathcal{D}om(\sigma)$, $\sigma(x)$ has rank at most $k-1$. By induction hypothesis (i), $\sigma(x)$ reduces to a compact term $\tau(x)$ in its convertibility class. Hence u reduces to $v = \hat{u}\tau = \hat{v}\theta$, where $\theta(y)$, for $y \in \mathcal{D}om(\theta)$ is either some $\tau(y)$ or one of its aliens. Hence $\theta(y)$ is compact and has rank at most $k-1$. We now reduce θ to θ' so that $\theta'(x) = \theta'(y)$ iff $\theta(x)$ and $\theta(y)$ are convertible, by induction hypothesis (ii,iii). Hence v reduces to $v' = \hat{v'}\theta'$. If $\hat{v'}$ is convertible to a variable, then v' reduces to the variable or one of its aliens, which are both compact. Otherwise, $\hat{v'}$ reaches a compact term w on its canonical cofinal derivation, and v' reaches the compact term $w\theta'$. Hence u reduces to a compact term.

Proof of (ii). Let $u = \hat{u}\sigma$ be a compact term of rank k, and $\mathcal{D}om(\sigma) = \{x_1, \ldots, x_n\}$. By induction hypothesis (ii,iii), for $x_j \in \mathcal{D}om(\sigma)$, the class of $\sigma(x_j)$ has a dense derivation $\{s_i^j\}_i$ hence $\sigma(x_j)$ reaches some $s_{i_j}^j$. By confluence assumption and Theorem 3.2.2, $\hat{u}$ reaches $s_{i_0}^0$ on a canonical cofinal derivation $\{s_i^0\}_i$, where all terms are compact by Lemma 3.4.3. We define $\{A_i := s_i^0\{x_j \mapsto s_i^j\}_j\}_i$ to be the dense derivation (possibly adding intermediate terms) for the class of u. Let $m = max(\{i_j\}_{j\in[0..n]})$. Then u reaches A_m.

Proof of (iii). Let $u = \hat{u}\sigma$ and $v = \hat{v}\tau$ be different convertible compact terms. By Lemma 3.4.4, u, v have the same rank k, $\hat{u}$ and $\hat{v}$ are convertible homogeneous terms (up to some variable renaming), and $\sigma(x)$ and $\tau(x)$ are convertible compact terms of rank at most $k-1$ for all $x \in \mathcal{D}om(\sigma) =$

$\mathcal{D}om(\tau)$. By induction hypothesis (iii), $\sigma(x)$ and $\tau(x)$ define the same dense derivation. By assumption, the cofinal derivations chosen for $\hat{u}$ and $\hat{v}$ are the same, since the canonical one. Therefore, the dense derivations constructed in (ii) are the same for u and v.

Properties (i-iii) imply that the dense derivations so constructed are cofinal. □

We believe that this proof is the simplest proof so far of Toyama's theorem and can hardly be improved. Compared to [JT08], the use of cofinal derivations provides the right argument for reachability of compact terms.

3.4.3 Term Rewriting Modulo Equations

Rewriting is based on orienting equality steps, but this does not always make clear sense. For example, the two sides of the commutativity axiom $x + y = y + x$ cannot be distinguished by their structure. Although it is however possible to distinguish their instances by using a well-founded order as an oracle [HR87, HR91].

There is a zoo of relations for rewriting modulo equations on terms, and we are going to abstract them away by characterizing some properties they satisfy. We assume given a set of rules R and a set of equations E. These rewrite relations differ in the way rewriting is defined, we consider only two of them here:

Class rewriting is defined as $s \to_{R/E} t$ if and only if there exist u, v such that $u \twoheadleftarrow\!\!\twoheadrightarrow_E s$, $v \twoheadleftarrow\!\!\twoheadrightarrow_E t$ and $u \to_R v$ [LB77].

Rewriting modulo is defined as $s \to^{p}_{R_E} t$ if and only if there exists u such that $u \twoheadleftarrow\!\!\twoheadrightarrow^{\geq \mathcal{P}p}_{E} s$ and $u \to^{p}_{R} t$ [PS81].

Class rewriting has a very strong property, namely that if a term s rewrites to a term t, then every term in the class of s rewrites (with class rewriting) to every term in the class of t. This property is buried in the definition, and has an important drawback: to know whether a term s is rewritable by class rewriting, we need to search its E-convertibility class in order to find a term u which is plain-rewritable. This may be undecidable, and at least very inefficient in practice.

Rewriting modulo answers this concern of making search efficient by using E-pattern matching. We therefore need to assume its decidability.

Peterson and Stickel remarked that whenever a set of rules is *closed under extensions*, then terms in an equivalence class are either all in normal form or all rewritable by rewriting modulo [PS81]. Extensions were indeed defined for associativity and commutativity and later extended to arbitrary equations [JK86]. Closing a set of rules under extensions requires unifiability modulo E to be decidable. This is the case for standard theories such as commutativity (C), or associativity and commutativity (AC). It is not hard to show that if the equations in E are linear and the rules in R are closed under extensions, then rewriting modulo is strongly-coherent as well. We make the assumptions explicit in the next section.

3.4.4 Modularity Modulo

We are now going to extend our proof of modularity to term rewrite systems $\langle S, E\rangle$ for which the rewrite relation $\rightarrow_S$ satisfies the strong coherence property with respect to E-convertibility. The modularity result of this section therefore applies to rewriting modulo, but also to class rewriting with the very same proof. On the other hand, the assumptions that the pair (R, E) of rules and equations need to satisfy are very different: no assumption is necessary for class rewriting to be strongly-coherent, while for rewriting modulo, strong coherence requires the equations in E to be both linear *and* regular, implying together that all variables of an equation occur exactly once on both sides of the equation. Further, it is also implicitly required in the latter case that unification modulo E is decidable, in order to be able to close effectively the set of rules under extensions. Regularity of the equations in E is required for class rewriting as well, since we shall need the property that any two E-convertible terms have the same set of variables. Equations in E are further assumed to be non-collapsing to simplify the proofs. We conjecture that this non-collapsingness assumption can be removed, but it is still open to check.

From now on, we do not need the rules in R to be mentioned anymore, all results can be stated and their proofs carried out abstractly with the relation $\rightarrow_S$.

We assume therefore given two strongly-coherent rewrite systems $\langle S, E\rangle$ and $\langle T, F\rangle$ built on the respective countable signatures $\mathcal{G}$ and $\mathcal{H}$, such that $\mathcal{G} \cap \mathcal{H} = \varnothing$ and equations in $E \cup F$ are regular and non-collapsing.

We keep the notions *homogeneous*, *heterogeneous*, *cap*, *alien*, *rank*, *compact* the same as in Section 3.4.2, except that we use $(S \cup E)$-*convertibility* instead of *convertibility* in the definitions. And we denote $S \cup E \cup T \cup F$ by U for convenience.

Now we modify Lemma 3.4.3 to fit with the modulo case:

Lemma 3.4.6. *Given some homogeneous term $s \in \mathcal{T}(\mathcal{G}, \mathcal{X})$, the cofinal stream of its $(S \cup E)$-convertibility class can be assumed to contain compact terms only.*

Proof. Same proof as for Lemma 3.4.3, using in addition the fact that E-convertible terms have the same set of variables by our regularity assumption. □

We are now ready for stating and proving the modularity of rewriting modulo:

Theorem 3.4.7 (Modularity Modulo [JT08])**.** *Assume that $\langle S, E\rangle$ and $\langle T, F\rangle$ are strongly-coherent rewrite systems. Then $\langle S \cup T, E \cup F\rangle$ is confluent modulo $E \cup F$ if and only if $\langle S, E\rangle$ and $\langle T, F\rangle$ are confluent modulo E and F, respectively.*

Proof. The proof is the same as the proof for Theorem 3.4.5 except that:

1. Instead of constructing dense cofinal derivations for the union system, we construct *dense* cofinal streams: any representative in the stream will reduce to a compact representative further in the sequence of representatives.

2. We use Lemma 3.4.6 instead of Lemma 3.4.3 to find a dense cofinal stream for homogeneous terms.

3. Given a compact term $u = \hat{u}\sigma$, we construct the dense cofinal stream in its U-convertibility class as $\{\overline{A_i} := \overline{s_i^0\{x_j \mapsto s_i^j\}_j}\}_i$, where $\{\overline{s_i^0}\}_i$ is the dense canonical cofinal stream for the U-class of $\hat{u}$ and $\{\overline{s_i^j}\}_i$ is the dense cofinal stream for the U-class of $\sigma(x_j)$ for any $x_j \in \mathcal{D}om(\hat{u})$.

4. Instead of proving all terms can reach (with S-steps) the dense cofinal derivations of their classes as in the plain case, we prove that each term originates a U-derivation hitting some compact representative in the dense cofinal stream of its U-class.

5. When proving the uniqueness of the constructed dense stream, we apply Lemma 3.4.4 by using $S \cup E$ and $T \cup F$ instead of S, T, respectively.

6. In the end, a last use of Lemma 3.2.6 is needed to show that the constructed dense streams are indeed cofinal. $\square$

Strong coherence and confluence modulo together imply the Church-Rosser property modulo [JK86], hence the result could be stated as a modularity of the Church-Rosser property modulo under our assumptions (strongly-coherent systems and countable signatures).

3.5 Conclusion

This chapter investigates a key property of rewrite relations, the Church-Rosser property, from three different points of view: via decreasing diagrams, via cofinal derivations, and via Toyama's famous modularity theorem.

Van Oostrom's decreasing diagrams characterize a constructive version of confluence. We give an alternative proof of this fundamental result, and extend it to rewriting modulo by defining a simple well-founded partial order that contains diagram rewriting.

He also showed a surprising important completeness property based on Klop's notion of cofinal derivation: any confluent relation can be labelled such that it enjoys decreasing diagrams. In case of rewriting modulo, cofinal stream, a generalization of cofinal derivation to the modulo case, allows us to generalize the completeness result to that case.

Finally, we give a new, simple proof of Toyama's modularity result based on the use of cofinal derivations, and of cofinal streams in the modulo case.

Our generalization of cofinal derivations assumes a property, strong coherence, which can always be satisfied by a rewrite system modulo, to the price of possibly having infinitely many rules (finiteness is preserved in many practical cases such as C and AC). This restriction is reflected in our diagrams by having the same minimum label for the equations, a label which cannot be used by the rules. While this labelling restriction fits well with the strong coherence assumption, we believe that removing it might lead to a more general modularity result in the modulo case, as in [JT08]. We give two examples that show the need for relaxing the labelling of equality steps, but have failed formulating a notion of decreasing diagrams for cliffs that would both preserve completeness and dispense with strong coherence.

Labelling term rewrite relations so as to obtain decreasing diagrams is hard. Indeed, one would like the labels to form an $\mathcal{F}$-algebra with respect to the signature $\mathcal{F}$ of the rewrite system in order to be able to lift the labels from the rule instances to the whole rewrite relation, and possibly reduce confluence to critical pair computations in the case of non-terminating rewrite systems. We exhibit more efforts in this direction in the coming chapters.

Four

Decreasing Diagrams on Abstract Positional Rewriting

Scientific fields undergo successive phases of specialization and unification.

The field of programming languages is in a phase of specialization. Among the main programming paradigms are imperative programming, functional programming, logic programming, object-oriented programming, concurrent programming and distributed programming. Each of these fields is further specialized. For example, there are many different paradigms for functional programming: LISP [McC60], McCarthy's original functional programming paradigm based on pure λ-calculus for lists enriched with recursion; ML [MTH90], Milner's paradigm based on a typed λ-calculus enriched with data types, a let construct and recursion which has become a standard; O'Donnell's paradigm [O'D85] based on orthogonal rewriting; and OBJ [GWM+00], Goguen's paradigm based on terminating rewriting in first-order algebra to cite a few. Similarly, logic programming has given rise to constraint logic programming, as well as query languages for databases.

Bridges have also been built across these programming languages: OCaml is a functional programming language with modules, objects, inheritance, and more [Pot06]. Maude is a functional, rewriting-based, programming language supporting concurrency [Mes11]. Similar to Maude, CafeOBJ [DF98b] supports in addition behavioural descriptions [NKOF08]. Functional, logic and constraint programming coexist in CoqMT [Str10]. Bridges have also been built at the more abstract level of programming paradigms. For one example, Kirchner's rho-calculus is an attempt to unify λ-calculus and rewriting [Kir12]. Meseguer's rewriting logic can be seen as an attempt to unify terminating rewriting with process algebra [Mes00]. Concurrent logic programming is constraint logic programming with concurrent access to a store representing the current state of shared logical facts [Sar90]. Attempts of unifying functional and logic programming are numerous, although not entirely conclusive so far.

In the area of functional programming, we think that a unification phase has started, and our goal in this chapter is to contribute to this trend.

The theory of functional programming languages relies on two major properties of rewriting, its computation mechanism: a syntactic property, confluence that is the target of this thesis, and a semantic property, called type preservation. Since rewriting is usually non-deterministic, the result could depend on particular choices made by the interpreter or compiler. Confluence ensures that rewriting is deterministic, that is, the result does not actually depend upon a particular evaluation path. Type preservation expresses the property that the input and the output have the same functional behaviour. Our goal in this chapter is to unify techniques for checking confluence of a given rewrite relation, independently of the rewriting mechanism itself, and of its termination properties.

Confluence Checking: the Principles

Historically, confluence checking has been influenced by a few foundational works, for terminating rewriting, and for non-terminating rewriting independently.

For the terminating case, Newman's Lemma and Knuth–Bendix's Lemma are the most powerful instruments, without doubt, for confluence checking at the abstract level and the term level, respectively. As for the non-terminating case, Hindley–Rosen's Lemma shows that confluence of an abstract rewrite relation is reducible to its strong confluence, while Tait proved that λ-

calculus is strongly confluent, thus confluent, via parallel rewriting. Driven by the many applications, the terminating branch of rewriting specialized further into rewriting modulo, constraint rewriting, higher-order rewriting and normal rewriting to cite a few. On the other hand, the non-terminating branch kept its unity by generalizing Tait's result to orthogonal rewrite systems, an important class of strongly confluent, term rewrite systems.

In recent years, techniques for proving confluence have been revisited so as to start the unification process.

First, van Oostrom succeeded to capture Newman's and Hindley–Rosen's results using the notion of decreasing diagrams. Second, stated in [JL12a], most existing results belonging to the terminating branch have been unified by Jouannaud and Li under the concept of a *Normal Abstract Rewrite System (NARS)*[1]. There are two main ideas behind NARSes. Rewriting is defined again on an abstract set, but each rewrite step is now decorated by a subset P_p of an abstract set $\mathcal{P}$ of *positions* equipped with a well-founded order $>_{\mathcal{P}}$, p being the minimum of P_p. It is then possible to characterize whether a local peak $u \ {}^{P_p}\!\!\leftarrow s \rightarrow^{Q_q} v$ is a *disjoint peak* ($p\#q$), an *ancestor peak* ($q >_{\mathcal{P}} P_p$), or a *critical peak* ($q \in P_p$) and to reduce confluence of a NARS to the joinability of its abstract critical peaks. The framework of NARSes appears therefore to be intermediate between abstract and concrete rewriting. Second, normal rewriting can specialize to all important concrete rewrite relations that have been introduced in the terminating case, and the associated notions of critical pairs are indeed instances of the abstract ones defined for a NARS.

Weaknesses of Decreasing Diagrams

Van Oostrom showed that the method of decreasing diagrams is complete under the countability assumption, using Klop's notion of cofinal derivations. However, since Klop's notion of cofinal derivation is non-constructive, this result does not tell us how to guess the labelling we need. On the other

[1]However, they only gave in the paper an investigation of applications of NARS to first-order term rewriting and several variants of Nipkow's higher-order normal rewriting [Nip91].

hand, it could give us hints. Unfortunately, this is not the case if we look for a *local* labelling, that is a mapping from rewrite steps to labels. Using the canonical labelling in Definition 3.3.2, consider for example a confluent system made of two distinct convertibility classes C_1 and C_2, the first having a cofinal derivation reduced to a single element a, and the second having an infinite one $\{t_i\}_{i<\omega}$. Let us add the rewrite step $a \to t_{1000}$. Then, the resulting system is still confluent, but the union of both cofinal derivations is not a cofinal derivation. Of course, $\{t_i\}_{i<\omega}$ is a cofinal derivation for the union, but the labels of all steps in C_1 must be increased by 1. $\{a, t_{i\geq 1000}\}$ is another with a similar effect on many steps in C_2. This shows that labelling can hardly be local.

A major strength of decreasing diagrams is that they capture Hindley–Rosen's Lemma as well as Newman's Lemma. To prove it, it suffices to label the rewrite steps by the same label in the first case, and by the origin s of the step $s \to t$ in the second. Doing so, we obtain a *constructive* labelling, rather than using the completeness result itself (which we could do). Of course, *all* known criteria for confluence of abstract relations are covered by van Oostrom's result, as a result of completeness. It however comes as a surprise to us that in each case, a labelling can be built. Assume P is a recursive set of confluent relations. Then, we would like to exhibit a recursive function L_P taking as input a relation $R \in P$ and returning a labelling function for R which satisfies van Oostrom's assumptions. If such a function exists for every P, then we say that the decreasing diagrams method is *constructively complete*. We suspect a negative answer to the open question whether this holds. Indeed, no constructive labelling is known for Huet's generalization [Hue80, Lemma 2.5] of Hindley–Rosen's Lemma.

To overcome this particular weakness, van Oostrom introduced a generalization of decreasing diagrams for local peaks that he calls *commutation diagrams*. The idea is to duplicate the original rewrite relation $\to$ as $\to$ and $\to$. Then any step in a conversion is painted in blue if heading to the left, and in red if heading to the right. We shall prefix all notions by the word *coloured*. The coloured version of van Oostrom's theorem says that coloured confluence (or commutation) follows from the coloured joinability of coloured local peaks. Coloured confluence implies confluence provided the transitive closures of both relations coincide with the transitive closure of the starting relation. Refining Tait's idea for showing confluence of the λ-calculus, we can indeed paint in blue the starting relation, and in red its transitive closure. Coloured confluence can be much easier to prove than confluence of the original relation, because the two coloured relations can have very different labellings, giving more flexibility. Whether the coloured version of the decreasing diagrams method is constructively complete for abstract relations is open, but there is now a constructive labelling for the commutation version of Huet's generalization [Hue80, Lemma 2.5]. We shall indeed prove that the most important criteria among those we know of can be proved with a constructive labelling when using coloured diagrams, which shows their importance.

The situation gets more complex when it comes to term rewrite systems. Van Oostrom's framework is abstract, only objects without structure are rewritten. The framework therefore allows for *critical peaks* only: an object a rewriting to objects b and c. Disjoint peaks enjoy a decreasing diagram for any well-behaved labelling. Our experience is that difficulties come essentially from ancestor peaks. Ancestor peaks are joinable in various ways, depending on whether or not a given rule is left-linear or right-linear. These joinability diagrams are not decreasing in general, unless the rules are linear, or simply left-linear, but the technicalities get more complex. Indeed, another result of Huet, called *parallel closedness* criterion [Hue80, Lemma 3.3], says that a left-linear system is confluent if all its critical peaks $v \leftarrow u \rightarrow w$ satisfy the condition $v \rightarrow^{p_1} \ldots \rightarrow^{p_n} w$ where $\{p_i\}_{i \in [1..n]}$ is a set of pairwise disjoint positions. We shall prove it, as well as its generalization [Toy88], by blending coloured *multi-labelled* diagrams with positional rewriting in order to abstract these results from a particular term structure. Multi-labelling refers to a powerful extension of van Oostrom's technique allowing for global interpretations defined locally by a sequence of labels.

Organization. Our goal is to lift van Oostrom's result to abstract positional rewriting, so as to capture the concrete results in both the terminating and the non-terminating case. Our abstract framework of (multi-) labelled abstract positional rewrite systems is described in Section 4.1 together with our strategy for proving confluence. We will review in subsequent sections several important results which are characteristic of the literature on confluence, and derive them as concrete cases of a same schema. On this journey, we are not going to consider all rewriting notions captured by a NARS, but only plain and parallel rewriting, the general case of NARS, for example higher-order rewriting that motivates the work in this thesis, being left for future work.

4.1 Labelled Positional Rewriting

Labelled positional rewriting brings together labelled rewriting as defined by van Oostrom and positional rewriting as introduced by Jouannaud and Li. As a consequence, our notations are possibly heavier than usual, and sometimes heavier than needed. We assume given:

- a set $\mathcal{L}$ of labels, as before, equipped with a partial quasi-order $\trianglerighteq$ whose strict part $\triangleright$ is well-founded;
- an *abstract* set $\mathcal{P}$ whose elements are called *positions*, equipped with a partial well-founded order $>_{\mathcal{P}}$, writing $p\#q$ for incomparable positions p, q, satisfying the axiom: $p'\#q$ if $p' >_{\mathcal{P}} p$ and $p\#q$, a binary (infix) *concatenation* operation "$\cdot$", and a minimum Λ satisfying the axioms: $p \cdot \Lambda = \Lambda \cdot p = p$ and $p \cdot q >_{\mathcal{P}} p$ provided $q \neq \Lambda$. Given a set of positions Q, we let $p \cdot Q := \{p \cdot q \mid q \in Q\}$;
- a set $\mathcal{O}$ of objects, as before.

We should note that the positions defined here and in this chapter are *different* from the ones defined in Chapter 2 and used in other chapters. The notion of positions in this chapter is at an abstract level. It would however be instantiated by the usual one when we apply the results of labelled positional rewriting to concrete term rewriting.

4.1.1 Domains

A *domain* P_p is any non-empty, *downward closed* set of positions $p' \geq_{\mathcal{P}} p$, that is, such that $p' \in P_p$ and $p' \geq_{\mathcal{P}} q \geq_{\mathcal{P}} p$ imply $q \in P_p$ (hence, $p \in P_p$). In some cases, p will not be mentioned, writing then P instead of P_p. In practice, a domain is meant to be the set of non-variable positions of some occurrence of a left-hand side of rule in a term. We denote by $\mathcal{D}_{\mathcal{P}}$ the set of domains over $\mathcal{P}$. We use the letters p, q for positions the notations P_p, Q_q for domains.

Given a position p and a set Q of positions, we write $p >_{\mathcal{P}} Q$ if $(\exists q \in Q)\, p >_{\mathcal{P}} q$ and $(\forall q \in Q)\, q \not\geq_{\mathcal{P}} p$. Given domains P_p and Q_q, we write $Q_q >_{\mathcal{P}} P_p$ if $q >_{\mathcal{P}} P_p$. Two domains P_p, Q_q are *parallel* or *disjoint*, written $P_p \# Q_q$ if $p \# q$.

We use the letters Γ, Δ for multisets (or sequences) of domains, and specifically Π, Θ for sets (or sequences) of *pairwise parallel* domains, which set is denoted by $\mathcal{D}_{\#\mathcal{P}}$.

We write:

$\Gamma \# P_p$ if $(\forall Q_q \in \Gamma)\, Q_q \# P_p\,$;
$\Gamma \# \Delta$ if $(\forall P_p \in \Gamma)\, P_p \# \Delta\,$;
$\Gamma \in P_p$ if $(\forall Q_q \in \Gamma)\, q \in P_p\,$;
$\Gamma \geq_{\mathcal{P}} p$ if $(\forall Q_q \in \Gamma)\, q \geq_{\mathcal{P}} p\,$;
$\Gamma >_{\mathcal{P}} P_p$ if $(\forall Q_q \in \Gamma)\, Q_q >_{\mathcal{P}} P_p\,$;
$P_p \bowtie Q_q$ if $p \notin Q_q \wedge q \notin P_p\,$;
$\Gamma \bowtie \Delta$ if $(\forall P_p \in \Gamma)(\forall Q_q \in \Delta) P_p \bowtie Q_q$.

We shall freely use the following straightforward key property of domains, which first three cases are called respectively "*disjoint case*", "*critical case*" and "*ancestor case*" in the literature:

Lemma 4.1.1. *$(\forall p, q \in \mathcal{P})(\forall P_p \in \mathcal{D}_{\mathcal{P}})(q \# p \vee q \in P_p \vee q >_{\mathcal{P}} P_p \vee p >_{\mathcal{P}} q)$.*

4.1.2 Rewriting

A *labelled positional rewrite step* is a tuple $\langle s, t, l, P_p \rangle$ for $s, t \in \mathcal{O}$, $l \in \mathcal{L}$ and $P_p \in \mathcal{D}_{\mathcal{P}}$, which is denoted by $s \to^{l}_{P_p} t$ and we may omit any of l, s, t or P_p. A *labelled positional rewrite relation* is a rewrite relation generated by labelled positional rewrite steps.

Notions of labelled (abstract) rewriting can be extended naturally to labelled positional rewriting by replacing labelled rewrite steps with labelled positional rewrite steps. The notations are extended as expected. In particular, *reachability* (resp., *convertibility*) is denoted by $\twoheadrightarrow^{\alpha}_{\Gamma}$ (resp., $\twoheadleftarrow\!\!\twoheadrightarrow^{\alpha}_{\Gamma}$) for some sequences α of labels and Γ of domains. Mention of l, P_p, α, Γ may be altogether omitted, or abbreviated appropriately, in general by the property that they satisfy, as in $\to^{l}_{\geq_{\mathcal{P}} p}$.

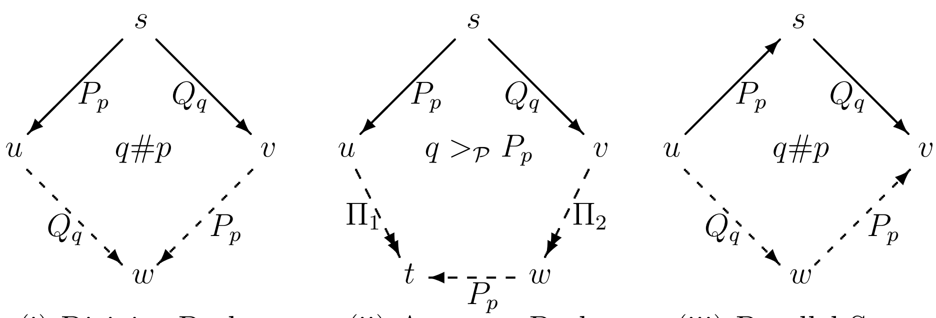
Conversions can be coloured as explained in the introduction, rewrites heading left in blue and those heading right in red. All notions have therefore a coloured version, which is from now on the one we consider in this chapter, the uncoloured one being obtained by taking identical labellings for both colours.

4.1.3 Rewriting Axioms

According to Lemma 4.1.1, there are three kinds of local peaks: *disjoint peaks* if $q \# p$, *ancestor peaks* if $q >_{\mathcal{P}} P_p$, and *critical peaks* if $q \in P_p$. Note that the fourth case in Lemma 4.1.1 is captured by symmetry.

Aiming at applications on first-order term rewriting in this thesis, we now assume that rewriting satisfies three (unlabelled) axioms, one for disjoint peaks, one for ancestor peaks and one for parallel steps that relates to the notion of *square permutations* [GLM92], which are displayed in Figure 4.1, where Π_1 and Π_2 are supposed to be sequences of pairwise parallel domains. The (universally quantified) assumptions are pictured with plain arrows, while the (existentially quantified) conclusions are pictured with dashed arrows.

In case rewrites are coloured, there are indeed two versions of the ancestor peak axiom, depending which colour is above the other.



(i) Disjoint Peak (ii) Ancestor Peak (iii) Parallel Steps

Figure 4.1: Positional Rewriting Axioms

The following lemma follows from the parallel steps axiom:

Lemma 4.1.2. *Given a set of domains $\Pi \in \mathcal{D}_{\#\mathcal{P}}$, and two enumerations Π_1 and Π_2 of Π, then $s \twoheadrightarrow_{\Pi_1} t$ if and only if $s \twoheadrightarrow_{\Pi_2} t$.*

We can therefore define *parallel positional rewriting* as the relation such that $s \Rightarrow_{\Pi} t$ iff $s \twoheadrightarrow_{\Pi_1} t$ for an arbitrary enumeration Π_1 of the set Π of parallel domains. We have the following straightforward properties of parallel rewriting:

Lemma 4.1.3. *$s \Rightarrow_{\{P_p\}} t$ if and only if $s \rightarrow_{P_p} t$.*

Lemma 4.1.4. *Assume that $\Pi\#\Theta$. Then $s \Rightarrow_{\Pi\cup\Theta} t$ if and only if $s \Rightarrow_{\Pi} u \Rightarrow_{\Theta} t$ for some u.*

4.1.4 Local Diagrams

In this chapter, since rewrites are coloured, we shall only consider coloured diagrams. The decreasing diagrams framework is carried out in its coloured version. A *coloured local diagram* D is therefore a pair made of a *coloured local peak* $D_{peak} = v \leftarrow u \rightarrow w$ and a *coloured conversion* $D_{conv} = v \twoheadleftarrow\!\!\twoheadrightarrow w$. We rephrase Theorem 2.2.6 in its coloured version:

Theorem 4.1.5 ([vO08a]). *A labelled rewrite relation is coloured Church-Rosser (hence coloured confluent) if all its coloured local peaks have a decreasing diagram.*

In [JvO09], Jouannaud and van Oostrom proved Theorem 2.2.6 by diagram rewriting (Definition 2.2.10). Despite the fact that it is proved there for uncoloured conversions, the proof applies without any change to coloured conversions, hence Theorem 4.1.5, since rewriting a coloured conversion yields a coloured conversion. In Chapter 3, we have shown that the idea of the proof by Jouannaud and van Oostrom based on diagram rewriting is to define a measure on conversions that decreases when replacing a local peak by the conversion associated to its decreasing diagram. Termination of diagram rewriting then implies the Church-Rosser property, thus confluence. A simpler measure has already been introduced in Chapter 3. Yet another two related measure are given in [FvO13]. We shall define here an alternative measure which blends the one in Chapter 3 and the monotonic one in [FvO13]:

Definition 4.1.6. The interpretation of a conversion π is defined as the multiset $[\![\pi]\!] := \{\langle l, \psi\rangle \mid \pi = \psi \to^l \kappa \text{ or } \pi = \kappa \ {}^l\!\!\leftarrow \psi\}$. Conversions are compared in the quasi-order $\pi \succeq\!\!\succ \psi$ iff $[\![\pi]\!]\ ((\trianglerighteq, \succeq\!\!\succ)_{lex})_{mul}\ [\![\psi]\!]$, the equivalence being the equality $\pi == \psi$ iff $[\![\pi]\!]\ ((=, ==)_{lex})_{mul}\ [\![\psi]\!]$.

Here is the main property of the above order, implying Theorems 2.2.6 and 4.1.5:

Lemma 4.1.7. $\succeq\!\!\succ$ *(defined in Definition 4.1.6) is a partial quasi-order, whose strict part* $\succ\!\!\succ$ *is well-founded, and such that* $\pi D_{peak} \psi \succ\!\!\succ \pi D_{conv} \psi$ *for any decreasing diagram* D *and conversions* π, ψ.

This property is proved first in [JvO09] with a complex order, in Chapter 3 with a simpler, related order, and in [FvO13] with two slightly different, yet novel orders. The order given here is easier to define than the one in Chapter 3, without using the notion of visible steps. But their proofs are similar.

In the sequel, the colouring will remain implicit.

A special kind of local diagrams called *fixed diagrams* is considered.

Definition 4.1.8. Given a labelled rewrite system R, a local diagram D is *fixed* if $\pi D_{peak} \psi == \pi D_{conv} \psi$ for any two conversions π, ψ.

The existence of fixed diagrams depends on the properties of the order on conversions. If this order is monotonic, as is the one introduced in [FvO13], then the above condition reduces to $D_{peak} == D_{conv}$. If it is not, as are the present one and those introduced in [JvO09] and Chapter 3, then the property must be checked whether it holds or not for a given diagram. The following simple fixed diagram is used in Theorem 4.4.14:

Lemma 4.1.9. *Let $D_{peak} = v \ {}^{m}\!\!\leftarrow u \rightarrow^{n} w$ and $D_{conv} = v \ {}^{m}\!\!\leftarrow u' \rightarrow^{n} w$, where $m, n \in \mathcal{L}$. Then D is a fixed diagram.*

We now consider n*-labelled* abstract rewrite systems with $n > 0$, for which each single rewrite step is labelled by a sequence $[l_1, \ldots, l_n]$, each label l_i belonging to a set $\mathcal{L}_i$ equipped with an order $\trianglerighteq_i$ whose strict part $\triangleright_i$ is well-founded.

Definition 4.1.10. Given $n > 0$, a set $\mathcal{O}$ of objects, and sets $\mathcal{L}_i$ of labels, each of which is equipped with an order $\trianglerighteq_i$ whose strict part $\triangleright_i$ is well-founded with $i \in [1, n]$. An *n-labelled rewrite step* is a triple $\langle s, t, [l_1, \ldots, l_n]\rangle$ for $s, t \in \mathcal{O}$ and $l_i \in \mathcal{L}_i$ with $i \in [1, n]$, denoted by $s \rightarrow^{[l_1,\ldots,l_n]} t$. An *$n$-labelled rewrite system* is composed of a set $\mathcal{O}$ and a set of n-labelled rewrite steps, while an *n-labelled rewrite relation* is the corresponding relation.

The sequence itself is not a label, this would then be a labelled system as before and we would use the word "tuple" instead. We generally call n-labelled rewrite steps (resp., rewrite systems, rewrite relations) for some $n > 0$ by *multi-labelled* rewrite steps (resp., rewrite systems, rewrite relations), omitting the mention of n.

Theorem 4.1.11. *An n-labelled abstract rewrite relation is coloured Church-Rosser (hence coloured confluent) if, for each local peak there exists some $j \leq n$ such that the local peak enjoys a fixed diagram for every ith-label with $i < j$ and a decreasing diagram for its jth-label.*

Proof. Conversions now decrease in the order $(\succcurlyeq\!\!\succ_1, \ldots, \succcurlyeq\!\!\succ_n)_{lex}$ when a local peak is replaced by its associated conversion. $\square$

The use of an n-labelled relation is actually different from the use of the tuple $\langle l_1, \ldots, l_n \rangle$ as a (single) label, since the order $(\succeq\!\!\succ_1, \ldots, \succeq\!\!\succ_n)_{lex}$ is different from the order $\succeq\!\!\succ$ generated by the n-tuple of labels. Multi-labelled systems are indeed a way to use labelling as a complex global interpretation on conversions, while still concentrating on local peaks.

We will show the important impact of this seemingly small extension of van Oostrom's technique in Theorem 4.4.14.

4.2 Terminating Systems

In this first application of Theorem 4.1.11, we assume a single colour and a single label, which means rewrite relations are 1-labelled, that is, van Oostrom's original labelling technique as described by Theorem 2.2.6 suffices. We further make three key assumptions throughout this section:

(i) rewriting satisfies the axioms for disjoint and ancestor peaks ;

(ii) the rewrite relation is terminating ;

(iii) we use *self-labelling*: a rewrite step $u \to v$ is labelled by u.

Self-labelling is made possible by assumption (ii), labels being compared in the order $\twoheadrightarrow$. The following important lemma is straightforward:

Lemma 4.2.1. *Joinable local peaks enjoy a decreasing diagram.*

The result then follows:

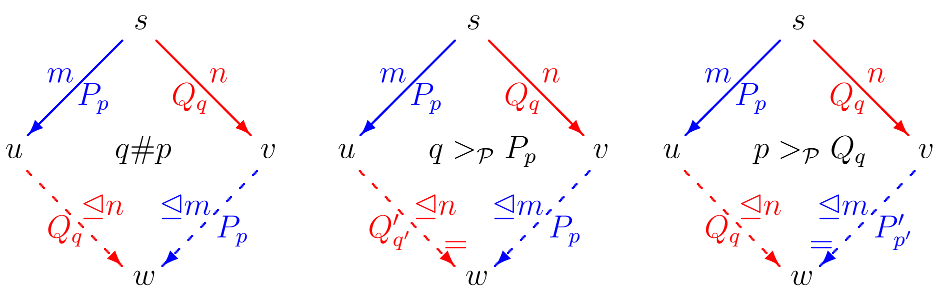
Theorem 4.2.2. *A terminating labelled positional rewrite relation satisfying the axioms for disjoint and ancestor peaks is confluent if and only if all its critical peaks are joinable.*

Proof. Using Lemma 4.2.1. □

Terminating, first-order rewriting satisfies Theorem 4.2.2, possibly the most celebrated result on the topic [KB70]. So do Church's simply typed λ-calculus [CR36], another celebrated result, and more generally algebraic, functional languages [JO91]. However, note that Theorem 4.2.2 is different from the critical pair criteria in the literature, since there is still a gap between the (abstract) critical peaks and the (concrete) critical pairs. It needs some work when applying Theorem 4.2.2 to concrete systems.

4.3 Linear Systems

In this second application of Theorem 4.1.11, we assume two colours and a single label. We further make a key assumption about the labelling and joinability of disjoint and (duplicated) ancestor peaks, which is displayed at Figure 4.2.



(i) Disjoint Peak (ii) Linear Ancestor Peak (a) (iii) Linear Ancestor Peak (b)

Figure 4.2: Linear Axioms for Disjoint and Ancestor Peaks

These revised axioms for disjoint and linear ancestor peaks are indeed decreasing diagrams. Note that comparing rewrite positions breaks the symmetry between the two colours, which results in two different axioms for ancestor peaks.

We still need to care about critical peaks, and again, comparing positions will break the symmetry between two colours, which will result this time in three kinds of critical peaks, the new kind corresponding to the case where the two rewrite positions are equal.

- *top critical peaks*: $u \; {}^{m}_{P_p}\!\leftarrow s \to^{n}_{Q_q} v$ with $q = p$
- *red subterm critical peaks*: $u \; {}^{m}_{P_p}\!\leftarrow s \to^{n}_{Q_q} v$ with $q \in P_p \setminus \{p\}$
- *blue subterm critical peaks*: $u \; {}^{m}_{P_p}\!\leftarrow s \to^{n}_{Q_q} v$ with $p \in Q_q \setminus \{q\}$

The following result follows easily from Theorem 4.1.11 and Lemma 4.1.1:

Theorem 4.3.1. *A labelled positional rewrite relation satisfying the axioms in Figure 4.2 for disjoint and linear ancestor peaks is coloured Church-Rosser if all its critical peaks enjoy a decreasing diagram.*

This result applies to any concrete system satisfying these axioms, which are very restrictive since they are true of *linear systems* only. In case the two coloured relations are identical, then we can conclude that the original relation is confluent. The particular case of first-order linear rewriting appears in [ZFM15], with a similar uni-coloured analysis.

Notice that critical peaks need be duplicated in the coloured version, that is, need to be distinguished by comparing the minimum positions of the two steps, unless the superposition is at the top, but not anymore if the two colours are identical, as is the case when we are interested in a direct proof of confluence of a given relation. On the other hand, having two colours gives more flexibility for the labelling, hence may help in finding decreasing diagrams for some critical pairs.

Theorem 4.3.1 implies Huet's generalization [Hue80, Lemma 2.5] of Hindley–Rosen's Lemma. Both are actually direct applications of the coloured version of Theorem 4.1.5, as first noted by van Oostrom [vO94a].

4.4 Left-Linear Systems

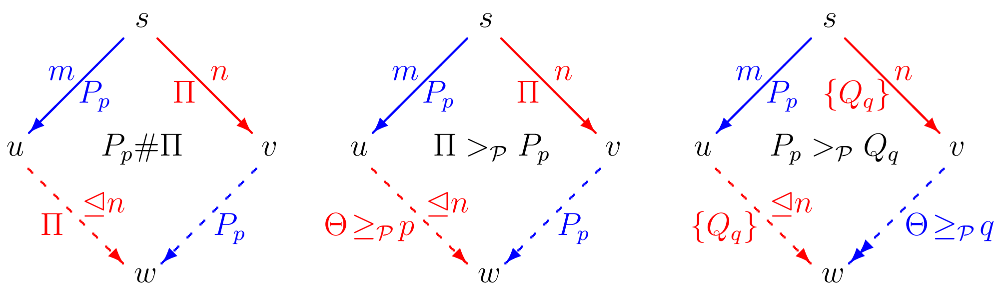
In this section, we relax the previous assumption for ancestor peaks, by allowing for rewriting in parallel at a set of disjoint occurrences on the right. To this end, we shall need the full power of Theorem 4.1.11 with two colours and sequences of labels. Technically, we shall follow Tait's steps that we refine with a variation by taking the given rewrite relation as blue, and its parallel rewriting version as red. This choice will be easier to carry out than taking parallel rewriting for both the blue and red relations as done by Tait and others.

We first introduce several kinds of local peaks needed in presence of parallel rewriting:

Definition 4.4.1. A local peak $u\ {}_{P_p}\!\!\leftarrow s \rightarrow_{\Pi} v$ is called a *disjoint peak* if $P_p \# \Pi$, a *(parallel) blue/red ancestor peak* if $\Pi >_{\mathcal{P}} P_p$, a *parallel blue/red critical peak* if $\Pi \in P_p$ and a *plain blue/red critical peak* if $\Pi = \{Q_q\}$ and $q \in P_p$. A local peak $u\ {}_{P_p}\!\!\leftarrow s \rightarrow_{\{Q_q\}} v$ is called a *(plain) red/blue ancestor peak* if $p >_{\mathcal{P}} Q_q$, and a *(plain) red/blue critical peak* if $p \in Q_q$.

Throughout this section, we revise the axioms for disjoint and ancestor peaks as in Figure 4.3, and make four assumptions on the labels used:

- red labels are strictly larger than blue labels;
- the set of red labels is a sup-semi-lattice;
- given a parallel step $s \rightarrow^{m}_{\Pi} t$, we assume that its label is the sup of the labels of its elementary parallel steps. Therefore, given any Π_1, Π_2 such that $\Pi = \Pi_1 \cup \Pi_2$ and $s \rightarrow^{m_1}_{\Pi_1} u \rightarrow^{m_2}_{\Pi_2} t$ for some u, then $m = sup\{m_1, m_2\}$;
- given $s \rightarrow^{m_1}_{\Pi_1} u \rightarrow^{m_2}_{\Pi_2} t$ with $\Pi_1 \# \Pi_2$, by Lemma 4.1.4 we have $s \rightarrow_{\Pi_2} v \rightarrow_{\Pi_1} t$ for some v, we further assume the labels satisfy $s \rightarrow^{m_2}_{\Pi_2} v \rightarrow^{m_1}_{\Pi_1} t$.



(i) Disjoint Peak (ii) Left-linear Blue/Red Ancestor Peak (iii) Left-Linear Red/Blue Ancestor Peak

Figure 4.3: Left-Linear Axioms for Disjoint and Ancestor Peaks

We use Σ to denote sequence of elements in $\mathcal{D}_{\#\mathcal{P}}$, writing $\Sigma \# \Gamma$ if $(\forall \Pi \in \Sigma)\, \Pi \# \Gamma$, and $\Sigma \geq_{\mathcal{P}} p$ if $(\forall \Pi \in \Sigma)\, \Pi \geq_{\mathcal{P}} p$.

To prepare the proof of the main theorem of this section, we need three auxiliary lemmas:

Lemma 4.4.2. *Given a derivation* $s \twoheadrightarrow^{\alpha}_{\Sigma} u \rightarrow^{n}_{\Pi} t$ *such that* $\Sigma \# \Pi$*, then* $s \rightarrow^{n}_{\Pi} v \twoheadrightarrow^{\alpha}_{\Sigma} t$ *for some* v*.*

Proof. By induction on the number of steps in $s \twoheadrightarrow^{\alpha}_{\Sigma} u$ and application of Lemma 4.1.4 and our assumptions on labels. □

Lemma 4.4.3. *Given a peak* $u \; {}_{\Gamma}\!\twoheadleftarrow s \rightarrow^{n}_{\Pi} v$ *such that* $\Gamma \# \Pi$*, then* $u \rightarrow^{n'}_{\Pi} t \; {}_{\Gamma}\!\twoheadleftarrow v$ *for some* t, n' *with* $n' \trianglelefteq n$*.*

Proof. By induction on the number of steps in $u \; {}_{\Gamma}\!\twoheadleftarrow s$ and application of the axiom for disjoint peaks. □

Lemma 4.4.4. *Given a peak* $u \; {}_{\Theta}\!\twoheadleftarrow s \rightarrow^{n}_{\Pi} v$ *such that* $\Theta \bowtie \Pi$*, then* $u \rightarrow^{n'}_{\Pi'} t \; {}_{\Gamma}\!\twoheadleftarrow v$ *for some* t, Π', Γ *and* n' *with* $n' \trianglelefteq n$*. If* $\Theta \cup \Pi \geq_{\mathcal{P}} p$ *is satisfied for some position* p*, then* $\Pi' \cup \Gamma \geq_{\mathcal{P}} p$*.* Π' *is called the* residual *of* Π *after the derivation* $s \twoheadrightarrow_{\Theta} u$*, denoted by* Π/Θ*.*

The notion of residual is quite old [CR36]. It is the key to many results, like the finite developments theorem and the standardization theorem, see [Ter03].

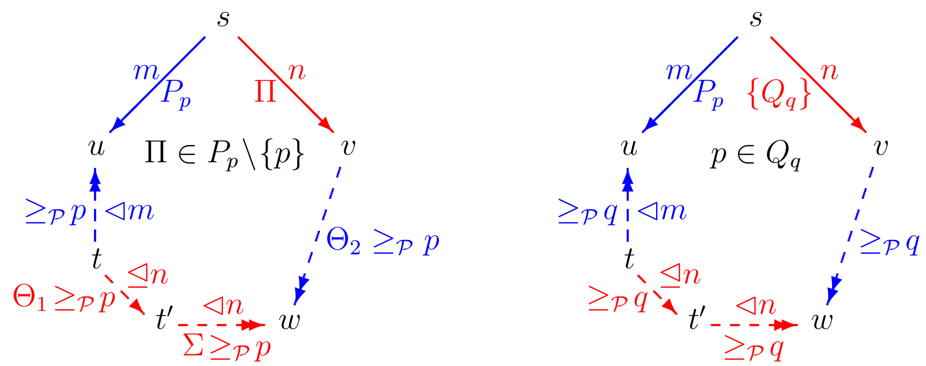
Proof. The proof is by induction on the number of steps in $s \twoheadrightarrow_{\Theta} u$.

Selecting the first step $s \rightarrow_{P^1_{p_1}} u'$ of $s \twoheadrightarrow_{\Theta} u$, we have $u \; {}_{\Theta'}\!\twoheadleftarrow u' \; {}_{P^1_{p_1}}\!\leftarrow s \rightarrow^{n}_{\Pi} v$ where $\Theta' = \Theta \setminus \{P^1_{p_1}\}$. To analyze the local peak $u' \; {}_{P^1_{p_1}}\!\leftarrow s \rightarrow^{n}_{\Pi} v$, we split Π as $\Pi = \Pi_1 \cup \Pi_2$ such that $\Pi_1 \# P^1_{p_1}$ and Π_2 satisfying either $\Pi_2 >_{\mathcal{P}} P^1_{p_1}$ or $(\forall Q_q \in \Pi_2)\, p_1 >_{\mathcal{P}} Q_q$, in which case Π_2 contains one element or is empty. It follows in both cases that $s \rightarrow^{n_1}_{\Pi_1} v' \rightarrow^{n_2}_{\Pi_2} v$. By the axiom for disjoint peaks, $u' \rightarrow^{n'_1}_{\Pi_1} w' \; {}_{P^1_{p_1}}\!\leftarrow v'$ for some w' with $n'_1 \trianglelefteq n_1$. Using now the axiom for ancestor peaks, $w' \; {}_{P^1_{p_1}}\!\leftarrow v' \rightarrow^{n_2}_{\Pi_2} v$ can be joined by $w' \rightarrow^{n'_2}_{\Pi'_2} w \; {}_{\Gamma}\!\twoheadleftarrow v$ for some Π'_2, Γ, w with $n'_2 \trianglelefteq n_2$, where $\Pi'_2 \geq_{\mathcal{P}} p_1$ if $\Pi_2 >_{\mathcal{P}} P^1_{p_1}$, or $\Pi'_2 = \Pi_2$ otherwise. In both cases, $\Pi'_2 \# \Pi_1$ and $\Pi'_2 \bowtie \Theta'$, thus $u' \rightarrow^{n'}_{\Pi_1 \cup \Pi'_2} w \; {}_{\Gamma}\!\twoheadleftarrow v$, with $n' = sup\{n'_1, n'_2\} \trianglelefteq sup\{n_1, n_2\} = n$ and $\Theta' \bowtie (\Pi_1 \cup \Pi'_2)$. If there exists some p such that $\Theta \cup \Pi \geq_{\mathcal{P}} p$, it is easy to see $\Theta' \cup \Pi_1 \cup \Pi'_2 \cup \Gamma \geq_{\mathcal{P}} p$.

Applying the induction hypothesis to the peak $u \;{}_{\Theta'}\!\twoheadleftarrow u' \rightarrow^{n'}_{\Pi_1 \cup \Pi'_2} w$ yields the result. $\square$

The following result follows:

Theorem 4.4.5. *Assuming that parallel steps have labels which are strictly larger than the labels of plain steps, a labelled positional rewrite relation satisfying the axioms for disjoint and left-linear ancestor peaks is confluent if its critical peaks satisfy the decreasing diagrams in Figure 4.4:*



$(\forall \Pi' \# \Pi$ s.t. $\Pi' >_{\mathcal{P}} P_p$ and $v \rightarrow_{\Pi'} v')$
$(\Theta_2 \bowtie \Pi'$, $\Theta_1 \# (\Pi'/\Theta_2)$ and $\Sigma \# (\Pi'/\Theta_2))$

(i) Parallel Blue/Red Critical Peaks (ii) Plain Red/Blue Critical Peaks

Figure 4.4: Assumptions for (Left-Linear) Critical Peaks

Proof. We show that every local peak $u \;{}^{m}_{P_p}\!\leftarrow s \rightarrow^{n}_{\Pi} v$ has a decreasing diagram. There are three cases according to the relative positions of P_p and Π:

1. $(\forall Q_q \in \Pi) P_p \bowtie Q_q$. We conclude by Lemma 4.4.4.

2. $(\exists Q_q \in \Pi)\, q \in P_p \setminus \{p\}$. The proof is represented in Figure 4.5. Since there exists no $Q_q \in \Pi$ such that $q < p$, we first split Π into $\Pi = \Pi_1 \cup \Pi_2 \cup \Pi_3$ with $\Pi_1 := \{Q_q \in \Pi \mid q \in P_p\}$, $\Pi_2 := \{Q_q \in \Pi \mid q >_{\mathcal{P}} P_p\}$ and $\Pi_3 := \{Q_q \in \Pi \mid q \# p\}$. Hence $s \rightarrow^{n_1}_{\Pi_1} v_1 \rightarrow^{n_2}_{\Pi_2} v_2 \rightarrow^{n_3}_{\Pi_3} v$ by Lemma 4.1.4, and $n = sup\{n_1, n_2, n_3\}$ by assumption on labels of

parallel steps. By assumption, the blue/red critical peak $u \;{}_{P_p}^{m}\!\!\leftarrow s \to_{\Pi_1}^{n_1} v_1$ has a conversion $u \;{}^{\lhd m}\!\!\twoheadleftarrow t \to_{\Theta_1}^{n_1'} t_1' \twoheadrightarrow_{\Sigma}^{\alpha} w_1 \;{}_{\Theta_2}\!\!\twoheadleftarrow v_1$, with $\Theta_2 \bowtie \Pi_2$, $\Theta_1 \cup \Theta_2 \geq_{\mathcal{P}} p$, $\Sigma \geq_{\mathcal{P}} p$, $n_1' \unlhd n_1$ and $\alpha \lhd n_1 \unlhd n$. By Lemma 4.4.4, the peak $w_1 \;{}_{\Theta_2}\!\!\twoheadleftarrow v_1 \to_{\Pi_2}^{n_2} v_2$ can be joined by $w_1 \to_{\Pi_2'}^{n_2'} w_2 \;{}_{\Gamma}\!\!\twoheadleftarrow v_2$ where $n_2' \unlhd n_2$ and $\Pi_2' \cup \Gamma \geq_{\mathcal{P}} p$. For the peak $w_2 \;{}_{\Gamma}\!\!\twoheadleftarrow v_2 \to_{\Pi_3}^{n_3} v$, since $P_p \# \Pi_3$ by definition, we have $\Gamma \# \Pi_3$, hence $w_2 \to_{\Pi_3}^{n_3'} w \;{}_{\Gamma}\!\!\twoheadleftarrow v$ by Lemma 4.4.3 with $n_3' \unlhd n_3$. By assumption in Figure 4.4 (i), $\Sigma \# \Pi_2'$, hence $t_1' \to_{\Pi_2'}^{n_2'} t_2' \twoheadrightarrow_{\Sigma}^{\alpha} w_2$ by Lemma 4.4.2. We also have $t_2' \to_{\Pi_3}^{n_3'} t' \twoheadrightarrow_{\Sigma}^{\alpha} w$ since $\Sigma \geq_{\mathcal{P}} p$ and $P_p \# \Pi_3$. Thanks to the assumption in Figure 4.4 (i), $\Theta_1 \# \Pi_2'$. Since $\Theta_1 \geq_{\mathcal{P}} p$, $\Pi_2' \geq_{\mathcal{P}} p$ and $P_p \# \Pi_3$, $t \to_{\Theta_1 \cup \Pi_2' \cup \Pi_3}^{n'} t'$ by Lemma 4.1.4, where $n' = \mathit{sup}\{n_1', n_2', n_3'\} \unlhd \mathit{sup}\{n_1, n_2, n_3\} = n$. The local peak $u \;{}_{P_p}^{m}\!\!\leftarrow s \to_{\Pi}^{n} v$ has therefore a decreasing conversion, namely $u \;{}^{\lhd m}\!\!\twoheadleftarrow t \to_{\Theta_1 \cup \Pi_2' \cup \Pi_3}^{n'} t' \twoheadrightarrow_{\Sigma}^{\lhd n} w \;{}_{\Gamma}\!\!\twoheadleftarrow v$.

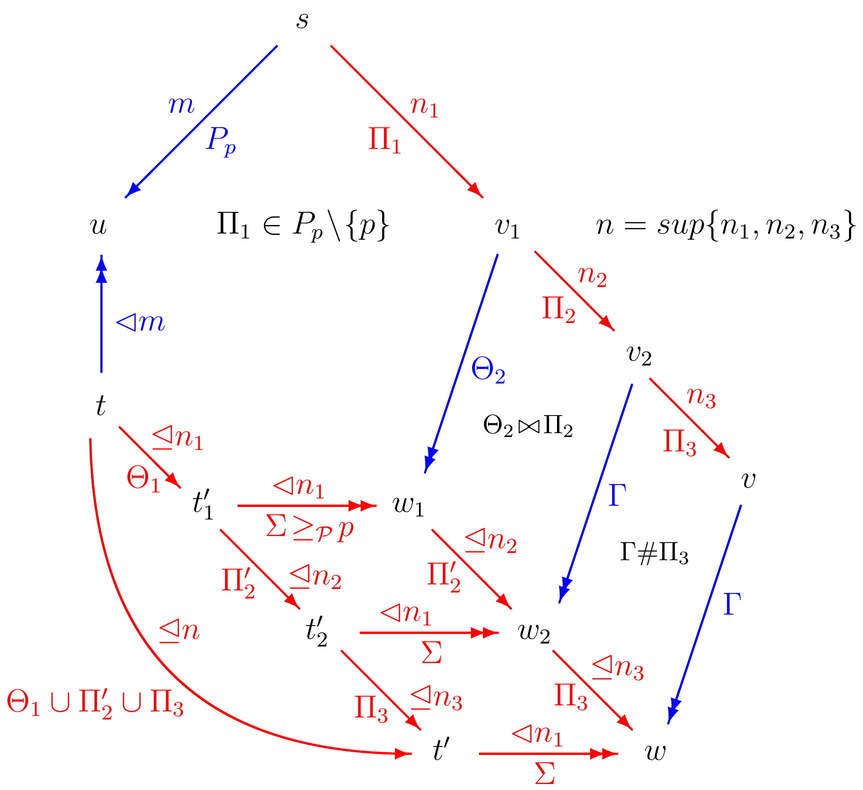


Figure 4.5: Proof of Theorem 4.4.5, Case 2

3. $(\exists Q_q \in \Pi)\, p \in Q_q$. We first split the step $s \rightarrow^{n}_{\Pi} v$ into $s \rightarrow^{n_1}_{\{Q_q\}} v' \rightarrow^{n_3}_{\Pi_3} v$ where $p \in Q_q$ and $\Pi_3 = \Pi \setminus \{Q_q\}$. By assumption, the plain red/blue critical peak $u \; {}_{P_p}^{m}\!\leftarrow s \rightarrow^{n_1}_{\{Q_q\}} v'$ admits the conversion $u \; {}^{\lhd m}\!\twoheadleftarrow t \rightarrow^{\lhd n_1}_{\Theta_1} t'_1 \twoheadrightarrow^{\lhd n_1}_{\Sigma} w_1 \; {}_{\Gamma}\!\twoheadleftarrow v'$ where $\Gamma \geq_{\mathcal{P}} q$, $\Sigma \geq_{\mathcal{P}} q$ and $\Theta_1 \geq_{\mathcal{P}} q$. Since $Q_q \# \Pi_3$, we have $\Gamma \# \Pi_3$, $\Sigma \# \Pi_3$ and $\Theta \# \Pi_3$. Then the proof continues similarly as in Case 2. $\square$

Note that the rewrites from v to w in Figure 4.4 (i) are pairwise disjoint, while those in Figure 4.4 (ii) are arbitrary, making these two figures incompatible when $\Pi = \{Q_p\}$. In fact, we can define a more general, but also more complex condition than the one given in Figure 4.4 (i).

Definition 4.4.6. Given a derivation $t \; {}_{\Gamma}\!\twoheadleftarrow s$ and a set Π of pairwise parallel domains, we say that Γ and Π are *overlap-free*, written $\Gamma \bowtie^{*} \Pi$, if and only if $\Gamma = nil$, or $t \; {}_{\Gamma'}\!\twoheadleftarrow t_1 \; {}_{P_p}\!\leftarrow s$, $(\forall Q_q \in \Pi)\, P_p \bowtie Q_q$ and one of the following three conditions holds:

Case (i): $P_p \# \Pi$, then $\Gamma' \bowtie^{*} \Pi$.

Case (ii): $(\exists Q_q \in \Pi)\, p >_{\mathcal{P}} Q_q$, then $\Gamma' \bowtie^{*} \Pi$.

Case (iii): $\Pi_1 := \{Q_q \in \Pi \mid Q_q >_{\mathcal{P}} P_p\} \neq \varnothing$, then $\Gamma' \bowtie^{*} (\Pi'_1 \cup \Pi_2)$, where $\Pi_2 = \Pi \setminus \Pi_1$ and $\Pi'_1 := \Pi_1 / \{P_p\}$.

Note that for any $\Theta, \Pi \in \mathcal{D}_{\#\mathcal{P}}$, $\Theta \bowtie^{*} \Pi$ if $\Theta \bowtie \Pi$. Then extensions of Lemma 4.4.4 and Theorem 4.4.5 follow easily:

Lemma 4.4.7. *Given a peak $u \; {}_{\Gamma}\!\twoheadleftarrow s \rightarrow^{n}_{\Pi} v$ such that $\Gamma \bowtie^{*} \Pi$, then $u \rightarrow^{n'}_{\Pi'} t \; {}_{\Gamma'}\!\twoheadleftarrow v$ for some t, Π', Γ' and n' with $n' \trianglelefteq n$. If $(\Gamma \cup \Pi) \geq_{\mathcal{P}} p$ is satisfied for some position p, then $(\Pi' \cup \Gamma') \geq_{\mathcal{P}} p$. We shall overload the word* residual *and call Π' the residual of Π after the derivation $s \twoheadrightarrow_{\Gamma} u$, denoting it by Π/Γ.*

Theorem 4.4.8. *Assuming that parallel steps have labels which are strictly larger than the labels of plain steps, a labelled positional rewrite relation satisfying the axioms for disjoint and left-linear ancestor peaks is confluent if its critical peaks satisfy the decreasing diagrams in Figure 4.4, replacing in Figure 4.4 (i) Θ_2 with Γ, and the bottom condition with the following one:*

$$(\forall \Pi' \# \Pi \ s.t.\ \Pi' >_{\mathcal{P}} P_p \ and\ v \rightarrow_{\Pi'} v')$$
$$(\Gamma \bowtie^* \Pi', \Theta_1 \# (\Pi'/\Gamma) \ and\ \Sigma \# (\Pi'/\Gamma)).$$

Proof. The proof is the same as for Theorem 4.4.5, replacing Lemma 4.4.4 by Lemma 4.4.7. □

With this new condition, take $\Pi = \{Q_q\}$ with $p = q$ in Figure 4.4 (i), giving then birth to a top critical peak. Then, the set Π' satisfying the condition above would be empty and the condition be trivially satisfied, making both figures identical in this case. This explains the condition $\Pi \in P_p \backslash \{p\}$ in Figure 4.4 (i), to avoid the duplication that would occur with $p = q$.

The overlap-free condition on Γ and Π' given in the theorem is somewhat complicated, because we cannot talk about variables at the abstract level. On the other hand, the condition will become quite simple at the concrete level where the notion of variable is available. This lack of expressivity of the abstract language is an obstacle for obtaining a better result.

4.4.1 First-Order Left-Linear Systems

Theorem 4.4.8 gives sufficient conditions for an abstract rewrite relation to be confluent. We shall now consider the concrete case of first-order (term) rewrite systems. To this end, we need to show that first-order rewriting satisfies our axioms, and that the abstract notion of critical peaks leads to the usual concrete notion of critical pairs.

Definition 4.4.9. Given a first-order term rewrite system R, a term u *rewrites in parallel* to a term v at *pairwise disjoint* positions $p_i \in \mathcal{P}os(u)$ with rules $l_i \rightarrow r_i \in R$, where $i \in [1, n]$, written as $u \Rightarrow_R^{\{p_1,\ldots,p_n\}} v$, if $u|_{p_i} = l_i\sigma_i$ and $v = u[r_1\sigma_1, \ldots, r_n\sigma_n]_{p_1,\ldots,p_n}$ for some substitutions $\{\sigma_i\}_{i\in[1,n]}$.

Here we use the coloured notation $\rightarrow$ instead of the uncoloured one $\Rightarrow$. We shall assume that the label of a plain rewrite step $v\ {}_{P_p}\!\!\leftarrow u$ is the integer 0 while the label of a parallel step $u \rightarrow_{\Pi} v$ is the integer 1, which satisfies our abstract assumption that the labels of parallel steps are strictly larger than that of plain steps. It also satisfies obviously the properties of labels for parallel steps.

Definition 4.4.10. Given a first-order rewrite system R, a rule $l \to r \in R$, a family of rules $\{g_i \to d_i\}_{i \leq n} \subseteq R$ and a set of disjoint positions $\{p_i \in \mathcal{FP}os(l)\}_i$ such that the unification problem $l|_{p_i} = g_i$ has most general unifier σ, then the pair $(r\sigma, l\sigma[d_1\sigma, \ldots, d_n\sigma]_{p_1,\ldots,p_n})$ is a *parallel red/blue critical pair* (a *plain critical pair* if $n = 1$) of the rules $g_1 \to d_1, \ldots, g_n \to d_n$ onto $l \to r$ at positions $p_1, \ldots, p_n$. A *top critical pair* is a plain critical pair with $p_1 = \Lambda$. Others are *subterm critical pairs*. Plain blue/red critical pairs are defined as expected.

There is no need for duplicating top critical pairs, we shall therefore consider that they are plain blue/red pairs, as in the abstract case. Decreasing diagrams for these pairs are obtained by instantiating the diagrams of Figure 4.4 and formulating their conditions appropriately:

Definition 4.4.11. Plain blue/red critical pairs are said to be *decreasing* if they satisfy the diagram of Figure 4.4 (ii).

Parallel red/blue critical pairs are said to be *decreasing* if they satisfy the diagram of Figure 4.4 (i), replacing Θ_2 by Γ, allowing domains that are not disjoint, with the conditions $\mathcal{V}ar(t'|_{\Theta_1}) \subseteq \mathcal{V}ar(s|_\Pi)$ and $(\forall\, s_i \to_{\Theta_i} t_i \in t' \twoheadrightarrow_\Sigma w)(\mathcal{V}ar(t_i|_{\Theta_i}) \subseteq \mathcal{V}ar(s|_\Pi))$.

This elegant condition is due to Toyama [Toy81] and used by Felgenhauer in [Fel13b]. It indeed follows quite naturally in the case of first-order terms from the abstract condition given at Figure 4.4. The condition allows to merge the parallel step below a parallel critical pair with the parallel step induced by its diagram, as we can see in the proof of Theorem 4.4.5. Note however that Felgenhauer's decreasing diagrams are different from ours since the labelling technique is not the same: he uses rule-labelling, each rule coming with an integer index. Rewrite steps, whether plain or parallel, use as label the set of rule indexes implied in the rewrite (a singleton set in case of plain rewrites). As a consequence, plain steps may have a bigger label than parallel steps, which gives more flexibility for building decreasing diagrams: in particular the steps between u and t in Figure 4.4 could be red as well as blue in this case. An interesting question is whether our approach is compatible with a more flexible schema for labelling plain and parallel steps.

Theorem 4.4.12. *A first-order term rewrite system R is confluent if all its parallel red/blue subterm critical pairs, plain blue/red subterm critical pairs and top critical pairs are decreasing.*

Proof. We simply need to verify the axioms and apply Theorem 4.4.8. □

4.4.2 When Plain Critical Pairs Suffice

The question we now investigate is whether parallel critical pairs are really needed, or if plain critical pairs are enough. This question has received quite a lot of attention in the past [Hue80, Toy88] under the name of parallel-closedness. Proofs all follow the same proof pattern introduced by Huet, by induction via a quite smart well-founded order. We will show how to obtain it, and generalize it, in van Oostrom's coloured labelled framework, therefore hiding this smart induction within the use of the novel multi-labelling technique. We shall as before state and prove our result at the abstract level of labelled rewrite relations, therefore making it available to a wider range of rewriting applications.

In this subsection, we use $\widetilde{\Sigma}$ to denote heterogeneous sequences consisting of domains and sets of pairwise parallel domains, since an arbitrary conversion $\twoheadleftarrow\!\!\!\twoheadrightarrow_{\widetilde{\Sigma}}$ may contain both (plain) blue steps and (parallel) red steps at the same time. We write $\widetilde{\Sigma}\#\Gamma$ if $((\forall P_p \in \widetilde{\Sigma})\, P_p\#\Gamma) \wedge ((\forall \Pi \in \widetilde{\Sigma})\, \Pi\#\Gamma)$, $\widetilde{\Sigma} \geq_{\mathcal{P}} p$ if $((\forall P_p \in \widetilde{\Sigma})\, P_p \geq_{\mathcal{P}} p) \wedge ((\forall \Pi \in \widetilde{\Sigma})\, \Pi \geq_{\mathcal{P}} p)$. We also use specific color to denote components or properties of steps in that specific color, for example, $s \twoheadleftarrow\!\!\!\twoheadrightarrow^{\alpha}_{\widetilde{\Sigma}} t$ meaning α is the sequence of labels of red steps in $s \twoheadleftarrow\!\!\!\twoheadrightarrow_{\widetilde{\Sigma}} t$. All related abbreviations come as expected.

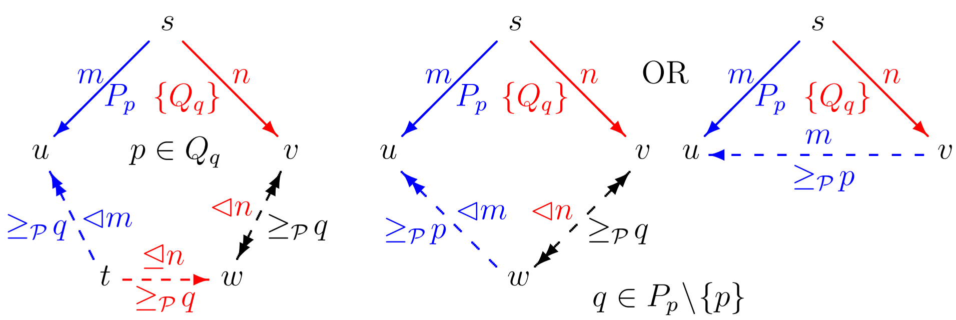
We need a lemma blending Lemma 4.4.2 with Lemma 4.4.3 before to show the main result.

Lemma 4.4.13. *Given conversion $u \twoheadleftarrow\!\!\twoheadrightarrow^{\alpha}_{\widetilde{\Sigma}} s \to^{n}_{\Pi} v$ such that $\widetilde{\Sigma}\#\Pi$, then $u \to^{n'}_{\Pi} t \twoheadleftarrow\!\!\twoheadrightarrow^{\alpha}_{\widetilde{\Sigma}} v$ for some t, n', with $n' \trianglelefteq n$.*

Proof. By induction on the number of steps in $u \twoheadleftarrow\!\!\twoheadrightarrow^{\alpha}_{\widetilde{\Sigma}} s$ and application of the axiom for disjoint peaks, Lemma 4.1.4 and our assumptions on labels. □

The main result of this section states that decreasingness of plain critical peaks implies the Church-Rosser property of rewriting:

Theorem 4.4.14. *A labelled positional rewrite relation satisfying, (i) our assumptions on labels and (ii) the axioms for disjoint and left-linear ancestor peaks, is coloured Church-Rosser, hence confluent, if its plain critical peaks enjoy the following local diagrams in Figure 4.6:*



(i) Plain Red/Blue Critical Peaks (ii) Plain Blue/Red Critical Peaks

Figure 4.6: Assumptions for (Left-Linear) Plain Critical Peaks

Proof. We apply Theorem 4.1.11 with two labels. To this end, we define an appropriate labelling for the rewrite steps before to analyze the local peaks.

We (re-) label the plain step $s \to^{m}_{P_p} t$ by the sequence $[m, 0]$, and the parallel step $s \to^{m}_{\Pi} t$ by $[m, |\Pi|]$ where $|\Pi|$ denotes the size (that is, cardinality) of the set Π. These labels for plain and parallel rewriting have the following structure: the first label remains the same as the original one in $\mathcal{L}$, and is compared in the order $\trianglerighteq$, while the second label is a natural number, which is compared in the familiar order $>$ on natural numbers.

The first label satisfies our assumptions on labels – in particular, the (first) label for parallel rewrites is strictly larger than the (first) label for plain rewrites –, the axioms for disjoint and left-linear ancestor peaks, and the assumptions for plain critical peaks. The second label will be used in case the first fails to conclude. It turns out that it does not need to satisfy (and actually does not satisfy) the axioms and assumptions that are required from the first. Theorem 4.1.11 allows us to use a sequence of labels possibly satisfying different assumptions, which is impossible with Theorem 4.1.5 even if grouping different labels as a single tuple of labels.

In the sequel, we shall omit the second label when the first allows to conclude.

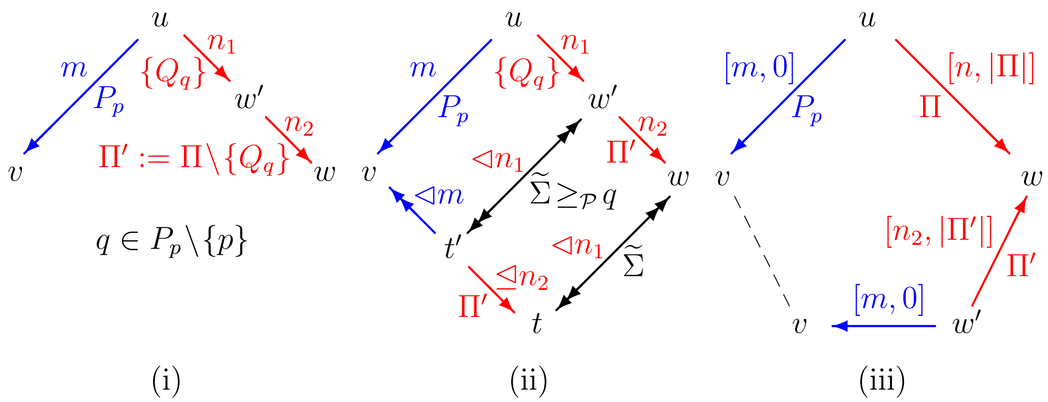
Given a local peak $v \;{}^{[m,0]}_{P_p}\!\!\leftarrow u \rightarrow^{[n,|\Pi|]}_{\Pi} w$, we distinguish three cases:

1. $(\forall Q_q \in \Pi)\, P_p \bowtie Q_q$. Using the first label, Lemma 4.4.4 concludes this case.

2. $(\exists Q_q \in \Pi)\, p \in Q_q$. The proof is similar to Case 3 of the proof of Theorem 4.4.5, using Lemma 4.4.13 instead of Lemma 4.4.2 and 4.4.3.

3. $(\exists Q_q \in \Pi)\, q \in P_p \setminus \{p\}$. As shown in Figure 4.7 (i), we first select $Q_q \in \Pi$ such that $q \in P_p \setminus \{p\}$ and split the local peak into $v \;{}^{m}_{P_p}\!\!\leftarrow u \rightarrow^{n_1}_{\{Q_q\}} w' \rightarrow^{n_2}_{\Pi'} w$ according to Lemma 4.1.4, where $\Pi' := \Pi \setminus \{Q_q\}$. Since $n = sup\{n_1, n_2\}$ by assumption on labels, we get $n_1 \trianglelefteq n, n_2 \trianglelefteq n$. By assumption, we have either $v \;{}^{\alpha}\!\!\twoheadleftarrow t' \twoheadleftarrow\!\!\!\twoheadrightarrow^{\beta}_{\widetilde{\Sigma}} w'$ for some $t', \alpha, \beta, \widetilde{\Sigma}$ with $\alpha \lhd m$, $\beta \lhd n_1$ and $\widetilde{\Sigma} \geq_{\mathcal{P}} q$, or $v \;{}^{m}\!\!\leftarrow w'$. The proof for the former case is represented in Figure 4.7 (ii). Since $\widetilde{\Sigma} \geq_{\mathcal{P}} q$, $\widetilde{\Sigma} \# \Pi'$, hence $t' \rightarrow^{n_2'}_{\Pi'} t \twoheadleftarrow\!\!\!\twoheadrightarrow^{\beta}_{\widetilde{\Sigma}} w$ for some t, n_2' with $n_2' \trianglelefteq n_2$ by Lemma 4.4.13. It then results in a decreasing diagram (using the first label only) shown in the figure. In the latter case, the conversion $v \;{}^{[m,0]}\!\!\leftarrow w' \rightarrow^{[n_2,|\Pi'|]}_{\Pi'} w$ is either decreasing for the first label if $n_2 \lhd n$, or is fixed for the first label by Lemma 4.1.9 while decreasing for the second, as displayed at Figure 4.7 (iii), which concludes the whole proof. □

Following Felgenhauer [Fel13a], the right diagram of Figure 4.6 (ii) can probably be relaxed by adding extra blue steps from v at arbitrary positions larger than q. We have not yet succeeded capturing this improvement in our setting.



The black dashed lines here relate two copies of a same term in order to make the picture look better.

Figure 4.7: Proof of Theorem 4.4.14, Case 3

Now we can turn our attention to concrete first-order rewrite systems, using the above abstract result to prove Toyama's generalization [Toy88] of Huet's parallel closedness criterion [Hue80, Lemma 3.3]. We still use two kinds of rewrite relations: the original one as blue, and the parallel one as red.

Lemma 4.4.15 ([Toy88])**.** *A left-linear term rewrite system R is confluent if for every plain subterm critical pair $\langle u, v\rangle$ we have $v \rightarrow u$, and for every top critical pair $\langle u, v\rangle$ we have $v \rightarrow t \twoheadleftarrow u$ for some t.*

Proof. We label a plain step $v \leftarrow u$ rewritten at position p by $\langle 0, |w|\rangle$ where $w = v|_p$, and all parallel steps by tuple $\langle 1, 0\rangle$. Then to apply Theorem 4.4.14, we need to verify the assumptions on labels and the axioms on peaks. □

Toyama's proof is very different, based on a slight generalization of Hindley–Rosen's Lemma that we already alluded to. As a result, it is much more involved. A further advantage of our proof, using colours and labels, is that it makes clear the origin of these different criteria for top and subterm critical pairs. We are indeed very surprised that Toyama was able to come up with the right condition using Huet's proof technique. Here, it follows quite naturally from the distinction between two sorts of plain critical peaks.

Our proof technique actually shows that it is possible to generalize a little bit Toyama's condition for top critical pairs, as we do now.

Definition 4.4.16. A rewrite rule $l \to r$ is called *size-increasing* if $(\forall x \in \mathcal{V}ar(l))\, \#_x(l) \leq \#_x(r)$ and $|l| \leq |r|$. Given a term rewrite system R, we denote by $R_{s\uparrow}$ its maximum subset of size-increasing rules, and by $\to_{R_{s\uparrow}}$ the corresponding rewrite steps.

Lemma 4.4.17. *A left-linear term rewrite system R is confluent if for every plain subterm critical pair $\langle u, v\rangle$ we have $v \to u$, and for every top critical pair $\langle u, v\rangle$ we have $v \ {}^{(\neq\Lambda)^*}_{R_{s\uparrow}}\!\twoheadleftarrow t' \ {}^{(\neq\Lambda)^*}\!\twoheadleftarrow t \to w \twoheadleftarrow u$ for some t, t', w provided the rewrite positions of $t' \ {}^{(\neq\Lambda)^*}\!\twoheadleftarrow t$ are pairwise disjoint.*

In fact, there are various ways to generalize Toyama's condition, based on our proof technique, using in particular variations of the size-increasing notion. We however prefer the present notion, which is clear and simple enough, and leave the possible variations to the interested reader.

4.5 Conclusion

In this chapter, we have described a general framework for proving confluence (actually Church-Rosser) properties of rewrite systems. Our approach is axiomatic, in the sense that we hide the term structure as long as possible, and derive concrete results from the abstract ones by first verifying the axioms and then instantiating the abstract conditions.

This abstract framework is based on a generalization of the decreasing diagrams approach which turns local labels into global measures on proofs by defining appropriate orders on conversions. It further blends this framework with the abstract notion of positions recently introduced by Jouannaud and Li. Thanks to the abstract notion of positions, we can reduce Church-Rosser properties of abstract rewrite relations to simple labelling properties of certain local peaks called critical. Thanks to the use of several labels, we can use complex inductive arguments which are actually hidden in the order used on conversions. Finally, the use of colours to generalize the Church-Rosser property allows us to encode and simplify old techniques based on the use of parallel rewriting to study the properties of plain rewriting.

We have devoted limited effort to instantiate our abstract results to concrete cases, since these instantiations are mostly straightforward in the plain rewriting setting. These simple technicalities should of course be carried out carefully in future work. Indeed, our ultimate goal is to capture the entire field of confluence (or Church-Rosser) proofs with a single abstract theorem reducing the Church-Rosser property of a NARS to the existence of decreasing diagrams for its critical peaks, classified with respect to the three manageable sub-components of NARSes, the terminating, linear non-terminating, and left-linear non-terminating ones.

The case of conditional rewriting is another potential subject for future work. However, since conditions serve filtering out critical pairs instances, this issue is somehow orthogonal to our effort. In this respect, the general case of NARSes is more important to us. This is the direction we want to investigate first. Such a result could become the basis of a very general implementation in which different concrete cases would be implemented via appropriate plug-ins.

Five

Confluence of Rewrite Unions

We have already shown the power of decreasing diagrams on abstract rewriting, an abstract level, and abstract positional rewriting, a slightly more concrete level. It is time to move our focus onto concrete term rewrite systems.

With termination, Knuth and Bendix [KB70] followed by Huet [Hue80] proved that confluence can be reduced to joinability of critical pairs. The basis of this result at the abstract level, Newman's Lemma, has been captured by the decreasing diagrams framework. On the other hand, Felgenhauer succeeded in reducing confluence of left-linear rewrite systems to the existence of decreasing diagrams of *parallel critical pairs* [Toy81, Gra96], without termination assumption [Fel13b]. It is our ambition to develop a criterion based on critical pair capturing both situations together.

In [JvO09], the decreasing diagrams method is applied to concrete term rewrite systems, opening a way to an analysis of non-terminating rewrite systems in terms of the joinability of their critical pairs. The idea is to split the set of rules into a set R_T of terminating rules and a set R_{NT} of non-terminating ones. While left-linearity is required from R_{NT} as shown by simple examples, it is not from R_T.

In this chapter, following the idea from [JvO09], we deliver the first true generalization of Knuth–Bendix test to rewrite systems made of two subsets, R_T of terminating rules and R_{NT} of possibly non-terminating, rank non-increasing, left-linear rules. The main idea of our approach is to reduce confluence – via decreasing diagrams – to joinability of the finitely many *critical pairs* of rules in R_T within rules in $R_T \cup R_{NT}$ and the finitely many *rigid parallel critical pairs* of rules in R_{NT} within rules in $R_T \cup R_{NT}$. The result is obtained thanks to a new notion, *sub-rewriting*, which appears as the key to glue together many concepts that appeared before in the study of termination and confluence of union systems, namely: caps and aliens, rank non-increasing rewrites, parallel rewriting, decreasing diagrams, stable terms, and constructor-lifting rules. This culminates with the discussion on a mysterious example raised by Huet [Hue80], which is a critical-pair-free, non-terminating, non-confluent system. We show that the computation of critical pairs should then involve unification over infinite rational trees, and then, indeed, Huet's example is no longer critical-pair-free.

Organization. Section 5.2 is devoted to the main result and its proof. We generalize this result in Section 5.3. Relevant literature is analyzed in Section 5.4.

5.1 Rewriting and Decomposition

In this chapter, we assume a set of variables $\mathcal{Y}$ disjoint from $\mathcal{X}$ and a bijective mapping ξ from the set of positions to $\mathcal{Y}$. Given $F \subseteq \mathcal{F}$, a term t is called *F-headed* if $t(\Lambda) \in F$. The notion extends to substitutions.

5.1.1 Rewriting

Our goal is to reduce the Church-Rosser property of the union of a terminating rewrite relation R_T and a non-terminating relation R_{NT} to that of finitely many critical pairs. The particular case where R_{NT} is empty was carried out by Knuth and Bendix and is based on Newman's Lemma stating that a terminating relation is Church-Rosser if and only if its local peaks are joinable. The other particular case, where R_T is empty, was considered by Orthogonality and is based on Hindley–Rosen's Lemma stating that a (non-terminating) relation is Church-Rosser provided its local peaks are strongly joinable. The general case requires using both, which has been made possible by van Oostrom, who introduced decreasing diagrams to replace joinability.

We first introduce our notion of parallel rewriting:

Definition 5.1.1. Given a term rewrite system R, a term u *rewrites in parallel (rigidly)* to v *at* a set $P = \{p_i\}_1^n$ of pairwise disjoint positions with rule $l \to r \in R$, written $u \Rightarrow_{l\to r\in R}^{P} v$, if $(\forall p_i \in P)\, u|_{p_i} = l\sigma_i$ and $v = u[r\sigma_1, \ldots, r\sigma_n]_P$. The term $l\sigma_i$ is a *redex*. We may omit P, R or $l \to r$, and replace P by a property that it satisfies.

We call our notion of parallel rewriting *rigid*. It departs from the literature [Hue80, ZFM15] by imposing the use of a *single* rule. The idea of using single rule in parallel rewriting has appeared in [vO08a, Theorem 6]. Rigid parallel rewriting extends naturally to lists of terms of the same length, hence to substitutions of the same domain.

Plain (term) rewriting introduced in Chapter 2 is actually obtained as the particular case of parallel rewriting when $n = 1$. We then still use the usual notation $u \to_{l\to r\in R}^{p} v$ when rewriting is plain. As a consequence, most of the following definitions given for parallel rewriting will degenerate into corresponding plain versions, which have been introduced in Chapter 2, when $n = 1$.

Consider two parallel rewrites issuing from the same term u with possibly different rules, say $u \Rightarrow_{l\to r}^{P} v$ and $u \Rightarrow_{g\to d}^{Q} w$. Following Huet [Hue80], we distinguish three cases,

$P\#Q$, that is, $(\forall p \in P)(\forall q \in Q)\, p\#q$; (disjoint case)

$P = \{p\}$, $Q >_{\mathcal{P}} p \cdot \mathcal{FP}os(l)$; (ancestor case)

$P = \{p\}$, $Q \subseteq p \cdot \mathcal{FP}os(l)$; (critical case)

all other cases being a combination of the above three.

Definition 5.1.2 (Rigid Parallel Critical Pairs)**.** Given a rule $l \to r$, a set $P = \{p_i \in \mathcal{FP}os(l)\}_1^n$ of disjoint positions and n copies $\{g_i \to d_i\}_1^n$ of a rule $g \to d$ sharing no variable among themselves nor with $l \to r$, such that

σ is a most general unifier of the terms $l, g_1, \ldots, g_n$ at P. Then $l\sigma$ is the *overlap* and $\langle r\sigma,\, l\sigma[d_1\sigma, \ldots, d_n\sigma]_P\rangle$ the *rigid (parallel) critical pair* of $g \to d$ on $l \to r$ at P (a *critical pair* if $n = 1$).

We now lift the parallel rewrite relation to a *labelled parallel rewrite relation*, equipping each rewrite step by a label from $\mathcal{L}$ with a partial quasi-order $\trianglerighteq$ whose strict part $\triangleright$ is well-founded. We write $u \Rightarrow^{P,m}_{l\to r\in R} v$ for a *labelled parallel rewrite step* from u to v at positions P with label m and rule $l \to r \in R$. Indexes $P, m, R, l \to r$ may be omitted, or replaced by properties they satisfy.

5.1.2 Decreasing Diagrams

In this chapter, we will apply the decreasing diagrams method in its directional version, that is Definition 2.2.5. Sometimes the mention of the word "joinably" is omitted for convenience. A notion of stability with respect to contexts and substitutions are needed.

Definition 5.1.3. A (joinably) decreasing diagram D is *stable* if $C[D\gamma]$ is (joinably) decreasing for arbitrary context $C[\cdot]$ and substitution γ.

In this chapter, we will also make a heavy use of Corollary 2.2.12 instead of Theorem 2.2.6. With a different choice of the set T in Corollary 2.2.12, it will be the basis of our main Church-Rosser result to come.

5.1.3 Decomposition

From now on, we assume two signatures $\mathcal{F}_T$ and $\mathcal{F}_{NT}$ satisfying

(A1) $\mathcal{F}_T \cap \mathcal{F}_{NT} = \varnothing$.

and proceed by slicing terms into homogeneous subparts, following definitions in [JT08] and Chapter 3, but with a slightly different notion of cap.

Definition 5.1.4. A term $s \in \mathcal{T}(\mathcal{F}_T \cup \mathcal{F}_{NT}, \mathcal{X})$ is *homogeneous* if it belongs to $\mathcal{T}(\mathcal{F}_T, \mathcal{X})$ or to $\mathcal{T}(\mathcal{F}_{NT}, \mathcal{X})$; otherwise it is *heterogeneous*.

Thanks to assumption (A1), a heterogeneous term can be uniquely decomposed (w.r.t. $\mathcal{Y}$ and ξ) into a topmost homogeneous part, its *cap*, and a multiset of remaining subterms, its *aliens*, headed by symbols of the other signature.

Definition 5.1.5 (Caps, Aliens)**.** Let $t \in \mathcal{T}(\mathcal{F}_T \cup \mathcal{F}_{NT}, \mathcal{X})$. An *alien* of t is a maximal non-variable subterm of t whose head does not belong to the signature of t's head. We use $\mathcal{A}l\mathcal{P}os(t)$ for its set of (necessarily) pairwise disjoint *alien positions*, $\mathcal{A}(t)$ for its list of aliens from left to right, and $\mathcal{C}a\mathcal{P}os(t) := \{p \in \mathcal{P}os(t) \mid p \not\geq_{\mathcal{P}} \mathcal{A}l\mathcal{P}os(t)\}$ for its set of *cap positions*. We (re-) define the *cap* $\bar{t}$ and *alien substitution* $\overline{\gamma}_t$ of t as follows:

(i) $\mathcal{P}os(\bar{t}) := \mathcal{C}a\mathcal{P}os(t) \cup \mathcal{A}l\mathcal{P}os(t)$;

(ii) $(\forall p \in \mathcal{C}a\mathcal{P}os(t))\ \bar{t}(p) = t(p)$;

(iii) $(\forall p \in \mathcal{A}l\mathcal{P}os(t))\ \bar{t}(p) = \xi(p) \wedge \overline{\gamma}_t(\xi(p)) = t|_p$.

It is worth noting that the caps defined in this chapter are different from those in Chapter 3, in which two variables are identical if and only if their corresponding aliens are identical. In fact, the notion of caps in Chapter 3 corresponds to a notion of *hats* that we will introduced in the next section.

The *rank* of t, denoted $\mathrm{rank}(t)$, remains the same as in Chapter 3 being 1 plus the maximal rank of its aliens.

Fact. *Given $t \in \mathcal{T}(\mathcal{F}_T \cup \mathcal{F}_{NT}, \mathcal{X})$, then $t = \bar{t}\overline{\gamma}_t$.*

Example 5.1.6. Let $\mathcal{F}_T = \{g^3\}$, $\mathcal{F}_{NT} = \{f^3, 0, 1\}$ and a term $t = f(g(0,1,1), g(0,1,x), g(0,1,1))$. Then t has cap $f(y_1, y_2, y_3)$ and aliens $g(0,1,1)$ and $g(0,1,x)$. $g(0,1,1)$ has cap $g(y_1, y_2, y_3)$ and homogeneous aliens 0 and 1, while $g(0,1,x)$ has cap $g(y_1, y_2, x)$ and the same set of homogeneous aliens. Hence, the rank of t is 3.

5.2 From Church-Rosser to Critical Pairs

Definition 5.2.1. A rewrite rule $l \to r$ is *rank non-increasing* if for all rewrites $u \to_{l \to r} v$, $\mathrm{rank}(u) \geq \mathrm{rank}(v)$. A rewrite system is rank non-increasing if all its rules are.

Rank non-increasingness is strongly relevant to our proof technique for the main result, allowing both to apply induction on the rank of terms, and to employ the decreasing diagrams method on subsets of terms with respect to the ranks.

From now on, we assume we are given two rewrite systems R_T and R_{NT} satisfying:

(A2) R_T is a terminating rewrite system in $\mathcal{T}(\mathcal{F}_T, \mathcal{X})$;

(A3) R_{NT} is a set of rank non-increasing, left-linear rules $f(\vec{s}) \to g(\vec{t})$ such that $f, g \in \mathcal{F}_{NT}$ and $\vec{s}, \vec{t} \in \mathcal{T}(\mathcal{F}_T \cup \mathcal{F}_{NT}, \mathcal{X})$;

(A4) if $g \to d \in R_T$ overlaps $l \to r \in R_{NT}$ at $p \in \mathcal{FP}os(l)$, then $l|_p \in \mathcal{T}(\mathcal{F}_T, \mathcal{X})$.

Note that assumption (A3) forbids collapsing rules in R_{NT}.

Our goal is to show that $R_T \cup R_{NT}$ is Church-Rosser provided its critical pairs have appropriate decreasing diagrams.

5.2.1 Proof Strategy

Since R_T and R_{NT} are both rank non-increasing, by assumption for the latter and homogeneity assumption of its rules for the former, we are enabled to prove our result by induction on the rank of terms. To this end, we introduce the set $\mathcal{T}_n(\mathcal{F}_T \cup \mathcal{F}_{NT}, \mathcal{X})$ of terms of rank at most n. Since rewriting is rank non-increasing, $\mathcal{T}_n(\mathcal{F}_T \cup \mathcal{F}_{NT}, \mathcal{X})$ is closed under diagram rewriting with a set of joinably decreasing diagrams. This is why we adopted this restricted form of decreasing diagrams rather than the more general form as in Definition 2.2.4.

We say that two terms in $\mathcal{T}_n(\mathcal{F}_T \cup \mathcal{F}_{NT}, \mathcal{X})$ are *n-($R_T \cup R_{NT}$)-convertible* (in short, *n-convertible*) if their conversion involves terms in $\mathcal{T}_n(\mathcal{F}_T \cup \mathcal{F}_{NT}, \mathcal{X})$ only. We shall assume that n-($R_T \cup R_{NT}$)-convertible terms are joinable, and show that $(n+1)$-($R_T \cup R_{NT}$)-convertible terms are joinable as well by exhibiting joinably decreasing diagrams for all their local peaks, using Corollary 2.2.12.

Since R_{NT} may have non-linear right-hand sides, we adopt the trick from [vO08a] to use parallel rewriting with R_{NT}-rules to enable the existence of decreasing diagrams for ancestor peaks in case R_{NT} is below R_{NT}. The main difficulty, however, has to do with ancestor peaks $v \;{}_{R_{NT}}\!\!\overset{q}{\leftarrow} u \rightarrow^{p}_{R_T} w$ for which R_{NT} is below R_T. Due to non-left-linearity of the rules in R_T, the classical diagram for such peaks, $v \twoheadrightarrow_{R_{NT}} s \rightarrow^{p}_{R_T} t \;{}_{R_{NT}}\!\!\twoheadleftarrow w$, can hardly be made decreasing in case $s \rightarrow^{p}_{R_T} t$ must be a facing step, since the side steps $v \twoheadrightarrow_{R_{NT}} s$ are usually with labels identical to that of the top R_{NT}-step. One way out is to make the labels of R_T-steps strictly larger than those of R_{NT}-steps, which will cause problems in ancestor peaks $v \;{}_{R_{NT}}\!\!\overset{q}{\leftarrow} u \rightarrow^{p}_{R_T} w$ where R_T is below R_{NT}. Another way out is to group them together as a single facing step from v to t. To this end, we introduce a specific rewrite relation:

Definition 5.2.2 (R_T-Sub-Rewriting)**.** A term u R_T*-sub-rewrites* (*sub-rewrites* for short) to v at $p \in \mathcal{P}os(u)$ with $l \rightarrow r \in R_T$, written $u \rightarrow^{p}_{R_{Tsub}} v$ if the following conditions hold:

(i) $\mathcal{FP}os(l) \subseteq \mathcal{C}a\mathcal{P}os(u|_p)$;

(ii) $u \twoheadrightarrow^{\geq_{\mathcal{P}} p \cdot \mathcal{A}l\mathcal{P}os(u|_p)}_{R_T \cup R_{NT}} w = u[l\sigma]_p$;

(iii) $v = u[r\sigma]_p$.

Condition (ii) allows *arbitrary rewriting* in $\mathcal{A}(u|_p)$ until an R_T-redex is obtained. Thanks to assumptions (A1–3), these aliens remain aliens along the derivation from u to w, implying (i). Condition (i) will however be needed later when relaxing assumptions (A1) and (A3). Note also that the cap of $w|_p$ may collapse in the last step, in which case $v|_p$ becomes $\mathcal{F}_{NT}$-headed.

5.2.2 A Hierarchy of Decompositions

R_T-sub-rewriting suggests another notion of cap for $\mathcal{F}_T$-headed terms. Let ζ_n be a bijective mapping from $\mathcal{Y} \cup \mathcal{X}$ to n-$(R_T \cup R_{NT})$-convertibility classes of terms in $\mathcal{T}(\mathcal{F}_T \cup \mathcal{F}_{NT}, \mathcal{X})$, which is the identity on $\mathcal{X}$. The rank of a term being at least one, 0-$(R_T \cup R_{NT})$-convertibility does not identify any two different terms; hence ζ_0 is a bijection from $\mathcal{Y} \cup \mathcal{X}$ to $\mathcal{T}(\mathcal{F}_T \cup \mathcal{F}_{NT}, \mathcal{X})$. Similarly we denote by ζ_∞ a bijective mapping from $\mathcal{Y} \cup \mathcal{X}$ to $(R_T \cup R_{NT})$-convertibility classes, abbreviated as ζ.

Definition 5.2.3 (Hats)**.** The *hat at rank* n of a term $t \in \mathcal{T}(\mathcal{F}_T \cup \mathcal{F}_{NT}, \mathcal{X})$ is the term $\widehat{t}^n$ defined as:

- if t is $\mathcal{F}_{NT}$-headed, $\widehat{t}^n = \zeta_n^{-1}(t)\,$;
- otherwise, $(\forall p \in \mathcal{C}a\mathcal{P}os(t))\ \widehat{t}^n(p) = \bar{t}(p)$ and
  $(\forall p \in \mathcal{A}l\mathcal{P}os(t))\ \widehat{t}^n(p) = \zeta_n^{-1}(t|_p)\,.$

Since n-$(R_T \cup R_{NT})$-convertibility is an infinite hierarchy of equivalences identifying more and more terms, given t, $\{\widehat{t}^i\}_i$ is an infinite sequence of terms, each of them being an instance of the previous one, which is stable from some index n_t. We use $\widehat{t}$ for $\widehat{t}^\infty$. Note that we overload here the notation which is used in Chapter 3 for caps.

Lemma 5.2.4. *Let $t \in \mathcal{T}(\mathcal{F}_T \cup \mathcal{F}_{NT}, \mathcal{X})$ and $m \geq n \geq 0$. Then $\widehat{t} \trianglerighteq \widehat{t}^m \trianglerighteq \widehat{t}^n \trianglerighteq \bar{t}$.*

The associated variable substitution from $\widehat{t}^n$ to $\widehat{t}^m$ is $\xi_{n,m}$, omitting m when infinite.

Note that $\xi_{n,m}$ does not actually depend on the term t, but only on the m- and n-convertibility classes. Also, $\widehat{t}^0$ corresponds to the case where identical terms only are identified by ζ_0^{-1}, while $\widehat{t}$ corresponds to the case where any two $(R_T \cup R_{NT})$-convertible terms are identified by ζ^{-1}. In the literature, $\widehat{t}^0$ is usually called a hat (or a cap, which is the case in Chapter 3).

Example 5.2.5. Let $\mathcal{F}_{NT} = \{f^3\}, \mathcal{F}_T = \{g^3, 0, 1\}$ and $R_T = \{1 \to 0\}$. Then, $g(f(1,0,x), f(1,0,x), 1) \to^{2\cdot 1}_{1\to 0} g(f(1,0,x), f(0,0,x), 1)$. 0-hats of these terms are $g(y,y,1)$ and $g(y,y',1)$, respectively. Their 1-hats are the same as their 0-hats, since their aliens have rank 2, hence cannot be 1-convertible. On the other hand, their $(i \geq 2)$-hats are $g(y,y,1)$ and $g(y,y,1)$, since $f(1,0,x)$ and $f(0,0,x)$ are 2-convertible.

We have the following lemmas, with $\zeta_t = \zeta_{0|\mathcal{V}ar(\widehat{t}^0)}$.

Lemma 5.2.6. *Let $t \in \mathcal{T}(\mathcal{F}_T \cup \mathcal{F}_{NT}, \mathcal{X})$. Then $t = \widehat{t}^0\zeta_t$.*

Lemma 5.2.7. *Let* $u \rightarrow^{p}_{R_T} v$*,* $p \in \mathcal{C}a\mathcal{P}os(u)$*. Then* $\widehat{u}^0 \rightarrow^{p}_{R_T} \widehat{v}^0$ *and* $(\forall y \in \mathcal{V}ar(\widehat{v}^0))\, \zeta_u(y) = \zeta_v(y)$*.*

Lemma 5.2.8. *Let* $u(\Lambda) \in \mathcal{F}_T$ *and* $u \rightarrow^{p}_{R_T \cup R_{NT}} v$ *at* $p \geq_{\mathcal{P}} \mathcal{A}l\mathcal{P}os(u)$*. Then* $\mathcal{C}a\mathcal{P}os(u) = \mathcal{C}a\mathcal{P}os(v)$*,* $(\forall q \in \mathcal{C}a\mathcal{P}os(u))\, u(q) = v(q)$*,* $\mathcal{A}l\mathcal{P}os(u) = \mathcal{A}l\mathcal{P}os(v)$*,* $(\forall q \in \mathcal{A}l\mathcal{P}os(u))\, u|_q \twoheadrightarrow_{R_T \cup R_{NT}} v|_q$*.*

Main properties of R_T-sub-rewriting are the following:

Lemma 5.2.9. *Let* u *be an* $\mathcal{F}_T$*-headed term of rank* $n+1$ *such that* $u \rightarrow^{\geq_{\mathcal{P}} \mathcal{A}l\mathcal{P}os(u)}_{R_T \cup R_{NT}} v$*. Then,* $(\forall i \geq n)\, \widehat{u}^i = \widehat{v}^i$*.*

Proof. Since both sides of rules in R_{NT} are $\mathcal{F}_{NT}$-headed, $\mathcal{A}l\mathcal{P}os(u) = \mathcal{A}l\mathcal{P}os(v)$. Rewriting using both R_T and R_{NT} in aliens does not change $\mathcal{C}a\mathcal{P}os(u)$, and does not change $(i \geq n)$-convertibility either, hence the statement. ☐

Lemma 5.2.10. *Let* u *be of rank* $n+1$*,* $p \in \mathcal{C}a\mathcal{P}os(u)$*, and* $u \rightarrow^{p}_{R_{Tsub}} v$*. Then,* $(\forall i \geq n)\, \widehat{u}^i \rightarrow^{p}_{R_T} \widehat{v}^i$*.*

Proof. By definition of sub-rewriting, we get $u \twoheadrightarrow^{\geq_{\mathcal{P}} p \cdot \mathcal{A}l\mathcal{P}os(u|_p)}_{R_T \cup R_{NT}} w \rightarrow^{p}_{l \to r \in R_T} v$, therefore $w|_p = l\sigma$ for some substitution σ and $v = w[r\sigma]_p$. Let $i \geq n$.

By Lemma 5.2.7, $\widehat{w}^0 \rightarrow^{p}_{l \to r} \widehat{v}^0$. By repeated applications of Lemma 5.2.8, $\mathcal{C}a\mathcal{P}os(u) = \mathcal{C}a\mathcal{P}os(w)$, $(\forall q \in \mathcal{C}a\mathcal{P}os(u))\, u(q) = w(q)$, and $\mathcal{A}(u)$ rewrites to $\mathcal{A}(w)$; hence aliens in $\mathcal{A}(u)$ are n-convertible if and only if the corresponding aliens in $\mathcal{A}(w)$ are n-convertible. By definition 5.2.3, we get $\widehat{u}^n = \widehat{w}^n$.

Putting things together, $\widehat{u}^i = \widehat{u}^n \xi_{n,i} = \widehat{w}^n \xi_{n,i} = \widehat{w}^0 \xi_{0,n} \xi_{n,i} \rightarrow^{p} \widehat{v}^0 \xi_{0,n} \xi_{n,i} = \widehat{v}^i$. ☐

Definition 5.2.11 (Rewrite Root)**.** The *root* of a rewrite $u \rightarrow^{p}_{R_{Tsub}} v$ is the minimal position, written $\widehat{p}$, such that $(\forall q : p \geq_{\mathcal{P}} q \geq_{\mathcal{P}} \widehat{p})\, u(q) \in \mathcal{F}_T$.

Note that $u|_p$ is a subterm of $u|_{\widehat{p}}$. By monotonicity of rewriting:

Lemma 5.2.12. *Let* $u \rightarrow^{p}_{R_{Tsub}} v$*. Then* $\widehat{u|_{\widehat{p}}} \rightarrow_{R_T} \widehat{v|_{\widehat{p}}}$*.*

5.2.3 Main Result

We assume from here on that rules are indexed, those in R_T by 0, and those in R_{NT} by (non-zero) natural numbers, making R_{NT} into a disjoint union $\{R_i\}_{i\in I}$ where $I \subseteq i > 0$. Having a strictly smaller index for R_T-rules is no harm nor necessity.

Our relations, parallel rewriting with R_{NT} and sub-rewriting with R_T, are labelled by triples made of the rank of the rewritten redex first, the index of the rule used, and – approximately – the hat of the considered redex, ordered by the well-founded order $\rhd := (>, >, \rightarrow^{+}_{R_T})_{lex}$. More precisely,

$u \Rightarrow^{P}_{R_{i>0}} v$ is given label $\langle k, i, \_\rangle$, where $k = max\{\text{rank}(u|_{p_i})\}_{p_i\in P}$;

$u \rightarrow^{q}_{R_{Tsub}} v$ is given label $\langle k, 0, \widehat{u|_{q'}}\rangle$, where $k = \text{rank}(u|_q)$ and q' is the root $\widehat{q}$ of q.

The third component of an R_{NT}-rewrite is never used. The notation $\Rrightarrow$ is used for the reflexive closure of $\Rightarrow$. We require decreasing diagrams for critical pairs to be stable and to satisfy a *variable condition* introduced by Toyama [Toy81], see also [ZFM15]:

Definition 5.2.13. The R_{NT} rigid critical peak $v \;{}_{l\to r}{\overset{\Lambda}{\leftarrow}}\; u \Rightarrow^{Q}_{g\to d} w$ (resp., rigid critical pair $\langle v, w\rangle$) is *naturally decreasing* if it has a stable joinably decreasing diagram in which:

(i) step $s \Rrightarrow^{Q'} s'$ facing $u \Rightarrow^{Q}_{g\to d} w$ uses the same rule $g \to d$ and satisfies $\mathcal{V}ar(s'|_{Q'}) \subseteq \mathcal{V}ar(u|_Q)$;

(ii) step $t \Rrightarrow t'$ facing $u \rightarrow^{\Lambda}_{l\to r} v$ uses the same rule $l \to r$.

Note the variable condition is automatically satisfied for an overlapping at the root.

Definition 5.2.14. The R_{NT}–R_T critical peak $v \;{}_{l\to r\in R_{NT}}{\overset{\Lambda}{\leftarrow}}\; u \rightarrow^{q}_{R_T} w$ (resp., critical pair $\langle v, w\rangle$) is *naturally decreasing* if it has a stable joinably decreasing diagram whose step $t \Rrightarrow^{P} t'$ facing $u \rightarrow^{\Lambda}_{l\to r\in R_{NT}} v$ uses the same rule $l \to r$.

Theorem 5.2.15 (Church-Rosser Unions)**.** *A rewrite union $R_T \cup R_{NT}$ satisfying:*

– *assumptions (A1–4),*

– *R_{NT}–R_T critical pairs are naturally decreasing,*

– *R_{NT} rigid critical pairs are naturally decreasing,*

is Church-Rosser if and only if its R_T critical pairs are joinable in R_T.

Proof. While the "only if" direction is trivial, we are going to prove the "if" direction.

Since $\rightarrow_{R_T \cup R_{NT}} \subseteq (\rightarrow_{R_{Tsub}} \cup \Rightarrow_{R_{NT}})$ and $(\rightarrow_{R_{Tsub}} \cup \Rightarrow_{R_{NT}})^* = \twoheadrightarrow_{R_T \cup R_{NT}}$, $R_T \cup R_{NT}$ is Church-Rosser iff $\rightarrow_{R_{Tsub}} \cup \Rightarrow_{R_{NT}}$ is. By induction on the rank, we therefore show that every local peak $v\,({}_{R_{Tsub}}\!\leftarrow \cup {}_{R_{NT}}\!\Leftarrow)\,u\,(\rightarrow_{R_{Tsub}} \cup \Rightarrow_{R_{NT}})\,w$, where $\mathrm{rank}(u) = n + 1$, enjoys a joinably decreasing diagram, implying confluence on terms of rank $n + 1$ by Corollary 2.2.12.

The proof is divided into three parts according to the considered local peak. Each key case is described by a picture to ease the reading, in which $\rightarrow$, $\rightarrow$ and $\rightarrow$ are used for plain steps with R_T, R_{Tsub} and $R_T \cup R_{NT}$, respectively, while $\rightarrow$ is used for parallel (sometimes plain) steps with R_{NT}. Every omitted case is symmetric to some considered case, or is easily solved by induction in case all rewrites take place in the aliens of u.

1. Consider a local peak $v \; {}^{P,\langle k,i,\_\rangle}_{R_{NT}}\!\!\Leftarrow u \Rightarrow^{Q,\langle m,j,\_\rangle}_{R_{NT}} w$. Following [Fel13b], we carry out first the particular case of a root peak, for which a rule $l \rightarrow r \in R_i$ applies at the root of u.

   a) Root case. Although our labelling technique is different from that of [Fel13b], with ranks playing a prominent role here, the proof can be adapted without difficulty, as described in Figure 5.1. Let $Q_1 := \{q \in Q \mid q \in \mathcal{FP}os(l)\}$. We first split the parallel rewrite from u to w into two successive parallel steps, at positions in Q_1 first, then at positions in $Q_2 = Q \setminus Q_1$. Note that the peak is specialized into ancestor peak when $Q_1 = \varnothing$. The inner part of the figure uses the fact that l unifies at Q_1 with some R_{NT}-rule, yielding a rigid critical peak $\langle v', u', w'\rangle$ of which the peak $\langle v, u, w'\sigma\rangle$ is a σ-instance. By assumption, $\langle v', w'\rangle$ has a stable diagram which is instantiated by σ in the figure. Since

$Q_1 \cup Q_2$ are pairwise disjoint positions and $Q_2 >_{\mathcal{P}} \mathcal{FP}os(w')$, by left-linearity of R_{NT}, $w'\sigma \Rightarrow^{Q_2}_{R_j} w'\sigma' = w$. Now, we can pull that parallel rewrite from $w'\sigma$ to $s'\sigma$ as indicated, using stability and monotonicity of rewriting, thereby making ancestor redexes commute.

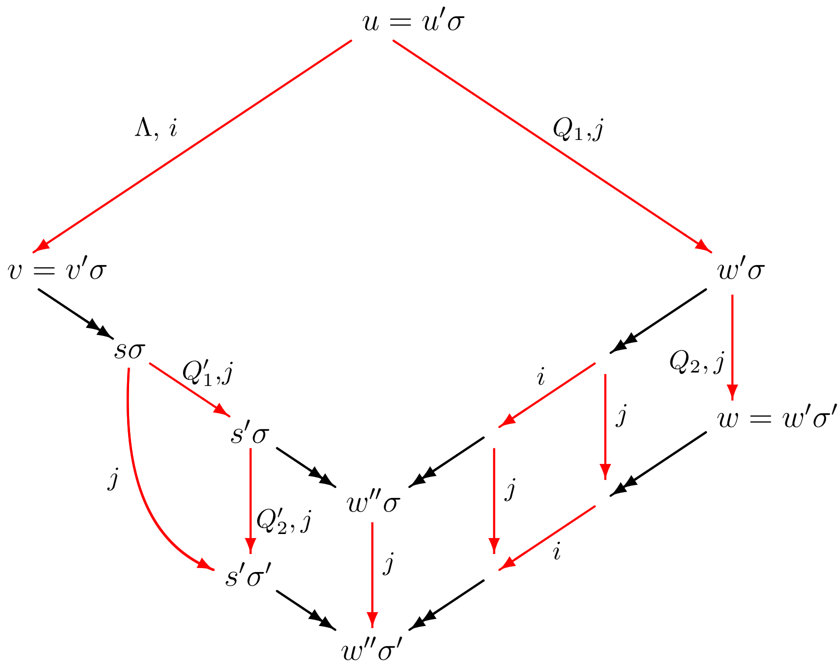


Figure 5.1: R_{NT} Root Peak

Finally, Toyama's variable condition ensures that Q'_1 and Q'_2 are disjoint sets of positions; hence $s\sigma$ rewrites to $s'\sigma'$ in one parallel step with the same j-rule as $u \Rightarrow w$. The obtained diagram is decreasing as a consequence of stability of the rigid critical pair diagram and rank non-increasingness of rewrites.

b) For the general case, we proceed again as in [Fel13b]. For every position $p \in min(P \cup Q)$, the peak $v \; {}^{P,\langle k,i,\_\rangle}_{R_{NT}}\!\!\Leftarrow u \Rightarrow^{Q,\langle m,j,\_\rangle}_{R_{NT}} w$ induces a root peak $v|_p \; {}^{P',\langle k',i,\_\rangle}_{R_{NT}}\!\!\Leftarrow u|_p \Rightarrow^{Q',\langle m',j,\_\rangle}_{R_{NT}} w|_p$. As just shown, root peaks have decreasing diagrams; hence, for each p, we have a decreasing diagram between $v|_p$ and $w|_p$. Notice that in the decreasing diagram we have shown, each facing step – if it exists – uses the same rule as that one it faces. Since positions in $min(P \cup Q)$ are pairwise disjoint, these decreasing diagrams combine into a single decreasing diagram: in particular, the facing steps $\Rightarrow^{\langle m',j,\_\rangle}_{R_{NT}}$ (resp., ${}^{\langle k',i,\_\rangle}_{R_{NT}}\Leftarrow$) yield the facing step $\Rightarrow^{\langle m,j,\_\rangle}_{R_{NT}}$ (resp., ${}^{\langle k,i,\_\rangle}_{R_{NT}}\Leftarrow$).

2. Consider a local peak $v \ {}^{p,\langle k,0,\widehat{u|_p}\rangle}_{R_{Tsub}}\!\leftarrow u \rightarrow^{q,\langle m,0,\widehat{u|_q}\rangle}_{R_{Tsub}} w$. We denote by $l \rightarrow r$ and $g \rightarrow d$ the R_T-rules applied from u to v at p and u to w at q, respectively. We discuss cases depending on $p, \widehat{p}, q, \widehat{q}$, instead of only p, q as usual.

   a) Disjoint case: $p\#q$. The usual commutation lemma yields $v \rightarrow^{q,\langle m,0,\widehat{v|_q}\rangle}_{R_{Tsub}} t \ {}^{p,\langle k,0,\widehat{w|_p}\rangle}_{R_{Tsub}}\!\leftarrow w$ for some t. It is decreasing easily by Lemma 5.2.12 or Lemma 5.2.9, decided by comparison between $\widehat{p}$ and $\widehat{q}$.

   b) Root ancestor case: $\widehat{q} >_{\mathcal{P}} p$. By Definition 5.2.11, $m < k$; hence $q \geq_{\mathcal{P}} \mathcal{A}l\mathcal{P}os(u|_{\widehat{p}})$. This case is thus similar to the R_T above R_{NT} ancestor case (Case 3b) considered later, pictured at Figure 5.3.

   c) Ancestor case: $\widehat{q} = \widehat{p}$; hence $k = m$, with $q >_{\mathcal{P}} p \cdot \mathcal{FP}os(l)$. This is the usual ancestor case, within a given layer with respect to the signature change from the root of u. The proof is depicted in Figure 5.2, simplified by taking $p = \Lambda$.

      Using Definition 5.1.5 and Lemma 5.2.6, then, by Definition 5.2.2, the rewrite from $u = \overline{u}\,\overline{\gamma}_u$, to $v = \widehat{v}^0\zeta_v$ (resp., $w = \widehat{w}^0\zeta_w$) factors out through $v' = \widehat{v'}^0\zeta_{v'}$ (resp., $w' = \widehat{w'}^0\zeta_{w'}$). By Lemma 5.2.7, ζ_v and $\zeta_{v'}$ coincide on $\mathcal{V}ar(\widehat{v'}^0)$, and so do ζ_w and $\zeta_{w'}$ on $\mathcal{V}ar(\widehat{w'}^0)$. By Lemma 5.2.8, $\mathcal{A}(u)$ rewrites to both $\mathcal{A}(v')$ and $\mathcal{A}(w')$, hence each alien in $\mathcal{A}(v)$ and $\mathcal{A}(w)$ originates from some in $\mathcal{A}(u)$. It follows that the aliens in $\mathcal{A}(v)$ and $\mathcal{A}(w)$ originating from the same one in $\mathcal{A}(u)$ are n-convertible. For each $y \in \mathcal{V}ar(\widehat{v}^n) \cup \mathcal{V}ar(\widehat{w}^n)$, we choose all aliens of v and w which belong to the n-convertibility class $\zeta^n(y)$, and repeatedly apply induction hypothesis to get

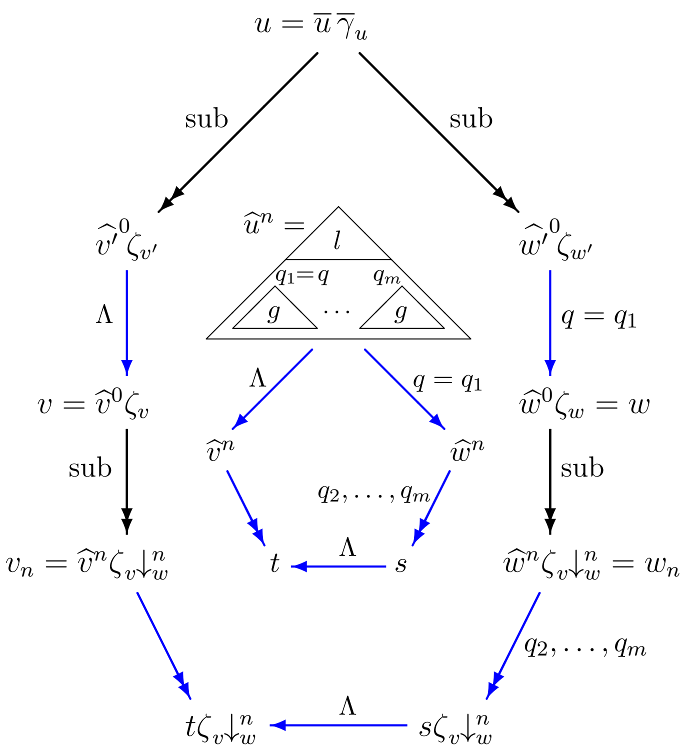


Figure 5.2: R_T Ancestor Peak

a common reduct t_y of them, mapping y to t_y to construct the substitution $\zeta_v\!\downarrow^n_w$. Letting v_n be the term $\widehat{v}^n\zeta_v\!\downarrow^n_w$, v rewrites to v_n. Similarly, w rewrites to w_n. This technique, which we call **equalization**, of equalizing all n-convertible aliens to construct $\zeta_v\!\downarrow^n_w$ is crucial in our proof. The last three steps follow from the inner ancestor diagram between hats of u, v, w, which upper part follows from Lemma 5.2.10 and bottom part from the fact that $q >_{\mathcal{P}} p \cdot \mathcal{FP}os(l)$, resulting in an ancestor peak between homogeneous terms. Such an ancestor peak has an easy stable decreasing diagram, which bottom part can be therefore lifted to the outside diagram. Using Lemmas 5.2.9 and 5.2.12, we can checking that the obtained diagram is decreasing.

d) Critical case: $\widehat{q} = \widehat{p}$; hence $k = m$, with $q \in \mathcal{FP}os(l)$. This is the usual critical case, happening necessarily within same layer. The proof works as in Case 2c, except that the inner diagram is now of a critical peak. Since the R_T critical peak has a joinability diagram by assumption, thanks to stability of rewriting, it can be lifted to the outer diagram, yielding a decreasing diagram for the starting peak.

3. Consider a local peak $v \;{}_{R_{Tsub}}^{p,\langle k,0,\widehat{u|_p}\rangle}\!\!\leftarrow u \Rightarrow_{R_{NT}}^{Q,\langle m,j,\_\rangle} w$. There are three cases.

   a) Disjoint case: $p \# Q$. We get the usual commuting diagram which is decreasing.

   b) Ancestor case. There are two sub-cases: (α) $p >_{\mathcal{P}} Q$; hence $m > k$. Since R_{NT} is left-linear, then $v \Rightarrow_{R_{NT}}^{\langle m',j,\_\rangle} t \;{}_{R_{Tsub}}^{\langle k,0,?\rangle}\!\!\twoheadleftarrow w$ for some t and $m' \leq m$, being a clearly decreasing diagram. (β) $p <_{\mathcal{P}} Q$. This case is a little bit more delicate, since the R_T-rule $l \to r$ used at position p may be non-left-linear. We use equalization as for Case 2c, depicted in Figure 5.3 in the particular case where $p = \Lambda$ for simplicity. The main difference with Case 2c is that the R_{NT}-step must occur in an alien; hence $\widehat{w}^n = \widehat{u}^n$, which somewhat simplifies the figure. Note that thanks to the introduction of R_T-sub-rewriting, the problematic R_{NT}-steps from w to $\widehat{w}^n \zeta_v{\downarrow}_w^n$, which is mentioned in Section 5.2.1, is hidden in a single R_{Tsub}-step directly from w to $\widehat{v}^n \zeta_v{\downarrow}_w^n$.

   c) Critical case. By assumptions (A1–3), $p \in q_i \cdot \mathcal{FP}os(l)$ for some $q_i \in Q$. The proof is depicted at Figure 5.4 with $Q = \{\Lambda\}$ for simplicity, implying a unique redex for that parallel rewrite at the top. Note that the R_T- and R_{NT}-redexes must have different ranks, hence $m > k$.

      By assumption, $u = l\theta \Rightarrow_{l\to r}^{\Lambda} r\theta = w$ and $u \twoheadrightarrow_{R_T \cup R_{NT}}^{\geq_{\mathcal{P}} p \cdot \mathcal{A}l\mathcal{P}os(u|_p)} u[g\theta]_p \to_{g\to d}^{p} v$ for some substitution θ (assuming l and g are renamed apart). The key of the proof is the fact that $u[g\theta]_p = l\theta'$ for some substitution θ' such that $\theta \twoheadrightarrow \theta'$. By assumption (A4), if o is a variable position in g and $p \cdot o \in \mathcal{FP}os(l)$, then $l|_{p\cdot o} \in$

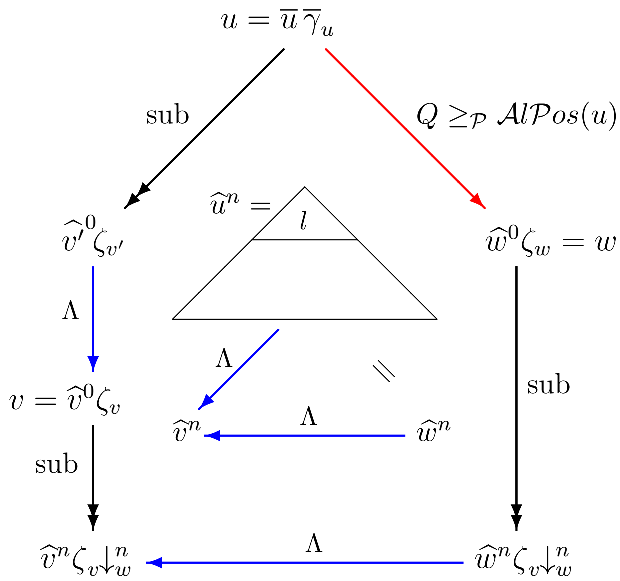


Figure 5.3: R_T above R_{NT} Ancestor Peak

$\mathcal{T}(\mathcal{F}_T, \mathcal{X})$. This indeed ensures that the sub-rewrites from u to v cannot occur at positions in $\mathcal{FP}os(l)$, therefore ensuring the fact $u[g\theta]_p = l\theta'$ since l is linear. It follows that $l\theta'$ rewrites to $r\theta'$ at the root, and to v at $p \in \mathcal{FP}os(l)$, which proves the existence of a critical pair of R_T inside R_{NT}. The rest of the proof is routine, the lifting part being ensured by stability.

To conclude, we simply remark that any two $(R_T \cup R_{NT})$-convertible terms are n-$(R_T \cup R_{NT})$-convertible for some n possibly strictly larger than their respective ranks. $\square$

5.3 Relaxing Assumptions

One must understand that there is no room for relaxing the conditions on R_T and little for R_{NT}. Left-linearity is mandatory, rank non-increasingness as well, and the fact that left-hand sides are headed by symbols which do not belong to $\mathcal{F}_T$ serves avoiding critical pairs of R_{NT} inside R_T. This does

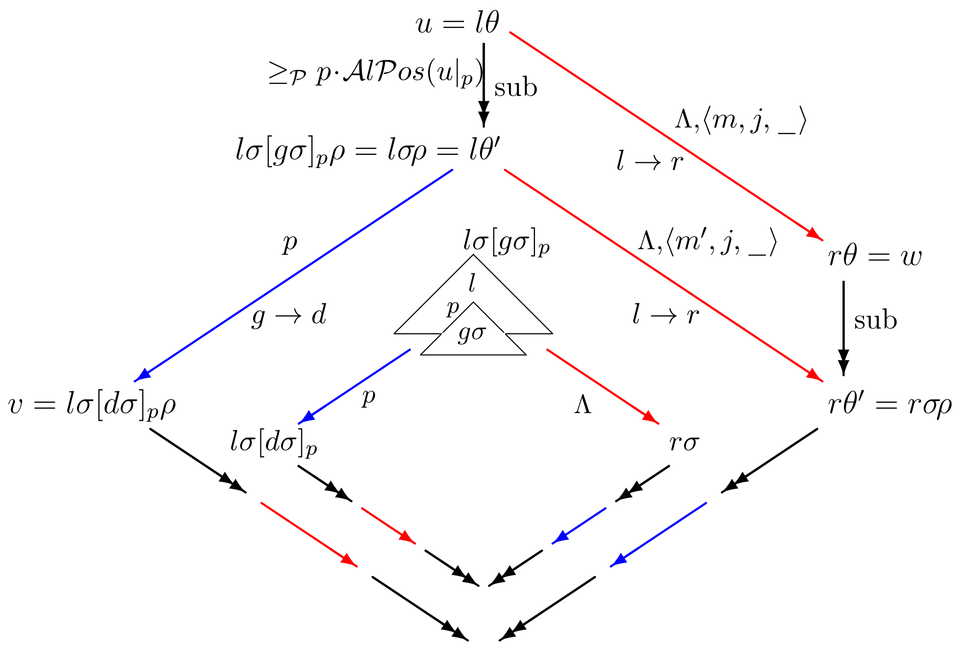


Figure 5.4: R_{NT} above R_T Critical Peak

not forbid left-hand sides to stretch over possibly several layers, making our result very different from known modularity results. Therefore, the only potential relaxations apply to the right-hand sides of R_{NT}-rules, which need not be headed by $\mathcal{F}_{NT}$-symbols, as we assumed to make the proof more comfortable. We will allow them to be headed by some symbols from $\mathcal{F}_T$.

From now on, we replace our assumption (A1) by the following:

(A1') Let $\mathcal{F}_C = \mathcal{F}_T \cap \mathcal{F}_{NT}$ be the set of *constructor symbols* such that no rule in $R_T \cup R_{NT}$ can have an $\mathcal{F}_C$-headed left-hand side.

We use $\mathcal{F}_{T\backslash C}$ and $\mathcal{F}_{NT\backslash C}$ as shorthand for $\mathcal{F}_T \backslash \mathcal{F}_C$ and $\mathcal{F}_{NT} \backslash \mathcal{F}_C$, respectively.

Terms in $\mathcal{T}(\mathcal{F}_C, \mathcal{X})$ are *constructor terms*, trivial ones if in $\mathcal{X}$. The definitions of rank, cap and alien for terms headed by $\mathcal{F}_{T\backslash C}$- or $\mathcal{F}_{NT\backslash C}$-symbols are as before with respect to $\mathcal{F}_T$ and $\mathcal{F}_{NT}$, respectively. An $\mathcal{F}_C$-headed term has its cap and aliens defined with respect to $\mathcal{F}_C$, and its rank is the maximal rank of its aliens, which are headed in $\mathcal{F}_{T\backslash C}$ or $\mathcal{F}_{NT\backslash C}$. The rank of a homogeneous constructor term is therefore 0, which explains why we started with rank 1 before.

Definition 5.3.1. We introduce names for three important categories of terms:
– *type 1*: $\mathcal{F}_{NT\setminus C}$-headed terms, which have a variable as cap and themselves as alien;
– *type 2*: terms u whose cap $\overline{u} \in \mathcal{T}(\mathcal{F}_C, \mathcal{Y})$ and aliens are all $\mathcal{F}_{NT\setminus C}$-headed;
– *type 3*: $\mathcal{F}_{T\setminus C}$-headed terms, whose cap $u \in \mathcal{T}(\mathcal{F}_T, \mathcal{X} \cup \mathcal{Y})$, and aliens are $\mathcal{F}_{NT\setminus C}$-headed.

We also modify our assumption (A3), which becomes:

(A3') R_{NT} is a left-linear, rank non-increasing rewrite system whose rules have the form $f(\vec{l}) \to r$, where $f \in \mathcal{F}_{NT\setminus C}$, $\vec{l} \in \mathcal{T}(\mathcal{F}_T \cup \mathcal{F}_{NT}, \mathcal{X})$ and r is a term of type 2.

The previous assumption (A3) is a particular case of (A3') when r has type 1 $\subseteq$ type 2.

The proof structure of Theorem 5.2.15 depends on layering and labelling. Allowing constructor lifting rules in R_{NT} invalidates Lemmas 5.2.9 and 5.2.10 used to control the label's third component of R_T-sub-rewrite steps, since R_{NT}-rewrites in aliens may now modify the cap of an $\mathcal{F}_T$-headed term. Our strategy is to modify the notion of hat and get analogues of Lemmas 5.2.9 and 5.2.10, making the whole proof work by changing the third component of the label of an R_T-sub-rewrite step. Following [JT08], the idea is to *estimate* the constructors which can pop up at the head of a given $\mathcal{F}_{NT\setminus C}$-headed term, by rewriting it until stabilization.

From here on, we assume the Church-Rosser property for n-convertible terms of rank up to n. Being fixed throughout this section, the rank n will often be left implicit.

5.3.1 Finite Constructor Lifting

Definition 5.3.2. A derivation $s \twoheadrightarrow u$, where s : *type* 1 and u : *type* 2 $\setminus$ *type* 1, is said to be *constructor lifting*. $R_T \cup R_{NT}$ is a *finite constructor* *lifting* rewrite system if for each s of type 1, there exists $n_s \geq 0$ such that for all constructor lifting derivations $s \twoheadrightarrow u$, $|\overline{u}| \leq n_s$ holds.

Definition 5.3.3 (Stable Terms)**.** A term whose multiset M of aliens only contains $\mathcal{F}_{NT\setminus C}$-headed terms is *stable* if M is stable. A multiset M of $\mathcal{F}_{NT\setminus C}$-headed terms is *stable* if

(i) reducts of terms in M are $\mathcal{F}_{NT\setminus C}$-headed;

(ii) any two convertible terms in M are equal.

Example 5.3.4. Let $\mathcal{F}_T = \{g^3, 0, 1\}$, $\mathcal{F}_{NT} = \{f^3\}$, $R_T = \{g(x, x, y) \to y,$ $g(x, y, x) \to y,\ g(y, x, x) \to y,\ 1 \to 0\}$, $R_{NT} = \{f(0, 1, x) \to f(x, x, x),$ $f(1, 0, x) \to f(x, x, x),\ f(0, 0, x) \to f(x, x, x)\}$.
Then, $u = g(f(0, 1, g(0, 0, 0)), f(0, 0, 0), f(1, 0, 0))$ is not stable since its aliens are all convertible but different. But u rewrites to the stable term $g(f(0, 0, 0), f(0, 0, 0), f(0, 0, 0))$.

From rank non-increasingness and the Church-Rosser assumption, we get:

Lemma 5.3.5. *Let u be a stable term of type 1 such that $u \twoheadrightarrow v$. Then v is a stable term of type 1.*

Lemma 5.3.6. *Let u be a stable term whose aliens are of rank up to n. Then, $(\forall i \leq n)\, \widehat{u}^i = \widehat{u}^0$.*

From now on we assume in this section $R_T \cup R_{NT}$ is finite constructor lifting.

Lemma 5.3.7 (Stabilization)**.** *A term s of type 1, 2, 3, whose aliens have rank up to n, has a stable term t such that $\widehat{t}^n = \widehat{s}^n\theta$ for some constructor substitution θ which depends only on the aliens of s.*

Proof. Let M be a multiset of terms of type 1, and $u \in M$. By assumption (A3'), the set of constructor positions on top can only increase along a derivation from u. Being bounded, it has a maximum. Let v be such a reduct. If v is of type 1, then it is stable. Otherwise, we still need to equalize its convertible aliens, using the Church-Rosser property of terms of rank up to n, and we are done. Applying this procedure to all terms in M, we are left equalizing as above the convertible stable terms which are stable by Lemma 5.3.5. Taking now a term of type 2 or type 3, we apply the procedure to its multiset of aliens, all of which have type 1. The relationship between the hats of s and t is clear: θ is generated by constructor lifting, which is the same for equivalent aliens, hence for equal aliens. $\square$

Lemma 5.3.8 (Structure)**.** *Let s be a term of type 1,2,3 whose aliens have rank up to n, and u, v be two stable terms obtained from s by stabilization. Then, $(\forall i \leq n)\, \widehat{u}^i = \widehat{v}^i$.*

Proof. Let $p \in \mathcal{A}l\mathcal{P}os(s)$. By stabilization $u|_p$ and $v|_p$ are convertible stable terms of type 2. By Church-Rosser assumption, $u|_p \twoheadrightarrow t \twoheadleftarrow v|_p$. Since constructors cannot be rewritten, $u|_p$ and $v|_p$ must have the same constructor cap, thus u, v have the same cap. Since they are stable, two convertible aliens of u (resp., v) must be equal, hence u, v have the same 0-hat. We conclude by Lemma 5.3.6. $\square$

Definition 5.3.9 (Estimated Hats)**.** Let u be a term of type 1,2,3 whose aliens have rank up to n and v a stable term obtained from u by stabilization. The *estimated hat* $\overset{\triangle n}{u}_v$ of u w.r.t. v is the term $\widehat{v}^n$.

By Lemma 5.3.8, the choice of v has no impact on $\overset{\triangle n}{u}_v$, hence we use the short notation $\overset{\triangle}{u}$.

The following two lemmas refine Lemmas 5.2.9 and 5.2.10 respectively, in the sense that if $\mathcal{F}_C = \varnothing$, then they coincide with Lemmas 5.2.9 and 5.2.10, respectively.

Lemma 5.3.10 (Alien Rewriting)**.** *Let u, v be terms of type 3, whose aliens are of rank up to n, such that $u \rightarrow^{\geq_{\mathcal{P}} \mathcal{A}l\mathcal{P}os(u)}_{R_T \cup R_{NT}} v$. Then $\overset{\triangle}{u} = \overset{\triangle}{v}$.*

Proof. Follows from Lemmas 5.3.7 and 5.3.8: any stable term for v is a stable term for u. $\square$

Lemma 5.3.11. *Let u be a term of type 3, whose aliens have rank up to n, such that $u \rightarrow^{p}_{R_{Tsub}} v$ with $p \in \mathcal{C}a\mathcal{P}os(u)$. Then $\overset{\triangle}{u} \rightarrow_{R_T} \overset{\triangle}{v}$.*

Proof. By definition of sub-rewriting, $u \twoheadrightarrow^{\geq_{\mathcal{P}} p \cdot \mathcal{A}l\mathcal{P}os(u|_p)} w \rightarrow^{p}_{R_T} v$. By Lemma 5.3.10, $\overset{\triangle}{u} = \overset{\triangle}{w}$. By Lemma 5.2.10, $\widehat{w}^n \rightarrow^{p}_{R_T} \widehat{v}^n$, and the aliens of v are the aliens of w. Let now w', v' be stable terms obtained from w, v by stabilization, hence $\widehat{w'}^n = \widehat{w}^n\theta_w$ and $\widehat{v'}^n = \widehat{v}^n\theta_v$ by Lemma 5.3.7, where θ_v, θ_w depend only on the aliens of v, w, respectively; hence θ_v and θ_w coincide on $\mathcal{V}ar(\widehat{v}^n) \subseteq \mathcal{V}ar(\widehat{w}^n)$ and $\widehat{v'}^n = \widehat{v}^n\theta_w$. We conclude by stability of rewriting and definition of estimated hats. □

Theorem 5.3.12. *With new assumptions (A1') and (A3'), Theorem 5.2.15 holds in the finite constructor lifting case.*

Proof. Same as for Theorem 5.2.15, with the exception of the cases involving R_{Tsub}-steps in the local peaks, which are modified by using stabilization instead of equalization of terms. □

5.3.2 Infinite Constructor Lifting

This section shows preliminary ideas to solve the infinite constructor lifting case, motivated by a famous rewrite system, which is inspired by an abstract example of Newman, algebraized by Klop and publicized by Huet [Hue80].

Example 5.3.13 (NKH [Hue80])**.** Let $\mathcal{F} = \{f^2, g^0, a^0, b^0, c^1\}$ and NKH $= \{f(x, x) \rightarrow a,\ f(x, c(x)) \rightarrow b,\ g \rightarrow c(g)\}$.

NKH is overlap-free, hence locally confluent by Huet's lemma [Hue80]. However, it enjoys non-joinable non-local peaks such as $a \leftarrow f(c(g), c(g)) \leftarrow f(g, c(g)) \rightarrow b$. If we split NKH into $R_T = \{f(x, x) \rightarrow a,\ f(x, c(x)) \rightarrow b\}$ and $R_{NT} = \{g \rightarrow c(g)\}$, such a peak $a \leftarrow f(c(g), c(g)) \leftarrow f(g, c(g)) \rightarrow b$ can be described by a sub-rewriting local peak $a \;{}_{R_{Tsub}}\!\overset{\Lambda}{\leftarrow} f(g, c(g)) \rightarrow^{\Lambda}_{R_{Tsub}} b$ again. In this sense, NKH is no more overlap-free.

It is easy to see that the only difficult case in the main proof is the elimination of sub-rewriting critical peaks. Consider the critical peak $v \;{}_{l\rightarrow r}\!\overset{\Lambda}{\leftarrow} v' \;{}^{\geq_{\mathcal{P}} \mathcal{A}l\mathcal{P}os(u)}_{R_T \cup R_{NT}}\!\twoheadleftarrow u \twoheadrightarrow^{\geq_{\mathcal{P}} p \cdot \mathcal{A}l\mathcal{P}os(u|_p)}_{R_T \cup R_{NT}} w' \rightarrow^{p}_{g \rightarrow d} w$, $p \in \mathcal{FP}os(l)$ and $l \rightarrow r, g \rightarrow d \in R_T$. To obtain a term instance of l whose subterm at position p is an instance of g, v' and w' must be equalized into a term s whose hat rewrites at Λ with $l \to r$ and at p with $g \to d$ to the hats of the corresponding equalizations of v and w. The heart of the problem lies therefore in equalization which constructs here a solution in the signature of $\mathcal{F}_T$ to $\mathcal{F}_T$-unification problems associated with critical pairs by rewriting in $R_T \cup R_{NT}$. Hence,

Theorem 5.3.14. *With new assumptions (A1') and (A3'), Theorem 5.2.15 holds if R_T critical pairs modulo $R_T \cup R_{NT}$ are joinable in R_T.*

Because sub-rewriting can only equalize aliens, the sole purpose of $(R_T \cup R_{NT})$-unification is to solve *occurs-check* [Col84] failures that occur in the plain unification problem $l|_p = g$.

Definition 5.3.15. Let $l \to r$ and $g \to d$ be two rules in R_T such that g Prolog unifies [Col82] with l at position $p \in \mathcal{FP}os(l)$. Let $\bigwedge_i x_i = s_i \wedge \bigwedge_j y_j = t_j$ be a dag solved form returned by Prolog unification, where $\bigwedge_i x_i = s_i$ is the finite substitution part, and $\bigwedge_j y_j = t_j$ the occurs-check part. Let now σ be the substitution $\{x_i \mapsto s_i\}_i$ and $\tau = \{y_j = t_j\}_j$. Then $\langle r\sigma, l\sigma[d\sigma]_p\rangle$ is a *Prolog critical pair* of R_T, constrained by the occurs-checks τ.

If the critical pairs obtained by Prolog unification are joinable in R_T constrained by the occurs-check equations, then the Church-Rosser property is satisfied:

Conjecture 5.3.16. *With new assumptions (A1') and (A3'), Theorem 5.2.15 holds if R_T critical pairs are joinable in R_T and Prolog critical pairs of R_T are joinable in R_T modulo their occurs-checks.*

Example 5.3.17 (Variation of NKH)**.** Let $R_T = \{f(c(x), x) \to a(x)$, $f(y, c(y)) \to b(y),\ a(x) \to e(x),\ b(y) \to e(c(y))\}$, $R_{NT} = \{g \to c(g)\}$. The unification problem $f(c(x), x) = f(y, c(y))$ results in an empty substitution and the occurs-check equations $\tau = \{x = c(y),\ y = c(x)\}$. The critical pair $\langle a(x), b(y)\rangle$ is then joinable by $a(x) \to e(x) =_\tau e(c(y)) \leftarrow b(y)$ with an application of the constraint τ, as exemplified in Figure 5.5, where $\theta_1 = \{x \mapsto c^n(g)\}, \theta_2 = \{y \mapsto c^m(g)\}$, and $n \leq m + 1$ is assumed.

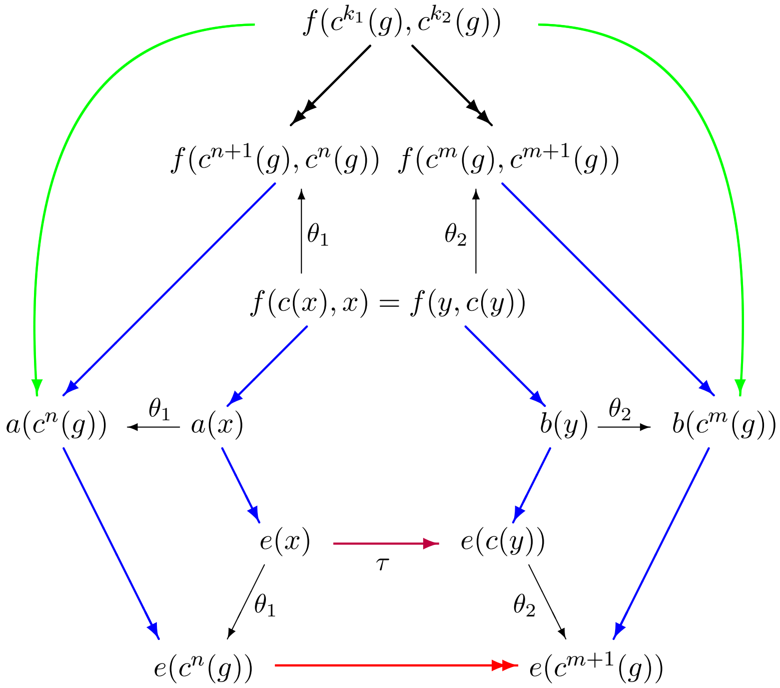


Figure 5.5: Decreasing Diagrams for Example 5.3.17

The idea of Conjecture 5.3.16 is shown in Example 5.3.17 and Figure 5.5. Note that the red bottom steps operate on aliens, hence have small ranks, making the whole joinability diagram decreasing. We have no clear formulation of the converse yet. Confluence is indeed satisfied if the occurs-check is unsolvable, that is, when there exists no $\mathcal{F}_{NT\setminus C}$-headed substitution θ of the y_j's such that $y_j\theta \twoheadleftarrow\!\!\twoheadrightarrow_{R_T \cup R_{NT}} t_j\theta$. We suspect this condition can be reinforced as $y_j\theta \twoheadrightarrow_{R_T \cup R_{NT}} t_j\theta$, possibly leading to interesting sufficient conditions for unsolvability of occurs-checks.

5.4 Related Work

In [JvO09], it is shown that confluence can be characterized by the existence of decreasing diagrams for the critical pairs in $R_T \cup R_{NT}$ provided all rules are linear[1]. This is a particular case of a recent result of Felgenhauer [Fel13b] showing that R_{NT} is confluent if all rules are left-linear and parallel critical pairs have decreasing diagrams with respect to rule indexes used as labels. When $\mathcal{F}_T$ is empty, all terms have rank 1, hence our labels for non-linear rules reduce to his. A difference is that we assume R_{NT}-rules to be non-collapsing. One could argue that collapsing R_{NT}-rules can be moved to R_T, but this answer is not satisfactory for two different reasons: the resulting change of labels may affect the search for decreasing diagrams, and it can also impact condition (A1). A second difference is that we use rigid parallel rewriting, which yields exponentially fewer parallel critical pairs than when allowing parallel steps with different rules of a given index (which we could have done too). The price to pay is having less flexibility for finding decreasing diagrams.

A result of Klein and Hirokawa, generalizing [HM11], extends Knuth and Bendix's critical pair test to relatively terminating systems [KH12]. It is an extension in the sense that it boils down to it when $R_{NT} = \varnothing$. Otherwise, unlike our result, it requires computing critical pairs of R_T *modulo* a confluent R_{NT}, hence modifies the critical pair test for the subset of terminating rules. That is why we call our result a true generalization of Knuth–Bendix test, and theirs a non-true generalization but an extension. Further, the result in [KH12] requires proving relative termination (termination of $\twoheadrightarrow_{R_{NT}} \rightarrow_{R_T} \twoheadrightarrow_{R_{NT}}$), complete unification modulo R_{NT}, and absence of critical pairs between R_T and R_{NT}, all tests implemented in CSI [ZFM11]. This is used to detect that NKH is non-confluent.

Theorem 5.2.15 can be seen as a modularity theorem to some extent, since rewriting a term in $\mathcal{T}(\mathcal{F}_T, \mathcal{X})$ can only involve R_T rules. But left-hand sides of R_{NT} rules may have $\mathcal{F}_T$-symbols. That is why we need to compute critical pairs of R_T inside R_{NT}. Our proof uses many concepts and techniques inherited from previous work on modularity, such as the decomposition of terms (caps and aliens, hats and estimated caps [Toy87]). We have not tried using van Oostrom's notion of caps, in which aliens must have maximal

[1] This is an assumption that was forgotten, but used, for R_T, as pointed out by Aart Middeldorp.

rank [vO08b], nor the method developed by Klein and Hirokawa for studying the Church-Rosser property of *disjoint* rewrite relations on terms [KH12], which we could do by considering cap rewriting with R_T-rules and alien rewriting with all rules. This remains to be done.

5.5 Conclusion

Decreasing diagrams opened the way for generalizing Knuth and Bendix's critical-pair test for confluence to non-terminating systems, re-igniting these questions. Our results answer important open questions, in particular by allowing both non-left-linear and non-terminating rules. While combining many existing as well as new techniques, our proof has proved quite robust. Two technical questions have been left open: having collapsing rules in R_{NT}, following [Fel13b], and eliminating assumption (A4).

A major theoretical question is whether layering requires assumption (A1). Our proof is based on two key properties, layering and the absence of overlaps of R_{NT} inside R_T. Currently, (A1) serves both purposes. The question is however open whether the latter property is sufficient to define some form of layering. We will further investigate it in the next chapter.

Transformation valuation is a static analysis that tries to verify that an optimizer is semantics preserving by constructing a *value graph* for both programs and showing their equivalence by rewriting techniques [TGM11]. Here, the user has a good feeling of which subset of rules is a candidate for R_{NT}. Where this is not the case, work is of course needed to find good splits automatically.

We end up this chapter with our long-term goal, applying this technique in practice. The need for showing the Church-Rosser property of mixed terminating and non-terminating computations arises in at least two areas, first-order and higher-order. The development of sophisticated type theories with complex elimination rules requires proving Church-Rosser *before* strong-normalization and type preservation, directly on untyped terms. Unfortunately, besides being collapsing, β-reduction is also rank-increasing in the presence of another signature. We therefore need to develop another notion of rank that would apply to pure λ-calculus, a question related to the previous one. More attempts will be carried out in the next chapter.

Six

Confluence of Layered Rewrite Systems

Notwithstanding many efforts [Ros73, Hue80, TO94, MOOO97, Oku98, MO01, vO08a, GOO98, JvO09, SO10, HM11, ZFM15, KH12, SOO15, ATU14], confluence of non-terminating systems is far from being understood in terms of critical pairs. Only recently did this question make important progress with decreasing diagrams, a generalization of joinability [vO94a, vO08a]. In particular, while Huet's result stated that linear systems are confluent provided their critical pairs are strongly joinable [Hue80], Felgenhauer showed that right-linearity could be removed provided parallel critical pairs have decreasing diagrams [Fel13b]. In Chapter 5, we have demonstrated that Knuth–Bendix's Lemma and Felgenhauer's theorem can join forces in presence of both terminating and non-terminating rules.

We show in this chapter that rank non-increasing layered systems are confluent provided their critical pairs have decreasing diagrams. Our confluence result achieved in this chapter for non-terminating non-linear systems by critical pair analysis is the first we know of. Further, the result holds in case critical pairs become infinite, solving the confluence problem of variations of a mysterious system raised in [Hue80], presented as NKH in Example 5.3.13. Prior solutions to the problem existed under different assumptions that could be easily challenged [TO94, GOO98, KH12].

Our results use a simplified, in some sense generalized, version of sub-rewriting introduced in Chapter 5, and a simple, but essential revisitation of unification in case overlaps generate occurs-check equations: *cyclic unification* is based on a new, important notion of *cyclic unifiers*, which enjoy all good properties of unifiers over finite trees such as existence of most general cyclic unifiers, and can therefore represent solutions of occurs-check equations by simple rewriting means.

The notion of terms is revised in Section 6.1. We introduce sub-rewriting and cyclic unification in Sections 6.2 and 6.3, respectively. Layered systems are discussed in Section 6.4 where our main result is developed, before concluding in Section 6.5.

6.1 Terms and Rewriting

In this chapter, we consider possibly infinite terms instead of only finite ones given in Chapter 2. We revise the notions related to terms, positions, substitutions and rewriting. In this section, we only mention the ones that need to be adapted, while keep the non-mentioned ones as usual.

Given a signature $\mathcal{F}$ of function symbols and a denumerable set $\mathcal{X}$ of variables, $\mathcal{T}(\mathcal{F}, \mathcal{X})$ now denotes the set of finite or *infinite rational* terms built up from $\mathcal{F}$ and $\mathcal{X}$. Terms are recognized by top-down tree automata in which some ω-states, and only those, are possibly traversed infinitely many times. As usual, terms can be viewed as labelled ordered trees. See [Tho90] for details.

Note that positions are finite strings of positive integers. However, $\mathcal{P}os(t)$ (resp., $\mathcal{FP}os(t)$) is now for the possibly infinite set of all (resp., non-variable) positions of t.

Given a term t, we denote by $\bar{t}$ any linear term obtained by replacing, for each variable $x \in \mathcal{V}ar(t)$, the occurrences of x at positions $\{p_i\}_i$ in t by *linearized variable* x^{k_i} such that $i \neq j$ implies $x^{k_i} \neq x^{k_j}$. Note that $\mathcal{V}ar(\bar{s}) \cap \mathcal{V}ar(\bar{t}) = \varnothing$ iff $\mathcal{V}ar(s) \cap \mathcal{V}ar(t) = \varnothing$. Identifying x^{k_0} with x, $\bar{t} = t$ for a linear term t.

A substitution σ is said to be *finite* if for each $x \in \mathcal{D}om(\sigma)$, $\sigma(x)$ is a finite term. The subsumption order $\trianglerighteq$ is defined on finite terms and finite substitutions as defined in Chapter 2.

A rewrite rule is a pair of *finite* terms, written $l \to r$, as we defined in Chapter 2. We write $u \to^{p,m}_{l\to r\in R} v$ for a *labelled rewrite step* from u to v at position p with label m and rule $l \to r \in R$. Indexes $p, m, R, l \to r$ may be omitted, or replaced by properties they satisfy.

Our goal is to reduce confluence of a non-terminating non-left-linear rewrite system R to that of finitely many critical pairs, based on the decreasing diagrams method. In this chapter, the directional version of decreasing diagrams defined in Definition 2.2.5 will be applied. Mention of the word "joinably" is sometimes omitted for convenience. As in Chapter 5, Corollary 2.2.12 will be heavily used in stead of Theorem 2.2.6, since it is more convenient for our purpose.

6.2 Sub-Rewriting

Consider the famous example NKH publicized by Huet [Hue80], as we have presented in Example 5.3.13. It is overlap-free, hence locally confluent by Huet's lemma [Hue80], but non-confluent. The main difficulty with NKH is that non-joinable peaks are non-local, such as $a \leftarrow f(g, g) \to f(g, c(g)) \to b$. To restore the usual situation for which the confluence of a relation can be characterized by the joinability of its local peaks, we need another rewrite relation whose local peaks capture the non-confluence of NKH as well as the confluence of its confluent variations.

A major insight in Chapter 5 is that this can be achieved by the *sub-rewriting* (in fact, R_T-*sub-rewriting*) relation, that allows us to rewrite $f(g, c(g))$ in one step to either a or b, therefore exhibiting the pair $\langle a, b\rangle$ as a sub-rewriting critical pair. The idea underlying sub-rewriting is that a preparatory *equalization* phase allows the variable instances of the left-hand side l of some rule $l \to r$ to be joined, which takes place before the rule is applied. However in Chapter 5, R_T-sub-rewriting requires a signature split to define layers in terms, the preparatory phase taking place in the lower layers. No a-priori layering is needed here:

Definition 6.2.1 (Sub-Rewriting)**.** A term u *sub-rewrites* to a term v at $p \in \mathcal{P}os(u)$ with some rule $l \to r \in R$, written $u \to^p_{R_R} v$, if $u \twoheadrightarrow_R^{(>_{\mathcal{P}} p \cdot \mathcal{FP}os(l))} u[l\theta]_p \to^p_R u[r\theta]_p = v$ for some substitution θ. The term $u|_p$ is called a *sub-rewriting redex*.

This definition of sub-rewriting allows *arbitrary rewriting* below the left-hand side of the rule until a redex is obtained. This is the major idea of sub-rewriting, ensuring that $R \subseteq R_R \subseteq R^*$. A simple but important property of a sub-rewriting redex is that it is an instance of some linearized left-hand side of rule:

Lemma 6.2.2 (Sub-Rewriting Redex)**.** *Assume u sub-rewrites to $u[r\sigma]_p$ with $l \to r$ at position p. Then $u|_p = \bar{l}\theta$ for some θ such that* $(\forall x \in \mathcal{V}ar(l))\,(\forall p_i \in \mathcal{P}os(l)\; s.t.\; l(p_i) = x)\; \theta(x^{p_i}) \twoheadrightarrow_R \sigma(x)$*. We say that σ is an* equalizer *of l, and the rewrite steps from $\bar{l}\theta$ to $l\sigma$ are an* equalization*.*

Sub-rewriting differs from rewriting modulo an equational theory by being directional. It differs from Klop's higher-order rewriting modulo developments [Ter03] used by Okui for first-order computations [Oku98], in that the preparatory phase uses arbitrary rewriting. Having non-left-linear rules with critical pairs at subterms seems incompatible with using developments. Sub-rewriting differs as well from relative rewriting [Ges90] in that the preparatory phase must take place below variables. The latter condition is essential to obtain plain critical pairs based on plain unification.

Assuming that local sub-rewriting peaks characterize the confluence of NKH, we need to compute the corresponding critical pairs. Unifying the left-hand sides $f(x, x)$ and $f(y, c(y))$ results in the conjunction $x = y \wedge y = c(y)$ containing the *occurs-check equation* $y = c(y)$, which prevents unification from succeeding on finite trees but allows it to succeed on infinite rational trees: the critical peak has therefore an infinite overlap $f(c^\omega, c^\omega)$ and a finite critical pair $\langle a, b\rangle$. At the level of infinite trees, we then have an infinite local rewriting peak $a \leftarrow f(c^\omega, c^\omega) = f(c^\omega, c(c^\omega)) \to b$, the properties of infinite trees making the sub-rewriting preparatory phase useless. Sub-rewriting therefore captures on finite trees some properties of rewriting on infinite trees, here the existence of a local peak.

Unification over finite rational trees resulting in infinite rational trees was first considered by Huet, who showed that, when unification over finite trees results in a possibly empty set of equations without occurs-check, and a non-empty set of equations with occurs-check, then the latter has solutions over infinite rational trees [Hue76]. Solving equations over infinite rational trees was also considered by Courcelle with a slightly different, fixpoint-oriented perspective [Cou83].

Consider now the equation $x = f(x)$ which has the most general rational unifier $\sigma = \{x \mapsto f^\omega\}$. Then, $x\sigma = f^\omega$ and $f(x)\sigma = f^{1+\omega}$. These two terms are syntactically different, although they correspond to the same infinite tree because the two ordinals $1 + \omega$ and ω are equal. In the next section, we develop a novel view of unification that will allow us to capture both finite and infinite overlaps by finite means. Struggling with the axiomatization of infinite rational trees will not be necessary.

6.3 Cyclic Unification

This section is adapted from [Hue76, Col84, DJ90, JK91] by treating finite and infinite unifiers uniformly: equality of terms is interpreted over the set of infinite rational terms *when needed*.

In this chapter, an *equation* is treated as an *oriented* pair of finite terms, written $u = v$. A *unification problem* P is a (finite) conjunction $\wedge_i\, u_i = v_i$ of equations, sometimes seen as a multiset of pairs written $\vec{u} = \vec{v}$. A *unifier* (resp., a *solution*) of P is a substitution (resp., a ground substitution) θ such that $(\forall i)\, u_i\theta = v_i\theta$. A unifier describes a generally infinite set of solutions via its ground instances. A major usual assumption, ensuring that solutions exist when unifiers do, is that the set $\mathcal{T}(\mathcal{F})$ of ground terms is non-empty. A unification problem P has a *most general finite unifier* $mgu(P)$, whenever a finite solution exists, which is minimal with respect to subsumption hence unique up to variable renaming. Computing $mgu(P)$ can be done by the unifier-preserving transformations in Table 6.1, starting with P until a *solved form* is obtained, $\perp$ denoting the absence of solution, whether finite or infinite. Our notion of solved form therefore allows for infinite unifiers (and solutions) as well as finite ones:

Definition 6.3.1. *Solved forms* of a unification problem P different from $\perp$ are unification problems $S := \vec{x} = \vec{u} \wedge \vec{y} = \vec{v}$ such that

(i) $\mathcal{P} = \mathcal{V}ar(P) \setminus (\vec{x} \cup \vec{y})$ is the set of *parameters* of S;

(ii) variables in $\vec{x} \cup \vec{y}$ (i.e. variables at left-hand sides of equations) are all distinct;

(iii) for each $x = u$ in $\vec{x} = \vec{u}$, $\mathcal{V}ar(u) \subseteq \mathcal{P}$;

(iv) for each $y = v$ in $\vec{y} = \vec{v}$, $\mathcal{V}ar(v) \subseteq \mathcal{P} \cup \vec{y}$, $\mathcal{V}ar(v) \cap \vec{y} \neq \varnothing$ and $v \notin \mathcal{X}$.

Equations $y = v \in \vec{y} = \vec{v}$ are called *cyclic* (or *occurs-check*, the vocabulary originating from [Col84] used so far), $\vec{x}$ is the set of *finite* variables, and $\vec{y}$ is the set of (infinite) *cyclic* (or *occurs-check*) variables. A solved form is a set of equations since $\vec{x} \cup \vec{y}$ is itself a set and an equation $x = y$ between variables can only relate a finite variable x with a parameter y.

Example 6.3.2. Consider NKH. $f(x, x) = f(y, c(y)) \rightarrow_{\textbf{Decomp}} x = y \wedge x = c(y) \rightarrow_{\textbf{Coalesce}} x = y \wedge y = c(y) \rightarrow_{\textbf{Merep}} x = c(y) \wedge y = c(y)$. Alternatively, $f(x, x) = f(y, c(y)) \rightarrow_{\textbf{Decomp}} x = y \wedge x = c(y) \rightarrow_{\textbf{Replace}} c(y) = y \wedge x = c(y) \rightarrow_{\textbf{Swap}} y = c(y) \wedge x = c(y)$.

Choose and **Swap** originate from [Col84]. **Replace** and **Coalesce** ensure that finite variables (but parameters) do not occur in equations constraining the infinite ones. **Merep** is a sort of combination of **Merge** and **Replace** ensuring condition $v \notin \mathcal{X}$ in Definition 6.3.1, item (iv). Unification over finite trees has another failure rule, called **Occurs-check**, fired in presence of cyclic equations.

Theorem 6.3.3. *Given an input unification problem P, the unification rules terminate, fail if the input has no solution, and return a solved form $S = \vec{x} = \vec{u} \wedge \vec{y} = \vec{v}$ otherwise.*

Proof. Proofs for termination, characterization of solved forms, and soundness, are all adapted from [JK91].

Remove	$s = s \wedge P$	$\to$	P
Decomp	$f(\vec{s}) = f(\vec{t}) \wedge P$	$\to$	$\vec{s} = \vec{t} \wedge P$
Conflict	$f(\vec{s}) = g(\vec{t}) \wedge P$	$\to$	$\perp$
			if $f \neq g$
Choose	$y = x \wedge P$	$\to$	$x = y \wedge P$
			if $x \notin \mathcal{V}ar(P)$, $y \in \mathcal{V}ar(P)$
Coalesce	$x = y \wedge P$	$\to$	$x = y \wedge P\{x \mapsto y\}$
			if $x, y \in \mathcal{V}ar(P)$, $x \neq y$
Swap	$u = x \wedge P$	$\to$	$x = u \wedge P$
			if $u \notin \mathcal{X}$
Merge	$x{=}s \wedge x{=}t \wedge P$	$\to$	$x = s \wedge s = t \wedge P$
			if $x \in \mathcal{X}$, $0 < \lvert s\rvert \leq \lvert t\rvert$
Replace	$x = s \wedge P$	$\to$	$x = s \wedge P\{x \mapsto s\}$
			if $x \in \mathcal{V}ar(P)$, $x \notin \mathcal{V}ar(s)$, $s \notin \mathcal{X}$
Merep	$y{=}x \wedge x{=}s \wedge P$	$\to$	$y = s \wedge x = s \wedge P$
			if $x \in \mathcal{V}ar(s)$, $s \notin \mathcal{X}, y \notin \mathcal{V}ar(s, P)$
			and no other rule applies

Table 6.1: Unification Rules

Termination. The quadruple $\langle n_u, |P|, n_v^r, n_v^l \rangle$ is used to interpret a unification problem P, where

– n_u is the number of unsolved variables (0 for $\perp$), where a variable x is *solved* in $x = s \wedge P'$ if $x \notin \mathcal{V}ar(s, P')$;

– $|P|$ is the multiset ($\varnothing$ for $\perp$) of natural numbers $\{max(|s|, |t|) \mid s = t \in P\}$;

– n_v^l (resp., n_v^r) is the number of equations in P whose left-hand (resp., right-hand) side is a variable and the other side is not.

Remove, **Decomp** and **Conflict** decrease $|P|$ without increasing n_u. **Choose** and **Coalesce** both decrease n_u. **Swap** decreases n_v^r without increasing n_u and $|P|$. **Merge** decreases n_v^l without increasing n_u, $|P|$ and n_v^r. **Replace** decreases n_u. Now, when **Merep** applies, no other rule can apply, and we can check that no rules can apply either after **Merep** (except another possible application of **Merep**). This can happen only finitely many times, by simply reasoning on the number of equations whose both sides are variables.

Solved form. We show by contradiction that the output P, which is in normal form with respect to the unification rules, is a solved form in case **Conflict** never applies. First, P must be a conjunction of equations $x = s$, since otherwise **Decomp** or **Swap** would apply. Let $\mathcal{P} = \mathcal{V}ar(P) \setminus (\vec{x} \cup \vec{y})$.

- Condition (i) is a definition.
- Condition (ii). Let $P = (x = s \wedge x = t \wedge P')$. Either s or t is a variable, since otherwise **Merge** would apply. Assume without loss of generality that $s \in \mathcal{X}$, call it y. If $x = y$, **Remove** applies. If $y \notin \mathcal{V}ar(t, P')$, then **Choose** applies. Otherwise, **Coalesce** applies. Hence $\vec{x}, \vec{y}$ are all different *sets*, and P is therefore itself a set.

  Let now $\vec{x} = \vec{u}$ be a maximal (with respect to inclusion) set of equations in P such that $\mathcal{V}ar(\vec{u}) \subseteq \mathcal{P}$, and $\vec{y} = \vec{v}$ be the remaining set of equations.
- Condition (iii). It is ensured by the definition of $\vec{x} = \vec{u}$.
- Condition (iv). Let $y = v \in \vec{y} = \vec{v}$.

  Let now $x = u \in \vec{x} = \vec{u}$, hence $x \notin \mathcal{V}ar(u)$. Assume $x \in \mathcal{V}ar(v)$. If $u \notin \mathcal{X}$, then **Replace** applies. Otherwise, if u has no other occurrence in P, then **Choose** applies, else **Coalesce** applies. Therefore $\mathcal{V}ar(v) \cap \vec{x} = \varnothing$ by contradiction.

  Assume $\mathcal{V}ar(v) \cap \vec{y} = \varnothing$. Then $\mathcal{V}ar(v) \subseteq \mathcal{P}$, which contradicts the maximality of $\vec{x} = \vec{u}$.

  We are left to show that v is not a variable. If it were, then $v \in \vec{y}$. First, $v \neq y$, otherwise **Remove** applies. Let $P = (y = v \wedge P')$ with $v \in \vec{y} \setminus \{y\}$. Let $v = z$, there must exist $(z = w) \in P'$ for some w, otherwise $z \in \mathcal{P}$. Hence $P' = (z = w \wedge P'')$. Now, $y \notin \mathcal{V}ar(w, P'')$, otherwise **Coalesce** applies. Then we show $z \in \mathcal{V}ar(w)$: firstly, $w \neq z$, otherwise **Remove** applies; secondly, w is not a variable, otherwise

$w \notin \mathcal{V}ar(y, P'')$ lets **Choose** apply, while $w \in \mathcal{V}ar(y, P'')$ makes **Coalesce** available; then if $z \notin \mathcal{V}ar(w)$, **Replace** applies. Thus $z \in \mathcal{V}ar(w)$, allowing **Merep**, which contradicts that we have indeed a solved form.

Soundness. The set of solutions is an invariant of the unification rules. This is trivial for all rules but **Coalesce**, **Merge**, **Replace**, **Merep**, for which it follows from the fact that substitutions are homomorphisms and equality is a congruence. □

The solved form is a *tree solved form* if $\vec{y} = \varnothing$, and otherwise an Ω *solved form* whose solutions are infinite substitutions taking their values in the set of infinite (rational) terms. We shall now develop our notion of *cyclic unifiers* capturing both solved forms by describing the infinite unifiers of a problem P as a pair of a finite unifier σ and a set of cyclic equations E constraining those variables that require infinite solutions. In case $E = \varnothing$, then P is a tree solved form and $\sigma = mgu(P)$. To avoid manipulating infinite unifiers when $E \neq \varnothing$, we shall work with the cyclic equations themselves considered as a ground rewrite system.

Definition 6.3.4 ([NO80])**.** Given a set of equations E, we denote by $=^{cc}_{E}$ the equational theory in which the variables in $\mathcal{V}ar(E)$ are treated as constants, also called *congruence closure* E.

We are interested in the congruence closure defined by cyclic equations, seen here as a set R of ground rewrite rules. We may sometimes consider R as a set of equations, to be either solved or used as axioms, depending on context.

Definition 6.3.5. A *cyclic rewrite system* is a set of rules $R = \{\vec{y} \to \vec{v}\}$ such that the unification problem $\vec{y} = \vec{v}$ is its own solved form with $\vec{y}$ as the set of infinite cyclic variables. Variables in R are treated as constants.

Lemma 6.3.6. *A cyclic rewrite system R is ground and critical pair free, hence Church-Rosser.*

We now introduce our definition of cyclic unifiers and solutions:

Definition 6.3.7. A *cyclic unifier* of a unification problem P is a pair $\langle \eta, R\rangle$ made of a substitution η and a cyclic rewrite system $R = \{\vec{y} \to \vec{v}\}$, satisfying:

(i) $\mathcal{D}om(\eta) \subseteq \mathcal{V}ar(P) \setminus \vec{y}$, $\mathcal{VR}an(\eta) \cap \vec{y} = \varnothing$, and $\mathcal{VR}an(\eta) \cap \mathcal{D}om(\eta) = \varnothing$;

(ii) P and $P \wedge R$ have identical sets of solutions ; and

(iii.a) $(\forall u = v \in P)\, u\eta =^{cc}_{R\eta} v\eta$, or equivalently by Lemma 6.3.6,

(iii.b) $(\forall u = v \in P)\, u\eta \twoheadrightarrow_{R\eta} \circ\, {}_{R\eta}\!\twoheadleftarrow v\eta$.

A *cyclic solution* of P is a pair $\langle \eta\rho, R\rangle$ made of a cyclic unifier $\langle \eta, R\rangle$ of P and an additional substitution ρ.

We shall use (iii.a) or (iii.b) indifferently, depending on our needs, by referring to (iii).

The idea of cyclic unifiers is that the need for infinite values for some variables is encoded via the use of the cyclic rewrite system R, which allows us to solve the various occurs-check equations generated when unifying P. Finite variables are instantiated by the finite substitution η, which ensures that cyclic unification reduces to finite unification in the absence of infinite variables. The technical restrictions on $\mathcal{D}om(\eta)$ and $\mathcal{VR}an(\eta)$ aim at making η idempotent. In (iii), parameters occurring in R are instantiated by η before rewriting takes place: cyclic unification is nothing but rigid unification modulo the cyclic equations in R [GRS87]. Instantiation of the infinite variables $\vec{y}$ is delegated to cyclic solutions via the additional substitution ρ which may also instantiate the variables introduced by η.

Example 6.3.8. Consider the equation $f(x, z, z) = f(a, y, c(y))$. A cyclic unifier is $\langle \{x \mapsto a\}, \{y \to c(z),\ z \to c(z)\}\rangle$, and a cyclic solution is $\langle \{x \mapsto a,\ y \mapsto a,\ z \mapsto c(a)\}, \{y \to c(z),\ z \to c(z)\}\rangle$, which is clearly an instance of the former by the substitution $\{y \mapsto a,\ z \mapsto c(a)\}$. For the former, $f(a, z, z) =^{cc}_{\{y=c(z), z=c(z)\}} f(a, y, c(y))$. Another cyclic unifier is $\langle \{x \mapsto a\}, \{z \to c(y), y \to c(y)\}\rangle$, for which $f(a, z, z) =^{cc}_{\{z=c(y), y=c(y)\}} f(a, y, c(y))$.

The set of cyclic unifiers of a problem P is closed under substitution instance, provided the variable conditions on its substitution part are met, as is the set of its unifiers. We believe that cyclic unifiers have many interesting properties similar to those of finite unifiers, of which we are going to investigate only a few which are relevant to the confluence of layered systems.

We now focus our attention on specific cyclic unifiers sharing a same cyclic rewrite system.

Definition 6.3.9. Given a unification problem P with solved form $S = \vec{x} = \vec{u} \wedge \vec{y} = \vec{v}$, let

– its cyclic rewrite system $R_S = \{\vec{y} \to \vec{v}\}$ and *canonical* substitution $\eta_S = \{\vec{x} \mapsto \vec{u}\}$,

– its S-based cyclic unifiers $\langle \eta, R_S \rangle$, among which $\langle \eta_S, R_S \rangle$ is said to be *canonical*.

We now show a major property of S-based cyclic unifiers, true for any solved form S:

Lemma 6.3.10. *Given a unification problem with solved form S, the set of S-based cyclic unifiers is preserved by the unification rules.*

Proof. The result is straightforward for **Remove**, **Choose**, and **Swap**. It is true for **Decomp** and **Conflict** since, using formulation (iii.b) of Definition 6.3.7, the rules in $R\eta$ cannot apply at the root of $\mathcal{F}$-headed terms. Next comes **Coalesce**. We need to prove that $\langle \eta, R \rangle$ is a cyclic unifier for $x = y \wedge P$ if and only if it is one for $x = y \wedge P\{x \mapsto y\}$. Let $u = v \in P$. For the only if case, we have $u\{x \mapsto y\}\eta = u\eta\{x\eta \mapsto y\eta\} =^{cc}_{R\eta} u\eta =^{cc}_{R\eta} v\eta =^{cc}_{R\eta} v\eta\{x\eta \mapsto y\eta\} = v\{x \mapsto y\}\eta$. The if case is similar. **Replace** is similar to **Coalesce**. Consider now **Merge** (**Merep** is similar). Showing that $\langle \eta, R \rangle$ is a cyclic unifier for $x = s \wedge x = t \wedge P$ if and only if it is one for $x = s \wedge s = t \wedge P$ is routine by using transitivity of the congruence closure $=^{cc}_{R\eta}$. □

We can now conclude:

Theorem 6.3.11. *Given a unification problem P with solved form $S = (\vec{x} = \vec{u} \wedge \vec{y} = \vec{v})$, the canonical S-based cyclic unifier is most general among the set of S-based cyclic unifiers of P.*

Proof. Let $\langle \eta, R_S \rangle$ be a cyclic unifier of P based on S.

Let $x = u \in \vec{x} = \vec{u}$. By definition of cyclic unification, $x\eta \twoheadrightarrow_{R_S\eta} \circ {}_{R_S\eta}\twoheadleftarrow u\eta$. By definition of a solved form and cyclic unifiers, we have: $\mathcal{V}ar(x\eta, u\eta) \subseteq (\vec{x} \cup \mathcal{P} \cup \mathcal{VR}an(\eta))$, $(\vec{x} \cup \mathcal{P}) \cap \vec{y} = \varnothing$, $\mathcal{VR}an(\eta) \cap \vec{y} = \varnothing$, and $\vec{y} \cap \mathcal{D}om(\eta) = \varnothing$. Therefore, $x\eta$ and $u\eta$ are irreducible by $R_S\eta$. Hence $x\eta = u\eta$. Since $x\eta_S = u$, it follows that $x\eta = u\eta = (x\eta_S)\eta = x(\eta_S\eta)$.

Let now $z \in \mathcal{V}ar(P) \setminus \vec{x}$. Since $z \notin \mathcal{D}om(\eta_S)$, then $\eta(z) = z\eta = (z\eta_S)\eta = z(\eta_S\eta)$.

Therefore, $\eta = \eta_S\eta$ and we are done. $\square$

This result, which suffices for our needs, is easily lifted to cyclic solutions, as they are instances of a cyclic unifier. We can further prove that η_S is more general than any S'-based cyclic unifiers, for any solved form S' of P. This is where our conditions on $\mathcal{VR}an(\eta)$ become important. We conjecture that it is most general among the set of all cyclic unifiers.

6.4 Layered Systems

NKH is non-confluent, but can be easily made confluent by adding the rule $a \to b$ (giving NKH^1), or removing the rule $g \to c(g)$ (giving NKH^2). It can be made non-right-ground by making the symbols a, b unary (using $a(c(x))$ and $b(c(x))$ in the right-hand sides of rules, giving NKH^3), or even non-right-linear by making them binary (giving NKH^4). There are classes of systems containing NKH for which it is possible to conclude its confluence. The following classes succeed for NKH^1: simple-right-linear [TO94], strongly depth-preserving [GOO98], and relatively terminating [KH12]. As for NKH^3, it is neither simple-right-linear nor strongly depth-preserving: only [KH12] can cover it. When it comes to NKH^4, relative termination becomes hard to satisfy in presence of non-right-linearity [KH12].

Our goal is to define a robust, Turing-complete class of rewrite systems capturing NKH and its variations, for which confluence can be analyzed in terms of critical diagrams.

Definition 6.4.1. A rewrite system R is *layered* iff it satisfies the *disjointness* assumption (DLO) that *linearized overlaps* of some left-hand sides of rules upon a given left-hand side l can only take place at a multiset of disjoint or equal positions of $\mathcal{FP}os(l)$:

$$\begin{array}{rcl} \text{(DLO)} & := & (\forall l \to r \in R)\,(\forall p \in \mathcal{FP}os(l)) \\ & & (\forall g \to d \in R \text{ s.t. } \mathcal{V}ar(\bar{l}) \cap \mathcal{V}ar(\overline{g}) = \varnothing) \\ & & (\forall \sigma : \mathcal{V}ar(\bar{l}|_p, \overline{g}) \to \mathcal{T}(\mathcal{F}, \mathcal{X}) \text{ s.t. } \bar{l}|_p\sigma = \overline{g}\sigma)\, \mathrm{SOF}(l|_p) \wedge \mathrm{SOF}(g) \\ \mathrm{SOF}(u) & := & (\forall q \in \mathcal{FP}os(u) \setminus \{\Lambda\})\, \mathrm{OF}(u|_q) \\ \mathrm{OF}(v) & := & (\forall g \to d \in R \text{ s.t. } \mathcal{V}ar(\overline{v}) \cap \mathcal{V}ar(\overline{g}) = \varnothing) \\ & & (\forall o \in \mathcal{FP}os(v))(\forall \sigma : \mathcal{V}ar(\overline{v}, \overline{g}) \to \mathcal{T}(\mathcal{F}, \mathcal{X}))\; \overline{v}|_o\sigma \neq \overline{g}\sigma \end{array}$$

SOF stands for *subterm overlap-free*, and OF for *overlap-free*. In words, if a linearized left-hand side $\overline{g}$ of a rule in R overlaps some linearized left-hand side $\bar{l}$ of some rule in R at position p, then neither g nor $l|_p$ contains a strict subterm that can be overlapped linearly. This implies the fact that if two left-hand sides of rules overlap (linearly) a left-hand side l of a rule at p and q, respectively, then either $p = q$ or $p \# q$. Overlaps at different positions along a path from the root to a leaf of l are forbidden.

Layered systems are a decidable class relating to overlay systems [DOS87], for which overlaps computed with plain unification can only take place at the root of terms – hence their name –, and generalizes strongly non-overlapping systems [SO10] which admit no linearized overlaps at all. All these classes are Turing-complete since they contain a complete class [Klo93].

Example 6.4.2. NKH is a layered system, which is also overlay. $\{h(f(x,y)) \to a,\ f(x,c(x)) \to b\}$ is layered but not overlay. $\{h(f(x,x)) \to a,\ f(x,c(x)) \to b,\ g \to c(g)\}$ is layered, but not strongly non-overlapping. $\{f(h(x)) \to x,\ h(a) \to a,\ a \to b\}$ is not overlay nor layered: $\mathrm{SOF}(h(x))$ succeeds while $\mathrm{SOF}(h(a))$ fails, hence their conjunction fails.

6.4.1 Layering

In this chapter, we define a new notion of rank with respect to *redex-depth*. The (new) rank of a term t is the maximum number of non-overlapping linearized redexes traversed from the root to some leaf of t, which differs from the usual redex-depth.

Definition 6.4.3. Given a layered rewrite system R, the *rank (with respect to redex-depth)* $\text{rank}^{rd}(t)$ ($\text{rank}(t)$ for simplicity) of a term t is defined by induction on the size of terms as follows:

– the maximal rank of its immediate subterms if t is not a linearized redex ; otherwise,

– 1 plus $max\{\text{rank}^{rd}(\sigma) \mid (\exists l \to r \in R)\, t = \bar{l}\sigma\}$, where $\text{rank}^{rd}(\sigma) := max\{\text{rank}^{rd}(\sigma(x)) \mid x \in \mathcal{V}ar(\bar{l})\}$.

Definition 6.4.4. A rewrite system R is *rank non-increasing* if for all terms u, v such that $u \to_R v$, then $\text{rank}(u) \geq \text{rank}(v)$.

The rewrite system $\{f(x) \to c(f(x))\}$ is rank non-increasing while $\{f(x) \to f(f(x))\}$ is rank increasing. The system $\{fib(0) \to 0,\ fib(S(0)) \to S(0),\ fib(S(S(x))) \to fib(S(x)) + fib(x)\}$ calculating the Fibonacci function is rank non-increasing. NKH is rank non-increasing. The coming decidable sufficient condition for rank non-increasingness captures our examples (but for Fibonacci, for which an even more complex decidable property is needed):

Lemma 6.4.5. *A layered rewrite system R is rank non-increasing if each rule $g \to d$ in R satisfies the following properties:*

(i) $(\forall l \to r \in R)$
$(\forall l' \to r' \in R$ *s.t.* $\mathcal{V}ar(d), \mathcal{V}ar(\bar{l}), \mathcal{V}ar(\overline{l'})$ *are pairwise disjoint*$)$
$(\forall p, q \in \mathcal{FP}os(d)$ *s.t.* $q > p \cdot \mathcal{FP}os(l))$
$(\forall \sigma : \mathcal{V}ar(g, \bar{l}, \overline{l'}) \to \mathcal{T}(\mathcal{F}))\ (d|_p\sigma \neq \bar{l}\sigma) \vee (d|_q\sigma \neq \overline{l'}\sigma)$ *;*

(ii) $(\forall l \to r \in R$ *s.t.* $\mathcal{V}ar(g) \cap \mathcal{V}ar(\bar{l}) = \varnothing)$
$(\forall p \in \mathcal{FP}os(l) \setminus \Lambda)$
$(\forall \sigma : \mathcal{V}ar(g, \bar{l}) \to \mathcal{T}(\mathcal{F})$ *s.t.* $d\sigma = \bar{l}|_p\sigma)$

$(\exists l' \to r' \in R \ s.t.\ \mathcal{V}ar(\overline{l'}) \cap \mathcal{V}ar(g, \bar{l}) = \varnothing)$
$(\exists x \notin \mathcal{V}ar(\bar{l}, \overline{l'}, g))\ \bar{l}[x]_p \trianglerighteq \overline{l'}.$

The intuition of property (i) is that the right-hand side d does not contain two vertically non-overlapped redexes, which may increase the rank of terms. And property (ii) gives an idea that rewriting with the rule $g \to d$ will not create a new redex above the rewritten position.

We can now again index term-related notions by the rank of terms. Let $\mathcal{T}_n(\mathcal{F}, \mathcal{X})$ (in short, $\mathcal{T}_n$) be the set of terms of rank at most n. Two terms in $\mathcal{T}_n$ are *n-convertible* (resp., *n-joinable*) if their R-conversion (resp., R-joinability) involves terms in $\mathcal{T}_n$ only.

6.4.2 Closure properties

We call a term u an *OF-term* if u satisfies OF(u), and a substitution an *OF-substitution* if it maps variables to OF-terms. OF-terms enjoy several important closure properties. Given two substitutions θ, σ and rank n, let

Conv$^\theta_n(\overline{u},\overline{v})$ if $\overline{u}\theta$ and $\overline{v}\theta$ are n-convertible, and

Equalize$_n(\overline{u})^\theta_\sigma$ if $\overline{u}\theta \twoheadrightarrow_{R_R} u\sigma$ with terms of rank at most n.

Lemma 6.4.6. *For all OF-terms u and substitutions γ, $u\gamma$ cannot sub-rewrite at a position $p \in \mathcal{FP}os(u)$.*

Corollary 6.4.7. *OF-terms are preserved under instantiation by OF-substitutions.*

Lemma 6.4.8. *Let u, v be two terms such that Conv$^\theta_n(\overline{u},\overline{v})$, Equalize$_n(\overline{u})^\theta_\sigma$ and Equalize$_n(\overline{v})^\theta_\sigma$. Then $u\sigma$ and $v\sigma$ are n-convertible.*

Lemma 6.4.9. *Let $\wedge_i\, u_i = v_i$ be obtained by decomposition of a unification problem P. Assume all equations $u_i = v_i$ satisfy the properties Conv$^\theta_n(\overline{u_i},\overline{v_i})$, Equalize$_n(\overline{u_i})^\theta_\sigma$, Equalize$_n(\overline{v_i})^\theta_\sigma$, OF$(u_i)$ and OF(v_i). Assume further that n-convertible terms are joinable. Then, unification of P succeeds, and returns a solved form of which all equations satisfy these five properties.*

In this lemma and coming proof, we assume that linearizations are propagated by the unification rules, implying in particular that $\overline{u|_p} = \overline{u}|_p$. P defines the initial linearization.

Proof. We show that these five properties are invariant by the unification rules. The claim follows since the unification rules terminate. We use notations in Table 6.1.

- **Remove**, **Choose**, **Swap** are straightforward.
- **Decomp**. By assumption, $\mathrm{Conv}_n^\theta(\overline{f(\vec{s})},\overline{f(\vec{t})})$, hence $\overline{f(\vec{s})}\theta$ and $\overline{f(\vec{t})}\theta$ are joinable by using terms of rank at most n, since R is rank non-increasing. By assumption $\mathrm{OF}(f(\vec{s}))$ and $\mathrm{OF}(f(\vec{t}))$, hence no rewrite can take place at the root. The result follows.
- **Conflict**. By the same token, $f = g$, a contradiction. Thus **Conflict** is impossible.
- **Coalesce**. By assumption, we have $\mathrm{Conv}_n^\theta(x^k,y^l)$, $\mathrm{Equalize}_n(x^k)_\sigma^\theta$, $\mathrm{Equalize}_n(y^l)_\sigma^\theta$, and for each $u = v$ in P, $\mathrm{Conv}_n^\theta(\overline{u},\overline{v})$, $\mathrm{Equalize}_n(\overline{u})_\sigma^\theta$, $\mathrm{OF}(u)$, $\mathrm{Equalize}_n(\overline{v})_\sigma^\theta$ and $\mathrm{OF}(v)$. Putting these things together, we get $\mathrm{Conv}_n^\theta(\overline{u}\{x^k \mapsto y^l\},\overline{v}\{x^k \mapsto y^l\})$, hence $\mathrm{Conv}_n^\theta(\overline{u\{x \mapsto y\}},\overline{v\{x \mapsto y\}})$. Similarly, properties $\mathrm{Equalize}_n(\overline{u\{x \mapsto y\}})_\sigma^\theta$ and $\mathrm{Equalize}_n(\overline{v\{x \mapsto y\}})_\sigma^\theta$ hold. Property $\mathrm{OF}(u)$ is of course preserved by variable renaming for any u.
- **Merge**. Assume $\mathrm{Conv}_n^\theta(x^k,\overline{s})$, $\mathrm{OF}(s)$, $\mathrm{Equalize}_n(\overline{s})_\sigma^\theta$, $\mathrm{Equalize}_n(x^k)_\sigma^\theta$, $\mathrm{Conv}_n^\theta(x^l,\overline{t})$, $\mathrm{OF}(t)$, $\mathrm{Equalize}_n(\overline{t})_\sigma^\theta$ and $\mathrm{Equalize}_n(x^l)_\sigma^\theta$. $\mathrm{Conv}_n^\theta(\overline{s},\overline{t})$ follows from $\mathrm{Conv}_n^\theta(x^k,\overline{s})$, $\mathrm{Conv}_n^\theta(x^l,\overline{t})$, $\mathrm{Equalize}_n(x^k)_\sigma^\theta$ and $\mathrm{Equalize}_n(x^l)_\sigma^\theta$. The other properties follow similarly.
- **Replace**. The proof is similar for the first 3 properties. Further, OF is preserved by replacement by Corollary 6.4.7.
- **Merep**. Similar to **Merge**. □

Example 6.4.10 (NKH)**.** Let $P = (f(x,x) = f(y,c(y)))$. Then $P \rightarrow_{\mathbf{Decomp}}$ $x = y \wedge x = c(y) \rightarrow_{\mathbf{Replace}} c(y) = y \wedge x = c(y) \rightarrow_{\mathbf{Swap}} y = c(y) \wedge x = c(y)$. Successive linearizations yield $f(x^1,x^2) = f(y^1,c(y^2))$, $x^1 = y^1 \wedge x^2 = c(y^2)$, $c(y^2) = y^1 \wedge x^2 = c(y^2)$ and $y^1 = c(y^2) \wedge x^2 = c(y^2)$. The announced properties of the solved form can be easily verified.

Corollary 6.4.11. *Let $l \to r, g \to d \in R$ and $p \in \mathcal{FP}os(l)$ such that $\mathcal{V}ar(l) \cap \mathcal{V}ar(g) = \varnothing$, and $\bar{l}|_p\theta = \bar{g}\theta$ are terms in $\mathcal{T}_{n+1}$. Then, unification of $l|_p = g$ succeeds, returning a solved form S such that, for each $z = s \in S$, $Conv^\theta_n(\bar{z},\bar{s})$, $OF(s)$, $Equalize_n(\bar{s})^\theta_\sigma$ for all σ satisfying $(\bar{l}\theta \twoheadrightarrow^{(>_{\mathcal{P}}\mathcal{FP}os(l))} l\sigma) \wedge (\bar{g}\theta \twoheadrightarrow^{(>_{\mathcal{P}}\mathcal{FP}os(g))} g\sigma)$, and further, $SOF(l|_p\eta_S) \wedge SOF(g\eta_S)$.*

Proof. Unification applies first **Decomp**. Conclude by Lemmas 6.4.9 and Corollary 6.4.7. □

Corollary 6.4.12. *Assume $t = \bar{l}\sigma$ for some $l \to r \in R$. Then, $rank(t) = 1 + rank(\sigma)$.*

Proof. Let $t = \overline{l_i}\sigma_i = \overline{l_i}\theta\gamma$ (note that γ does not depend on i), where $\theta = mgu(=_i \overline{l_i})$. Then, $\mathrm{rank}(t) = 1 + max_i\{\mathrm{rank}(\sigma_i)\} = 1 + max_i\{\mathrm{rank}(\theta\gamma)\} = 1 + \mathrm{rank}(\gamma) = 1 + \mathrm{rank}(\sigma_i)$ since θ satisfies OF at all non-variable positions by Lemma 6.4.9. □

Example 6.4.13 (NKH)**.** Consider $f(c(g),c(g))$ of rank 2, using either linearized left-hand side $f(x^1,x^2)$ or $f(y^1,c(y^2))$ to match $f(c(g),c(g))$. Corresponding substitutions have rank 1.

A major consequence is that the preparatory phase of sub-rewriting operates on terms of a strictly smaller rank. This would not be true anymore, of course, with a conversion-based preparatory phase. More generally, we can also show that the rank of terms does not increase – but may remain stable – when taking a subterm, a property which is not true of non-layered systems. Consider the system $\{f(g(h(x))) \to x,\ g(x) \to x,\ h(x) \to x\}$. The redex $f(g(h(a)))$ has rank 1 with our definition, but its subterm $g(h(a))$ has rank 2.

6.4.3 Testing Confluence of Layered Systems via Cyclic Critical Pairs

Since R is rank non-increasing we shall prove confluence by induction on the rank of terms. Since rewriting is rank non-increasing, the set of $\mathcal{T}_n$-conversions is closed under diagram rewriting, hence allowing us to use Corollary 2.2.12.

Definition 6.4.14 (Cyclic Critical Pairs)**.** Given a layered rewrite system R, let $l \to r, g \to d \in R$ and $p \in \mathcal{FP}os(l)$ such that $\mathcal{V}ar(l) \cap \mathcal{V}ar(g) = \varnothing$, and $l|_p = g$ is unifiable with canonical cyclic unifier $\langle \eta_S = \{\vec{x} \mapsto \vec{u}\}, R_S = \{\vec{y} \to \vec{v}\}\rangle$. Then, $r\eta_S \;{}_R\!\!\leftarrow l\eta_S =^{cc}_{R_S\eta_S} l[g]_p\eta_S \to_R l[d]_p\eta_S$ is a *cyclic critical peak*, and $\langle r\eta_S, l[d]_p\eta_S\rangle$ is a *cyclic critical pair*, which is said to be *realizable* by the substitution θ iff $(\forall y \to v \in R_S)\, y\theta \twoheadrightarrow_R \circ \;{}_R\!\!\twoheadleftarrow v\theta$.

The relationship between critical peaks and realizable cyclic critical pairs, usually called critical pair lemma, is more complex than usual:

Lemma 6.4.15 (Cyclic Critical Pair Lemma)**.** *Let $l \to r, g \to d \in R$ such that $\mathcal{V}ar(l) \cap \mathcal{V}ar(g) = \varnothing$. Let $r\sigma \;\underset{l\to r}{\overset{\Lambda}{\leftarrow}}\; l\sigma \;{}^{(>_{\mathcal{P}}\mathcal{FP}os(l))}\!\!\twoheadleftarrow \bar{l}\theta = \bar{l}\theta[\bar{g}\theta]_p \twoheadrightarrow^{(>_{\mathcal{P}}p\cdot\mathcal{FP}os(g))} \bar{l}\theta[g\sigma]_p \to^{p}_{g\to d} \bar{l}\theta[d\sigma]_p$ be a sub-rewriting local peak in $\mathcal{T}_{n+1}$, satisfying $p \in \mathcal{FP}os(l)$ and $\mathcal{V}ar(\bar{l}\theta) \cap \mathcal{V}ar(l,g) = \varnothing$. Assume further that R is Church-Rosser on the set $\mathcal{T}_n$. Then, there exists a cyclic solution $\langle\gamma, R_S\rangle$ such that S is a solved form of the unification problem $l|_p = g$, $\gamma = \eta_S\rho$ for some ρ of domain included in $\mathcal{V}ar(l,g)$, $\sigma \twoheadrightarrow_R \gamma$, and R_S is realizable by γ.*

Proof. Corollary 6.4.11 asserts the existence of a solved form $S = (\vec{x} = \vec{u} \wedge \vec{y} = \vec{v})$ of the problem $l|_p = g$. But $\langle\sigma, R_S\rangle$ may not be a cyclic solution. We shall therefore construct a new substitution γ such that $\sigma \twoheadrightarrow_{R_R} \gamma$ and $\langle\gamma, R_S\rangle$ is a cyclic solution of the problem, obtained as an instance by some substitution ρ of the most general cyclic unifier $\langle\eta_S, R_S\rangle$ by Theorem 6.3.11.

The construction of γ has two steps. The first aims at forcing the equality constraints given by S. This step will result in each parameter having possibly many different values. The role of the second step will be to construct a single value for each parameter.

We start equalizing independently equations $z=s \in S$. Since $\mathrm{Conv}_n^\theta(z^j,\overline{s})$, $\mathrm{Equalize}_n(z^j)_\sigma^\theta$ and $\mathrm{Equalize}_n(\overline{s})_\sigma^\theta$, Lemma 6.4.8 ensures that $z\sigma$ and $s\sigma$ are n-convertible. By assumption, $z\sigma$ and $s\sigma$ are joinable, hence there exists a term t_z^s such that $z\sigma \twoheadrightarrow_R t_z^s\ {}_R\!\twoheadleftarrow s\sigma$. Since $\mathrm{OF}(s)$ by Corollary 6.4.11, the derivation from $s\sigma$ to t_z^s must occur at positions below $\mathcal{FP}os(s)$. Maintaining equalities in $s\sigma$ between different occurrences of each variable in $\mathcal{V}ar(s)$, we get $t_z^s = s\tau_z^s$ for some τ_z^s. For each parameter p, $p\sigma \twoheadrightarrow_R p\tau_z^s$, hence the elements of the non-empty set $\{p\tau_z^s \mid p \in \mathcal{V}ar(s) \text{ for some } z = s \in S\}$ are n-convertible thanks to rank non-increasingness. By our Church-Rosser assumption, they can all be rewritten to a same term t_p. We now define γ:

(i) parameters. Given $p \in \mathcal{P}$, we define $\gamma(p) = t_p$. By construction, $p\sigma \twoheadrightarrow_R t_p = p\gamma$.

(ii) finite variables. Given $x = u \in \vec{x} = \vec{u}$, let $\gamma(x) = u\gamma_{|\mathcal{P}}$, thus $x\gamma = u\gamma$. By construction, $x\sigma \twoheadrightarrow_R u\tau_x^u \twoheadrightarrow_R u\gamma$, hence $x\sigma \twoheadrightarrow_R x\gamma$.

(iii) cyclic variables. Given $y = v \in \vec{x} = \vec{u}$, let $\gamma(y) = y\sigma$, making $y\sigma \twoheadrightarrow_R y\gamma$ trivial.

(iv) variables in $\mathcal{V}ar(l,g) \setminus \mathcal{V}ar(l|_p,g)$, that is, those variables from the context $l[\cdot]_p$ which do not belong to the unification problem $l|_p = g$, hence to the solved form S. Given $z \in \mathcal{V}ar(l,g) \setminus \mathcal{V}ar(l|_p,g)$, let $\gamma(z) = z\sigma$, making $z\sigma \twoheadrightarrow_R z\gamma$ trivial.

Therefore $\sigma \twoheadrightarrow_R \gamma$. We proceed to show $\langle\gamma, R_S\rangle$ is a cyclic solution of $l|_p = g$. Take $\rho = \gamma|_{\neg\vec{x}}$. It is routine to see $\gamma = \eta_S\rho$, and to check that $\langle\eta_S, R_S\rangle$ is a cyclic unifier of S by Definition 6.3.7, hence of $l|_p = g$ by Lemma 6.3.10. Hence the statement.

We end up the proof by noting that γ is a realizer of R_S. □

In case of NKH, the lemma is straightforward since solved forms have no parameters.

Our proof strategy for proving confluence of layered systems is as follows: assuming that n-convertible terms are joinable, we show that $(n+1)$-convertible terms are $(n+1)$-joinable by exhibiting appropriate joinably decreasing diagrams for all their local peaks. To this end, we need to define a labelling schema for sub-rewriting. Assuming that each rule has a natural number index, different rules having possibly the same index, a step $u \rightarrow^p_{R_R} v$ with the rule $l_i \rightarrow_i r_i$ is labelled by the pair $\langle \text{rank}(u|_p), i\rangle$ composed of the rank of the redex and then the rule index. Pairs are compared in the order $\trianglerighteq = (\geq, \geq)_{lex}$ whose strict part is well-founded. Indexes give more flexibility (shared indexes give even more) in finding decreasing diagrams for critical pairs, this is their sole use.

Definition 6.4.16. Let $l \rightarrow_i r, g \rightarrow_j d \in R$ and $p \in \mathcal{FP}os(l)$ such that $l|_p = g$ has a solved form S. Then, the cyclic critical pair $\langle r\eta_S, l[d]_p\eta_S\rangle$ has a *cyclic-joinable decreasing diagram* if $r\eta_S \twoheadrightarrow^{\langle 1,I\rangle}_R s =^{cc}_{R_S\eta_S} t \; {}^{\langle 1,J\rangle}_{R}\!\twoheadleftarrow l[d]_p\eta_S$, whose sequences of indexes I and J satisfy the decreasingness condition, with the additional condition, in case $\mathcal{V}ar(l[\cdot]_p) \neq \varnothing$, that all steps have a rule index $k < i$.

By Corollary 6.4.11, the ranks of $l\eta_S$ and $l[g]_p\eta_S$ are 1. Thanks to rank non-increasingness and Definition 6.4.3, the cyclic-joinable decreasing diagram – but the congruence closure part – is made of terms of rank 1 except possibly s and t which may have rank 0. It follows that all redexes rewritten in the diagram have rank 1. The decreasingness condition is therefore ensured by the rule indexes, which justifies our formulation.

Note further that the condition $\mathcal{V}ar(l[\cdot]_p) = \varnothing$ is automatically satisfied when $p = \Lambda$, hence no additional condition is needed in case of a root overlap. In case where $\mathcal{V}ar(l[\cdot]_p) \neq \varnothing$, implying a non-root overlap, the additional condition aims at ensuring that the decreasing diagram is *stable* under substitution. It implies in particular that there exists no i-facing step. This may look restrictive, and indeed, we are able to prove a slightly better condition: (i) there exists no i-facing step, and (ii) each step $u \rightarrow^q_k v$ using rule k at position q satisfies $k < i$ or $\mathcal{V}ar(u|_q) \subseteq \mathcal{V}ar(g\eta_S)$. We will restrict ourselves here to the simpler condition which yields a less involved confluence proof.

We can now state and prove our main result:

Theorem 6.4.17. *Rank non-increasing layered systems are confluent provided their realizable cyclic critical pairs have cyclic-joinable decreasing diagrams.*

Proof. Since $\rightarrow_R \subseteq \rightarrow_{R_R} \subseteq \twoheadrightarrow_R$, R-convertibility and R_R-convertibility coincide. We can therefore apply Corollary 2.2.12 to R_R-conversions, and reason by induction on the rank. We proceed by inspection of the sub-rewriting local peaks $v \;{}_{(l\to r)_R}\!\overset{p}{\leftarrow}\; u \rightarrow^q_{(g\to d)_R} w$, with $\mathcal{V}ar(l) \cap \mathcal{V}ar(g) = \varnothing$. We also assume for convenience that $\mathcal{V}ar(l, g) \cap \mathcal{V}ar(u, v, w) = \varnothing$. This allows us to consider u, v, w as ground terms by adding their variables as new constants. We assume further that variables $x, y \in \mathcal{V}ar(l, g)$ become linearized variables x^i, y^j in $\bar{l}, \overline{g}$, and that ξ is the substitution such that $\xi(x^i) = x$ and $\xi(y^j) = y$, hence implying $\mathcal{V}ar(\bar{l}) \cap \mathcal{V}ar(\overline{g}) = \varnothing$.

By definition of sub-rewriting, $u|_p = \bar{l}\theta \twoheadrightarrow_R^{(>_{\mathcal{P}}\mathcal{FP}os(l))} v'|_p = l\sigma$ and $v = u[r\sigma]_p$, where for all positions $o \in \mathcal{P}os(l)$ such that $l|_o = x$ and $\bar{l}|_o = x^i$, then $x^i\theta \twoheadrightarrow_R x\sigma$. Similarly, $u|_q = \overline{g}\theta \twoheadrightarrow_R^{(>_{\mathcal{P}}\mathcal{FP}os(g))} w'|_q = g\sigma$ and $w = u[d\sigma]_q$, where for all positions $o \in \mathcal{P}os(g)$ such that $g|_o = y$ and $\overline{g}|_o = y^j$, then $y^j\theta \twoheadrightarrow_R y\sigma$. There are three cases:

1. $p\#q$. The case of disjoint redexes is as usual for rule labelling, since ranks are only determined by the redexes, which are not changed.

2. $q >_{\mathcal{P}} p \cdot \mathcal{FP}os(l)$, the so-called ancestor peak case, for which sub-rewriting shows its strength. W.l.o.g. we assume $u|_p$ has some rank $n + 1$ and note that $u|_q$ has some rank $m \leq n$ by Corollary 6.4.12. Since the sub-rewrite steps from u to w occur strictly below $p \cdot \mathcal{FP}os(l)$, then $q = p \cdot o \cdot q'$ where $l|_o = \xi(y^j)$ and $\bar{l}|_o = y^j$. It follows that $w = \bar{l}\tau$ for some τ which is equal to θ for all variables in $\bar{l}$ except y^j for which $\tau(y^j) = \theta(y^j)[d\sigma]_{q'}$.

   We proceed as follows: we equalize all n-convertible terms $\{x\sigma \mid x \in \mathcal{V}ar(r)\}$ in v and $\{y\tau \mid y \in \mathcal{V}ar(\bar{l})\}$ in w by induction hypothesis, yielding s, t. Note that steps from v to s have ranks strictly less than the rank $n + 1$ of the step $u \rightarrow_{R_R} v$ by Corollary 6.4.12 and rank non-increasingness. Then, t is an instance of l by some γ, and s is the corresponding instance of r, hence t rewrites to s with $l \rightarrow r$. The equalization steps from w to t have ranks which are not guaranteed to be strictly less than m, hence cannot be kept to build a decreasing diagram. But they can be absorbed in a sub-rewrite step from w to

s whose first label is at most $n+1$, hence faces the step $u \to_{R_R} v$: sub-rewriting allows us to rewrite directly from w to s, short-cutting the rewrites from w to t that would otherwise yield a non-decreasing diagram. The proof is depicted at Figure 6.1, assuming $p = \Lambda$ for simplicity. Black color is used for the given sub-rewriting local peak, blue for arrows whose redexes have ranks at most $n+1$, and red when redex has rank at most n.

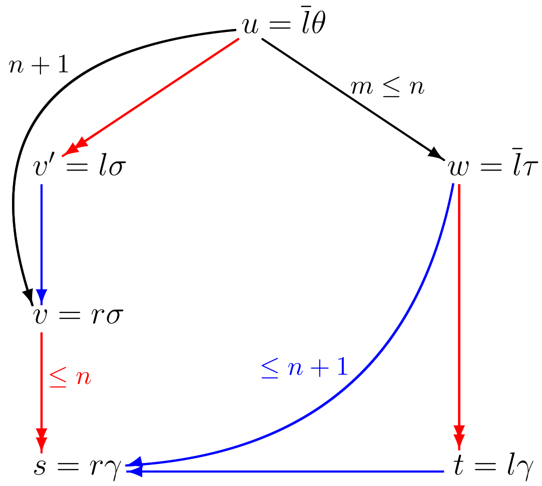


Figure 6.1: Ancestor Peak

3. $q \in p \cdot \mathcal{FP}os(l)$, the so-called critical case, whose left and right rewrite steps have labels $\langle n{+}1, i\rangle$ and $\langle m, j\rangle$, respectively, with rules $l \to r$ and $g \to d$ having indexes i and j. Assuming without loss of generality that $p = \Lambda$, the proof is depicted at Figure 6.2. Most technical difficulties here originate from the fact that the context $l[\cdot]_q$ may have variables. In this case, we first rewrite w to $t' = l\sigma[d\sigma]_q = l[d]_q\sigma$ by replaying those equalization steps, of rank at most n, used in the derivation from u to v', which apply to variable positions in $\mathcal{V}ar(\bar{l}[\cdot]_q)$.

   Now, since $\bar{l}\theta = \bar{l}\theta[\bar{g}\theta]_q$, by Lemma 6.4.15, there is a substitution γ and a solved form S of the unification problem $l|_q = g$, such that $\sigma \twoheadrightarrow_R \gamma$, $\gamma = \eta_S\rho$ for some ρ, and R_S is realizable by γ. By assumption, the cyclic critical pair $\langle r\eta_S, l[d]_q\eta_S\rangle$ has a cyclic-joinable decreasing

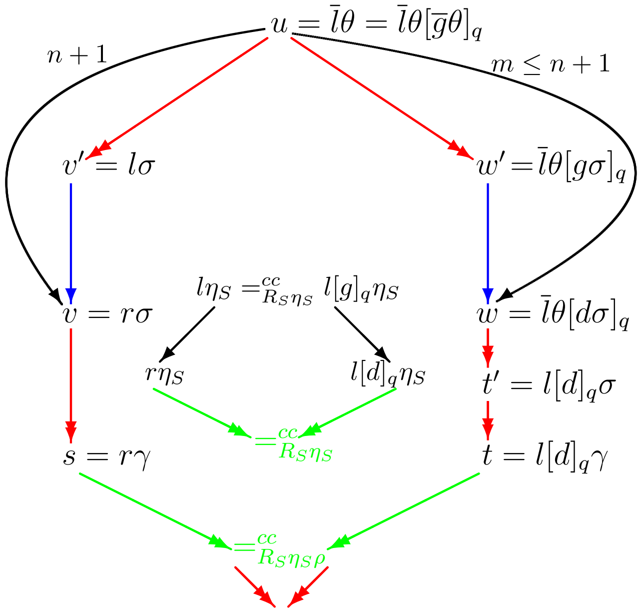


Figure 6.2: Critical Peak

diagram (modulo $=^{cc}_{R_S\eta_S}$). We can now lift this diagram to the pair $\langle s, t\rangle$ by instantiation with the substitution ρ. The congruence closure used in the lifted diagram becomes therefore $=^{cc}_{R_S\eta_S\rho}$. We are left showing that the obtained diagram for the pair $\langle v, w\rangle$ is decreasing with respect to the local peak $v \leftarrow u \rightarrow w$.

This diagram is made of three distinct parts: the equalization steps, the rewrite steps instantiating the cyclic-joinability assumption with ρ, which originate from s and t – we call them the middle part –, and the congruence closure steps. By Corollary 6.4.12, the left equalization steps $v = r\sigma \twoheadrightarrow_R r\gamma = s$ use rewrites with redexes of rank at most n, hence their labels are strictly smaller than $\langle n+1, i\rangle$. The right equalization steps $w \twoheadrightarrow t' \twoheadrightarrow t$ are considered together with the (green-)middle-part rewrite steps. There are two cases depending on whether $l[\cdot]_q$ is variable-free or not:

a) $\mathcal{V}ar(l[\cdot]_q) = \varnothing$, hence $m = n+1$ by Corollary 6.4.12. In this case, $w = t'$, and by Corollary 6.4.12, the rewrite steps $w =$

$l[d]_q\sigma \twoheadrightarrow_R l[d]_q\gamma = t$ have redexes of rank at most n, making their labels strictly smaller than $\langle m, j\rangle = \langle n+1, j\rangle$. Let us now consider the middle-part rewrite steps. Thanks to rank non-increasingness, all terms in this part have rank at most $n+1$. It follows that the associated labels are pairs of the form $\{\langle n', i'\rangle \mid n' \leq n+1, i' \in I\}$ on the left, or $\{\langle n', j'\rangle \mid n' \leq n+1, j' \in J\}$ on the right. The assumption that I, J satisfy the decreasingness condition for the critical peak ensures that these rewrites do satisfy the decreasingness condition with respect to the local peak $v \leftarrow u \rightarrow w$ as well.

b) $\mathcal{V}ar(l[\cdot]_q) \neq \varnothing$. By Corollary 6.4.12, the right equalization steps $w \twoheadrightarrow t' \twoheadrightarrow t$ have redexes of rank at most n, making their labels strictly smaller than $\langle n+1, i\rangle$. Consider now the middle part. Thanks to rank non-increasingness and the additional condition on the cyclic-joinability assumption of the cyclic critical pair, all labels $\langle n', k\rangle$ in the middle part satisfy $n' \leq n+1$ and $k < i$, hence are strictly smaller than $\langle n+1, i\rangle$.

We are left with the congruence closure steps. Given $y = v \in R_S$, $y\gamma \twoheadrightarrow_R \circ {}_R\twoheadleftarrow v\gamma$ since R_S is realizable by γ. By Lemma 6.4.9, $\mathrm{OF}(v)$ holds, hence $y\gamma$ and $v\gamma$ are n-convertible by rank non-increasingness. We are left with replacing the $=^{cc}_{\vec{y}\gamma=\vec{v}\gamma}$-steps by a joinability diagram whose all steps have rank at most n. The obtained diagram is therefore decreasing, which ends the proof. $\square$

Using the improved condition of cyclic-joinability mentioned after Definition 6.4.16 requires modifying the discussion concerning the (green-)middle-part rewrite steps. Although this does not cause any conceptual difficulties, it is technically delicate. The interested reader can try to reconstruct this proof for himself or herself.

Our result gives an answer to NKH: confluence of critical pair free rewrite systems can be analyzed via their sub-rewriting critical pairs, which are actually the cyclic critical pairs.

NKH is critical pair free but non-confluent. Indeed, it has the Ω solved form $x = c(y) \wedge y = c(y)$ obtained by unifying $f(x,x) = f(y,c(y))$. The cyclic critical peak is then $a \leftarrow f(x,x) =^{cc} f(y,c(y)) \rightarrow b$ yielding the cyclic critical pair $\langle a,b \rangle$ which is not joinable modulo $\{x = c(y),\ y = c(y)\}$.

We now give a slight modification of NKH making it confluent:

Example 6.4.18. The system $R = \{f(x,x) \rightarrow_2 a(x,x),\ f(x,c(x)) \rightarrow_2 b(x),\ f(c(x),c(x)) \rightarrow_3 f(x,c(x)),\ a(x,x) \rightarrow_1 e(x),\ b(x) \rightarrow_1 e(c(x)),\ g \rightarrow_0 c(g)\}$ is confluent. Showing that R satisfies (DLO) is routine, and it is rank non-increasing by Lemma 6.4.5. There are three cyclic critical pairs, which all have a cyclic-joinable decreasing diagram. For instance, the unification problem $f(x,x) = f(y,c(y))$ returns a canonical cyclic unifier $\langle \eta_S = \varnothing,\ R_S = \{x \rightarrow c(y),\ y \rightarrow c(y)\} \rangle$, the corresponding cyclic critical peak $a(x,x)\ {}^{\langle 1,2 \rangle}\!\!\leftarrow f(x,x) =^{cc}_{R_S \eta_S} f(y,c(y)) \rightarrow^{\langle 1,2 \rangle} b(y)$ has a cyclic-joinable decreasing diagram $a(x,x) \rightarrow^{\langle 1,1 \rangle} e(x) =^{cc}_{R_S \eta_S} e(c(y))\ {}^{\langle 1,1 \rangle}\!\!\leftarrow b(y)$. The unification problem $f(x,x) = f(c(y),c(y))$ returns $\langle \eta_S = \{x = c(y)\},\ R_S = \varnothing \rangle$, the corresponding (normal) critical peak $a(c(y),c(y))\ {}^{\langle 1,2 \rangle}\!\!\leftarrow f(c(y),c(y)) \rightarrow^{\langle 1,3 \rangle} f(y,c(y))$ decreases by $a(c(y),c(y)) \rightarrow^{\langle 1,1 \rangle} e(c(y))\ {}^{\langle 1,1 \rangle}\!\!\leftarrow b(y)\ {}^{\langle 1,2 \rangle}\!\!\leftarrow f(y,c(y))$. By Theorem 6.4.17, R is confluent.

Theorem 6.4.17 can be easily used positively: if all cyclic critical pairs have cyclic-joinable decreasing diagrams, then confluence is met. This was the case in Example 6.4.18. But there is another positive use that we illustrate now: showing that $\{f(x,x) \rightarrow a,\ f(x,c(x)) \rightarrow b,\ g \rightarrow d(g)\}$ is confluent requires proving that the cyclic critical pair given by unifying the first two rules is not realizable. Although realizability is undecidable in general, this is the case here since there is no term s convertible to $c(s)$. Theorem 6.4.17 can also be used negatively by exhibiting some realizable cyclic critical pair which is not joinable: this is the case of example NKH. In general, if some realizable cyclic critical pair leading to a local peak is not joinable, then the system is non-confluent. Whether a realizable cyclic critical pair always yields a local peak is still an open problem which we had no time to investigate yet.

A main assumption of our result is that rules may not increase the rank. One can of course challenge this assumption, which could be due to the proof method itself. The following counter-example shows that it is not the case.

Example 6.4.19. Consider $R = \{d(x,x) \to 0,\ f(x) \to d(x, f(x)),\ c \to f(c)\}$ due to Klop, which predates NKH, as an example of critical pair free but non-confluent system. It is layered but its second rule is rank increasing since $d(x, f(x))$ has rank 2 while $f(x)$ has rank 1. This system is non-confluent, since $f(f(c)) \to d(f(c), f(f(c))) \to d(f(f(c)), f(f(c))) \to 0$ while $f(f(c)) \to f(d(c, f(c))) \to f(d(f(c), f(c))) \to f(0)$ which generates the regular tree language $\{S \to d(0,S),\ S \to f(0)\}$ not containing 0. Note that replacing the second rule by the right-linear rule $f(x) \to d(x, f(c))$ yields a confluent system [SO10].

Releasing rank non-increasingness would indeed require strengthening another assumption, possibly imposing left- or right-linearity.

6.5 Conclusion

The decreasing diagrams method has shown its power to study confluence of non-terminating systems based on critical pairs computing. Our results give a partial solution by allowing non-terminating rules which can also be non-linear on the left as well as on the right. The notion of layered systems is our first conceptual contribution here.

Another, technical contribution of our work is the generalized notion of sub-rewriting, which can indeed be compared to parallel rewriting. Both relations contain plain rewriting, and are included in its transitive closure. That is, $\to\ \subseteq\ \to_{R_R}\ \subseteq\ \to^+$ and $\to\ \subseteq\ \Rightarrow\ \subseteq\ \to^+$. Both can therefore be used for studying confluence of plain rewriting. Tait and Martin-Löf's parallel rewriting – as presented by Barendregt in his famous book on λ-calculus [Bar84] – has been recognized as the major tool for studying confluence of left-linear non-terminating rewrite relations when they are not right-linear. We believe that sub-rewriting will be equally successful for studying confluence of non-terminating rewrite relations that are not left-linear. In the present work where no linearity assumption is made, assumption (DLO) ensuring the absence of stacked critical pairs in left-hand sides makes the combined use of sub-rewriting and parallel rewriting superfluous. Without that assumption, as is the case in Chapter 5, their combined use becomes necessary.

A last contribution, both technical and conceptual, is the notion of cyclic unifiers. Although their study is still preliminary, we have shown that they constitute a powerful new tool to handle unification problems with cyclic equations in the same way we deal with unification problems without cyclic equations, thanks to the existence of most general cyclic unifiers which generalize the usual notion of most general unifiers. This indeed opens the way to a *uniform treatment* of problems where unification, whether finite or infinite, plays a central role.

As mentioned in Chapter 5, our long-term goal goes beyond improving the current toolkit for carrying out confluence proofs for non-terminating rewrite systems. We aim at designing new tools for showing confluence of complex type theories (with dependent types, universes and dependent elimination rules) directly on raw terms, which would ease the construction of strongly normalizing models for typed terms. Since redex-depth, the notion of rank used here, does not behave well for higher-order rules, as the case in Chapter 5, appropriate new notions of ranks are still required in that setting.

Seven

Conclusion

In this thesis, we presented a thorough investigation of the notion of decreasing diagrams, from the notion itself up to its applications, aiming at confluence proofs of non-terminating non-left-linear rewrite systems based on critical-pair analysis. Along this journey, we inspect the notion at three different levels.

At the abstract level, we first revise the proof of the decreasing diagrams method in Chapter 3. An alternative simpler proof is given, allowing to generalize the method, as well as its completeness, to the modulo case. The basis of the completeness result, cofinal derivation due to Klop [Klo80], leads to new proofs of existing modularity results [Toy87, JT08]. Moreover, we extend the decreasing diagrams technique with a multi-labelled version in Chapter 4, which enhances the expressivity of the technique by localizing global measures of conversions into step labels.

Then still in Chapter 4, following the work by Jouannaud and Li [JL12a], we move our focus onto a slightly more concrete level of rewriting, called abstract positional rewriting. The decreasing diagrams method is lifted to abstract positional rewrite relations, where (abstract) positional information is available to bridge the gap between abstract rewriting and term rewriting.

Finally at the concrete term level, we investigate different classes of non-terminating non-left-linear term rewrite systems by decreasing diagrams via introducing a new rewrite relation, sub-rewriting, in the following two chapters. In Chapter 5, inspired by the work of Jouannaud and van Oostrom [JvO09], we prove that the confluence of a union of two systems – one is terminating, the other is non-left-linear, rank non-increasing and possibly non-terminating – can be reduced to the existence of decreasing diagrams for its various kinds of critical pairs, based on a signature split. In Chapter 6, motivated by a famous example raised by Huet [Hue80], we demonstrate, in absence of signature assumptions, that rank non-increasing layered systems are confluent provided their cyclic critical pairs have cyclic-joinable decreasing diagrams. Since there is no signature split, the notion of rank is of course different, and indeed, intrinsic.

These various issues are still worth investigating.

One interesting direction would be to draw a complete picture of decreasing diagrams in the NARS framework [JL12a]. While the strength of the NARS framework is its capability to unify existing rewriting definitions, and therefore their Church-Rosser properties assuming some terminating property, the power of the decreasing diagrams technique is its ability to capture confluence proofs at the abstract level no matter whether the rewrite relation terminates or not. It seems a natural idea to combine this two elegant frameworks to build a comprehensive new setting in order to study the Church-Rosser properties of possibly non-terminating systems based on their critical pairs at an abstract level, even in presence of equations and simplifiers. The efforts made in Chapter 4 are only preliminary. A thorough investigation is needed.

Another important direction that we have not touched is the use of the decreasing diagrams method in conditional rewriting, in which case the use of the rewrite rules is subjected to conditions to be satisfied. Conditional rewriting is the basis of rewriting-based, declarative programming languages, such as Maude [CDE+02, CDE+07], CafeOBJ [DF98a] and ELAN [BKK+96, BKK+98], which have shown their power in describing and verifying network protocols, cryptographic protocols, embedded systems to cite a few [Mes12]. We realize that our notion of sub-rewriting is somehow related to conditional rewriting with left-linear rules and the conditions are joinability predicates between variables. We suspect that applying the decreasing diagrams method to conditional rewriting will allow to enhance the capabilities of these formal verification tools.

Our long-term goal goes beyond improving the current toolkit for higher-order computations. We are interested in carrying out confluence proofs for complex type theories, with dependent types, universes, dependent elimination rules, directly on untyped terms. Three properties of a type theory – type preservation, strong normalization and confluence – are essential to prove consistency and decidability of type checking. However in dependent type theories, confluence and type preservation are needed to build strongly normalizing models; confluence is needed to show preservation of product types by rewriting, which is an essential ingredient of the type preservation proof; type preservation is needed to show that derivations issued from well-typed terms are well-typed, which is an essential ingredient of the confluence proof. One can break this circularity in two ways: by proving all three properties together within a single huge induction [Gog94]; or by proving confluence on untyped terms, then allowing to prove successively type preservation, confluence on typed terms, and strong normalization, which motivates our long-term objective. Since β-reduction becomes then non-terminating in the latter case, the only potential technique of use is that of decreasing diagrams. Current techniques for showing confluence by using decreasing diagrams in higher-order rewrite systems [vO97], admit type theories in which the rules are left-linear, have development closed critical pairs, and do not build associativity and commutativity into pattern matching. But allowing for non-left-linear rules and/or for non-trivial critical pairs, and computing over non-free data structures like sets and/or abstraction, is out of scope of current techniques. Such computations are however present in type theories such as in Dedukti[1], and, more recently, in Agda[2]. We have already started promising investigations in this direction for the $\lambda\Pi$-calculus modulo [CD07, Ass15], the theory on which Dedukti is based. One important thing we have learned from this thesis is that, decreasing diagrams make it possible to work modularly: we can split a rewrite system

[1]The INRIA project Dedukti is described at `http://dedukti.gforge.inria.fr/`

[2]The Agda project is described at `http://wiki.portal.chalmers.se/agda`

into different pieces, and even split and/or duplicate a rewrite relation into different ones, and discriminate them by labelling them appropriately. This technique can be very useful for higher-order rewrite systems as well, as shown by a recent work of Ali Assaf, Gilles Dowek, Jean-Pierre Jouannaud and myself, presented in workshop HOR [ADJL16]. Dependent type theories that allow for user-defined rewrite rules in addition to β-reduction, like Dedukti and Agda, are good targets for such techniques. We believe that we have opened the way to using a technique that will play a key role in proving confluence in type theory.

Bibliography

[ADJL16] Ali Assaf, Gilles Dowek, Jean-Pierre Jouannaud, and Jiaxiang Liu. Untyped Confluence in Dependent Type Theories. In *Proceedings Higher-Order Rewriting Workshop*, Porto, Portugal, June 2016.

[Ass15] Ali Assaf. *A framework for defining computational higher-order logics. (Un cadre de définition de logiques calculatoires d'ordre supérieur).* PhD thesis, École Polytechnique, Palaiseau, France, 2015.

[AT97] Takahito Aoto and Yoshihito Toyama. Persistency of confluence. *J. UCS*, 3(11):1134–1147, 1997.

[AT12] Takahito Aoto and Yoshihito Toyama. A reduction-preserving completion for proving confluence of non-terminating term rewriting systems. *Logical Methods in Computer Science*, 8(1), 2012.

[ATU14] Takahito Aoto, Yoshihito Toyama, and Kazumasa Uchida. Proving confluence of term rewriting systems via persistency and decreasing diagrams. In Dowek [Dow14], pages 46–60.

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

[BC04] Yves Bertot and Pierre Castéran. *Interactive Theorem Proving and Program Development - Coq'Art: The Calculus of Inductive*

Constructions. Texts in Theoretical Computer Science. An EATCS Series. Springer, 2004.

[BD07] Maria Paola Bonacina and Nachum Dershowitz. Abstract canonical inference. *ACM Trans. Comput. Log.*, 8(1), 2007.

[BKK+96] Peter Borovanský, Claude Kirchner, Hélène Kirchner, Pierre-Etienne Moreau, and Marian Vittek. ELAN: A logical framework based on computational systems. *Electr. Notes Theor. Comput. Sci.*, 4:35–50, 1996.

[BKK+98] Peter Borovanský, Claude Kirchner, Hélène Kirchner, Pierre-Etienne Moreau, and Christophe Ringeissen. An overview of ELAN. *Electr. Notes Theor. Comput. Sci.*, 15:55–70, 1998.

[BN98] Franz Baader and Tobias Nipkow. *Term rewriting and all that*. Cambridge University Press, 1998.

[CC77] Patrick Cousot and Radhia Cousot. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In Robert M. Graham, Michael A. Harrison, and Ravi Sethi, editors, *Conference Record of the Fourth ACM Symposium on Principles of Programming Languages, Los Angeles, California, USA, January 1977*, pages 238–252. ACM, 1977.

[CD07] Denis Cousineau and Gilles Dowek. Embedding pure type systems in the lambda-Pi-calculus modulo. In Simona Ronchi Della Rocca, editor, *Typed Lambda Calculi and Applications, 8th International Conference, TLCA 2007, Paris, France, June 26-28, 2007, Proceedings*, volume 4583 of *Lecture Notes in Computer Science*, pages 102–117. Springer, 2007.

[CDE+02] Manuel Clavel, Francisco Durán, Steven Eker, Patrick Lincoln, Narciso Martí-Oliet, José Meseguer, and Jose F. Quesada. Maude: specification and programming in rewriting logic. *Theor. Comput. Sci.*, 285(2):187–243, 2002.

[CDE+07] Manuel Clavel, Francisco Durán, Steven Eker, Patrick Lincoln, Narciso Martí-Oliet, José Meseguer, and Carolyn L. Talcott, editors. *All About Maude - A High-Performance Logical Framework, How to Specify, Program and Verify Systems in Rewriting Logic*, volume 4350 of *Lecture Notes in Computer Science*. Springer, 2007.

[CGP01] Edmund M. Clarke, Orna Grumberg, and Doron A. Peled. *Model checking*. MIT Press, 2001.

[Col82] Alain Colmerauer. Prolog and infinite trees. *Logic Programming*, 16:231–251, 1982.

[Col84] Alain Colmerauer. Equations and inequations on finite and infinite trees. In *FGCS*, pages 85–99, 1984.

[Cou83] Bruno Courcelle. Fundamental properties of infinite trees. *Theor. Comput. Sci.*, 25:95–169, 1983.

[CR36] Alonzo Church and J. B. Rosser. Some properties of conversion. *Transactions of the American Mathematical Society*, 39(3):472–482, 1936.

[dB78] N. G. de Bruijn. A note on weak diamond properties. Memorandum 78–08, Eindhoven University of Technology, 1978.

[DF98a] Razvan Diaconescu and Kokichi Futatsugi. *CafeOBJ Report - The Language, Proof Techniques, and Methodologies for Object-Oriented Algebraic Specification*, volume 6 of *AMAST Series in Computing*. World Scientific, 1998.

[DF98b] Razvan Diaconescu and Kokichi Futatsugi. An overview of CafeOBJ. *Electr. Notes Theor. Comput. Sci.*, 15:285–298, 1998.

[DJ90] Nachum Dershowitz and Jean-Pierre Jouannaud. Rewrite systems. In *Handbook of Theoretical Computer Science, Volume B: Formal Models and Semantics (B)*, pages 243–320. 1990.

[DOS87] Nachum Dershowitz, Mitsuhiro Okada, and G. Sivakumar. Confluence of conditional rewrite systems. In Stéphane Kaplan and Jean-Pierre Jouannaud, editors, *Conditional Term Rewriting Systems, 1st International Workshop, Orsay, France, July 8-10, 1987, Proceedings*, volume 308 of *Lecture Notes in Computer Science*, pages 31–44. Springer, 1987.

[Dow14] Gilles Dowek, editor. *Rewriting and Typed Lambda Calculi - Joint International Conference, RTA-TLCA 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14-17, 2014. Proceedings*, volume 8560 of *Lecture Notes in Computer Science*. Springer, 2014.

[Fel13a] Bertram Felgenhauer. Personal communication, 2013.

[Fel13b] Bertram Felgenhauer. Rule labeling for confluence of left-linear term rewrite systems. In *International Workshop on Confluence*, pages 23–27, 2013.

[FvO13] 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.

[Ges90] Alfons Geser. *Relative Termination*. PhD thesis, University of Passau, Germany, 1990.

[GLM92] Georges Gonthier, Jean-Jacques Lévy, and Paul-André Melliès. An abstract standardisation theorem. In *Proceedings of the Seventh Annual Symposium on Logic in Computer Science (LICS '92), Santa Cruz, California, USA, June 22-25, 1992*, pages 72–81. IEEE Computer Society, 1992.

[Gog94] 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.

[GOO96] Hiroshi Gomi, Michio Oyamaguchi, and Yoshikatsu Ohta. On the Church-Rosser property of non-E-overlapping and strongly depth-preserving term rewriting systems. *IPSJ*, 37(12):2147–2160, 1996.

[GOO98] Hiroshi Gomi, Michio Oyamaguchi, and Yoshikatsu Ohta. On the Church-Rosser property of root-E-overlapping and strongly depth-preserving term rewriting systems. *IPSJ*, 39(4):992–1005, 1998.

[Gra96] Bernhard Gramlich. Confluence without termination via parallel critical pairs. In Hélène Kirchner, editor, *Trees in Algebra and Programming - CAAP'96, 21st International Colloquium, Linköping, Sweden, April, 22-24, 1996, Proceedings*, volume 1059 of *Lecture Notes in Computer Science*, pages 211–225. Springer, 1996.

[GRS87] Jean H. Gallier, Stan Raatz, and Wayne Snyder. Theorem proving using rigid E-unification equational matings. In *Proceedings of the Symposium on Logic in Computer Science (LICS '87), Ithaca, New York, USA, June 22-25, 1987*, pages 338–346. IEEE Computer Society, 1987.

[GWM+00] Joseph A Goguen, Timothy Winkler, José Meseguer, Kokichi Futatsugi, and Jean-Pierre Jouannaud. Introducing OBJ. In *Software Engineering with OBJ*, pages 3–167. Springer, 2000.

[Hin64] James Roger Hindley. *The Church-Rosser property and a result in combinatory logic.* PhD thesis, University of Newcastle upon Tyne, 1964.

[HM11] Nao Hirokawa and Aart Middeldorp. Decreasing diagrams and relative termination. *J. Autom. Reasoning*, 47(4):481–501, 2011.

[HR87] Jieh Hsiang and Michaël Rusinowitch. On word problems in equational theories. In Thomas Ottmann, editor, *ICALP*, volume 267 of *LNCS*, pages 54–71. Springer, 1987.

[HR91] Jieh Hsiang and Michaël Rusinowitch. Proving refutational completeness of theorem-proving strategies: The transfinite semantic tree method. *J. ACM*, 38(3):559–587, 1991.

[Hue76] Gérard Huet. Résolution d'équations dans des langages d'ordre 1,2,...,ω. Thèse de Doctorat es Sciences Mathématiques, Université Paris VII, Septembre 1976.

[Hue80] Gérard P. Huet. Confluent reductions: Abstract properties and applications to term rewriting systems. *J. ACM*, 27(4):797–821, 1980.

[JK86] Jean-Pierre Jouannaud and Hélène Kirchner. Completion of a set of rules modulo a set of equations. *SIAM J. Comput.*, 15(4):1155–1194, 1986.

[JK91] Jean-Pierre Jouannaud and Claude Kirchner. Solving equations in abstract algebras: A rule-based survey of unification. In *Computational Logic - Essays in Honor of Alan Robinson*, pages 257–321, 1991.

[JL12a] Jean-Pierre Jouannaud and Jianqi Li. Church-Rosser properties of normal rewriting. In Patrick Cégielski and Arnaud Durand, editors, *CSL*, volume 16 of *LIPIcs*, pages 350–365. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2012.

[JL12b] Jean-Pierre Jouannaud and Jiaxiang Liu. From diagrammatic confluence to modularity. *Theor. Comput. Sci.*, 464:20–34, 2012.

[JM84] Jean-Pierre Jouannaud and Miguel Muñoz. Termination of a set of rules modulo a set of equations. In Robert E. Shostak, editor, *7th International Conference on Automated Deduction, Napa,* *California, USA, May 14-16, 1984, Proceedings*, volume 170 of *Lecture Notes in Computer Science*, pages 175–193. Springer, 1984.

[JO91] Jean-Pierre Jouannaud and Mitsuhiro Okada. A computation model for executable higher-order algebraic specification languages. In *Proceedings of the Sixth Annual Symposium on Logic in Computer Science (LICS '91), Amsterdam, The Netherlands, July 15-18, 1991*, pages 350–361, 1991.

[Jou06] Jean-Pierre Jouannaud. Modular Church-Rosser modulo. In Frank Pfenning, editor, *RTA*, volume 4098 of *LNCS*, pages 96–107. Springer, 2006.

[JT08] Jean-Pierre Jouannaud and Yoshihito Toyama. Modular Church-Rosser modulo: The complete picture. *Int. J. Software and Informatics*, 2(1):61–75, 2008.

[JvO09] Jean-Pierre Jouannaud and Vincent van Oostrom. Diagrammatic confluence and completion. In Susanne Albers, Alberto Marchetti-Spaccamela, Yossi Matias, Sotiris E. Nikoletseas, and Wolfgang Thomas, editors, *ICALP (2)*, volume 5556 of *LNCS*, pages 212–222. Springer, 2009.

[KB70] Donald E. Knuth and Peter B. Bendix. Simple word problems in universal algebras. In J. Leech, editor, *Computational Problems in Abstract Algebra*, pages 263–297. Elsevier, 1970.

[KH12] Dominik Klein and Nao Hirokawa. Confluence of non-left-linear TRSs via relative termination. In *LPAR*, volume 7180 of *Lecture Notes in Computer Science*, pages 258–273. Springer, 2012.

[Kir12] Claude Kirchner. Rho-calculi for computation and logic (invited talk). In Ashish Tiwari, editor, *RTA*, volume 15 of *LIPIcs*, pages 2–4. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2012.

[Klo80] Jan Willem Klop. *Combinatory reduction systems*. PhD thesis, Univ. Utrecht, 1980.

[Klo93] Jan Willem Klop. Term rewriting systems. In *Handbook of Logic in Computer Science, Vol.2*, pages 1–116. Oxford University Press, 1993.

[KMTdV94] Jan Willem Klop, Aart Middeldorp, Yoshihito Toyama, and Roel C. de Vrijer. Modularity of confluence: A simplified proof. *Inf. Process. Lett.*, 49(2):101–109, 1994.

[LB77] Dallas S. Lankford and A. M. Ballantyne. Decision procedures for simple equational theories with commutative-associative axioms: Complete sets of commutative-associative reductions. Memo ATP-39, University of Texas, Austin, August 1977.

[LDJ14] Jiaxiang Liu, Nachum Dershowitz, and Jean-Pierre Jouannaud. Confluence by critical pair analysis. In Dowek [Dow14], pages 287–302.

[LJ14] 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.

[LJO15] 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.

[McC60] John McCarthy. Recursive functions of symbolic expressions and their computation by machine, part I. *Commun. ACM*, 3(4):184–195, 1960.

[Mes00] José Meseguer. Rewriting logic and Maude: Concepts and applications. In Leo Bachmair, editor, *RTA*, volume 1833 of *Lecture Notes in Computer Science*, pages 1–26. Springer, 2000.

[Mes11] José Meseguer. Maude. In David A. Padua, editor, *Encyclopedia of Parallel Computing*, pages 1095–1102. Springer, 2011.

[Mes12] José Meseguer. Twenty years of rewriting logic. *J. Log. Algebr. Program.*, 81(7-8):721–781, 2012.

[MO01] Ken Mano and Mizuhito Ogawa. Unique normal form property of compatible term rewriting systems: a new proof of Chew's theorem. *Theor. Comput. Sci.*, 258(1-2):169–208, 2001.

[MOOO97] Kunihiro Matsuura, Michio Oyamaguchi, Yoshikatsu Ohta, and Mizuhito Ogawa. On the E-overlapping property of nonlinear term rewriting systems (in Japanese). *IEICE*, 80-D-I(11):847–855, 1997.

[MTH90] Robin Milner, Mads Tofte, and Robert Harper. *The definition of Standard ML*. The MIT Press, Massachusetts and London, England, 1990.

[New42] M. H. A. Newman. On theories with a combinatorial definition of 'equivalence'. *Ann. Math.*, 43(2):223–243, 1942.

[Nip91] Tobias Nipkow. Higher-order critical pairs. In *Proceedings of the Sixth Annual Symposium on Logic in Computer Science (LICS '91), Amsterdam, The Netherlands, July 15-18, 1991*, pages 342–349, 1991.

[Nip98] Tobias Nipkow, editor. *Rewriting Techniques and Applications, 9th International Conference, RTA-98, Tsukuba, Japan, March 30 - April 1, 1998, Proceedings*, volume 1379 of *LNCS*. Springer, 1998.

[NKOF08] Masaki Nakamura, Weiqiang Kong, Kazuhiro Ogata, and Kokichi Futatsugi. A specification translation from behavioral specifications to rewrite specifications. *IEICE Transactions*, 91-D(5):1492–1503, 2008.

[NO80] Greg Nelson and Derek C. Oppen. Fast decision procedures based on congruence closure. *J. ACM*, 27(2):356–364, 1980.

[vO94a] Vincent van Oostrom. Confluence by decreasing diagrams. *Theor. Comput. Sci.*, 126(2):259–280, 1994.

[vO94b] Vincent van Oostrom. *Confluence for abstract and higher-order rewriting*. PhD thesis, Vrije Universiteit Amsterdam, 1994.

[vO97] Vincent van Oostrom. Developing developments. *Theor. Comput. Sci.*, 175(1):159–181, 1997.

[vO08a] Vincent van Oostrom. Confluence by decreasing diagrams converted. In Andrei Voronkov, editor, *RTA*, volume 5117 of *LNCS*, pages 306–320. Springer, 2008.

[vO08b] Vincent van Oostrom. Modularity of confluence, constructed. In Alessandro Armando, Peter Baumgartner, and Gilles Dowek, editors, *IJCAR*, volume 5195 of *LNCS*, pages 348–363. Springer, 2008.

[O'D85] Michael J. O'Donnell. Equational logic as a programming language. In Rohit Parikh, editor, *Logics of Programs, Conference, Brooklyn College, June 17-19, 1985, Proceedings*, volume 193 of *Lecture Notes in Computer Science*, page 255. Springer, 1985.

[Ohl94] Enno Ohlebusch. On the modularity of termination of term rewriting systems. *Theor. Comput. Sci.*, 136(2):333–360, 1994.

[Ohl98] Enno Ohlebusch. Church-Rosser theorems for abstract reduction modulo an equivalence relation. In Nipkow [Nip98], pages 17–31.

[Oku98] Satoshi Okui. Simultaneous critical pairs and Church-Rosser property. In Nipkow [Nip98], pages 2–16.

[OOT95] Y. Ohta, M. Oyamaguchi, and Y. Toyama. On the Church-Rosser property of simple-right-linear TRS's (in Japanese). *Trans. IEICE*, J78-D-I(3):263–268, 1995.

[ORS92] Sam Owre, John M. Rushby, and Natarajan Shankar. PVS: A prototype verification system. In Deepak Kapur, editor, *Automated Deduction - CADE-11, 11th International Conference on Automated Deduction, Saratoga Springs, NY, USA, June 15-18, 1992, Proceedings*, volume 607 of *Lecture Notes in Computer Science*, pages 748–752. Springer, 1992.

[Pau94] Lawrence C. Paulson. *Isabelle - A Generic Theorem Prover (with a contribution by T. Nipkow)*, volume 828 of *Lecture Notes in Computer Science*. Springer, 1994.

[Pot06] François Pottier. An overview of Cαml. *Electr. Notes Theor. Comput. Sci.*, 148(2):27–52, 2006.

[PS81] Gerald E. Peterson and Mark E. Stickel. Complete sets of reductions for some equational theories. *J. ACM*, 28(2):233–264, 1981.

[Ros73] Barry K. Rosen. Tree-manipulating systems and Church-Rosser theorems. *J. ACM*, 20(1):160–187, 1973.

[Sar90] Vijay A. Saraswat. The paradigm of concurrent constraint programming. In *ICLP*, pages 777–778, 1990.

[Sho82] Robert E. Shostak. Deciding combinations of theories. In Donald W. Loveland, editor, *CADE*, volume 138 of *LNCS*, pages 209–222. Springer, 1982.

[SO10] Masahiko Sakai and Mizuhito Ogawa. Weakly-non-overlapping non-collapsing shallow term rewriting systems are confluent. *Inf. Process. Lett.*, 110(18-19):810–814, 2010.

[SOO15] Masahiko Sakai, Michio Oyamaguchi, and Mizuhito Ogawa. Non-E-overlapping, weakly shallow, and non-collapsing TRSs are confluent. In Amy P. Felty and Aart Middeldorp, editors, *Automated Deduction - CADE-25 - 25th International Conference on Automated Deduction, Berlin, Germany, August 1-7, 2015, Proceedings*, volume 9195 of *Lecture Notes in Computer Science*, pages 111–126. Springer, 2015.

[Str10] Pierre-Yves Strub. Coq modulo theory. In Anuj Dawar and Helmut Veith, editors, *CSL*, volume 6247 of *Lecture Notes in Computer Science*, pages 529–543. Springer, 2010.

[Ter03] Terese. Term rewriting systems. In *Cambridge Tracts in Theoretical Computer Science (Jan Willem Klop et al editors)*, volume 55. Cambridge University Press, 2003.

[TGM11] John-Baptiste Tristan, Paul Govereau, and Greg Morrisett. Evaluating value-graph translation validation for LLVM. In *Proceedings of the ACM SIGPLAN Conference on Programming Design and Implementation (PLDI)*, New York, NY, USA, 2011. ACM.

[Tho90] Wolfgang Thomas. Automata on infinite objects. In *Handbook of Theoretical Computer Science, Volume B: Formal Models and Semantics (B)*, pages 133–192. 1990.

[TO94] Yoshihito Toyama and Michio Oyamaguchi. Church-Rosser property and unique normal form property of non-duplicating term rewriting systems. In Nachum Dershowitz and Naomi Lindenstrauss, editors, *Conditional and Typed Rewriting Systems, 4th International Workshop, CTRS-94, Jerusalem, Israel, July 13-15, 1994, Proceedings*, volume 968 of *Lecture Notes in Computer Science*, pages 316–331. Springer, 1994.

[Toy81] Yoshihito Toyama. On the Church-Rosser property of term rewriting systems (in Japanese). NTT ECL Technical Report 17672, December 1981.

[Toy87] Yoshihito Toyama. On the Church-Rosser property for the direct sum of term rewriting systems. *J. ACM*, 34(1):128–143, 1987.

[Toy88] Yoshihito Toyama. Commutativity of term rewriting systems. *Programming of future generation computers II*, pages 393–407, 1988.

[ZFM11] Harald Zankl, Bertram Felgenhauer, and Aart Middeldorp. CSI - a confluence tool. In *CADE*, volume 6803 of *Lecture Notes in Computer Science*, pages 499–505. Springer, 2011.

[ZFM15] Harald Zankl, Bertram Felgenhauer, and Aart Middeldorp. Labelings for decreasing diagrams. *J. Autom. Reasoning*, 54(2):101–133, 2015.

Index

ÉCOLE DOCTORALE
Sciences et technologies de l'information et de la communication (STIC)

Titre : Propriétés de Confluence des Règles de Réécriture par des Diagrammes Décroissants

Mots clefs : confluence, paires critiques, diagrammes décroissants

Résumé : Cette thèse porte sur la confluence de systèmes de réécriture en l'absence d'hypothèse de terminaison, pour des applications aux langages fonctionnels de premier ordre comme MAUDE ou d'ordre supérieur avec typage dépendant comme Dedukti. Dans le premier cas, les calculs portant sur des structures de données infinies ne terminent pas. Dans le second, les calculs sur les termes non typés ne terminent pas à cause de la beta-réduction. Lorsque les calculs ont la propriété de terminaison, la confluence se réduit à celle des "pics critiques", qui sont les calculs divergents minimaux issus d'un même terme, dont la paire de résultats est dite "critique". Dans le cas des calculs qui ne terminent pas, un résultat essentiel est tout ensemble de règles de calcul linéaires à gauche et sans paires critiques est confluent. Cela suggère que la notion de paire critique jouer un rôle là-encore essentiel, mais qui reste largement incompris à ce jour.
Notre étude de la confluence est basée sur la méthode des diagrammes décroissants de van Oostrom, qui généralise les techniques utilisées antérieurement, que ce soit en la présence ou en l'absence de la terminaison des calculs. Cette méthode est abstraite en le sens qu'elle s'applique à des relations quelconques sur des ensembles arbitraires.
Dans la première partie, nous révisons les résultats de van Oostrom et proposons un preuve alternative qui s'étend au cas dit "modulo", pour lequel les calculs mélangent des étapes de récriture avec d'autres qui sont purement équationnelles. Le résultat de complétude de van Oostrom est étendu lui-aussi lorsque les calculs sont fortement cohérents.
La seconde partie de cette thèse applique la méthode et sa généralisation à des systèmes de réécriture de termes, et en particulier à plusieurs probèmes ouverts du domaine.

Title : Confluence Properties of Rewrite Rules by Decreasing Diagrams

Keywords : confluence, critical pairs, decreasing diagrams

Abstract : This thesis is devoted to the confluence of rewrite systems in the absence of termination, for applications in first-order functional languages like MAUDE or higher-order languages with dependent types, as Dedukti. In the first case, the computations on infinite data structures do not terminate, while in the second case, untyped computations do not terminate because of beta-reduction. In the case where the computations terminate, confluence is reduced to that of critical peaks, the "minimal diverging computations", made of a minimal middle term called "overlap" which computes in two different ways, resulting in a so-called "critical pair". In the case of non-terminating computations, a main result is that left-linear rewrite rules that have no critical pairs are always confluent. This suggests that the notion of critical pairs plays a key role there too, but a general understanding of the confluence of non-terminating computations in terms of critical pairs is still missing.
Our investigation of confluence is based on the decreasing diagrams method due to van Oostrom, which generalizes the techniques used previously for both terminating and non-terminating computations. The method is abstract in the sense that it applies to arbitrary relations on an abstract set. In the first part, we revise the results of decreasing diagrams, and propose an alternative proof that extends the method to the "modulo" case, in which computations mix rewrite steps and equational steps. Van Oostrom's completeness result, showing that decreasing diagrams always exist for confluent relations, is extended as well for strongly coherent computations.
The second part of the thesis applies the decreasing diagrams method and its generalization to concrete systems rewriting terms, in particular to several open problems in this area.

Université Paris-Saclay
Espace Technologique / Immeuble Discovery
Route de l'Orme aux Merisiers RD 128 / 91190 Saint-Aubin, France