Int J Software Informatics, Vol.2, No.1, July 2008, pp. 61–75 E-mail: ijsi@iscas.ac.cn
International Journal of Software and Informatics ISSN 1673-7288 http://www.ijsi.org

Tel: +86-10-62661040

Modular Church-Rosser Modulo: The Complete Picture*

Jean-Pierre Jouannaud[1], Yoshihito Toyama[2]

[1](Projet INRIA TypiCal, École Polytechnique, LIX, 91400 Palaiseau, France,
jouannaud@lix.polytechnique.fr)

[2](Tohoku University, Japan, toyama@nue.riec.tohoku.ac.jp)

Abstract In Ref.[19], Toyama proved that the union of two confluent term-rewriting systems that share absolutely no function symbols or constants is likewise confluent, a property called modularity. The proof of this beautiful modularity result, technically based on slicing terms into an homogeneous cap and a so called alien, possibly heterogeneous substitution, was later substantially simplified in Refs.[8,12]. In this paper, we present a further simplification of the proof of Toyama's result for confluence, which shows that the crux of the problem lies on two different properties: a cleaning lemma, whose goal is to anticipate the application of collapsing reductions and a modularity property of ordered completion that allows to pairwise match the caps and alien substitutions of two equivalent terms obtained from the cleaning lemma. The approach allows for arbitrary kinds of rules, and scales up to rewriting modulo arbitrary sets of equations.

Key words: term rewriting; confluence; modularity; modulo

Jouannaud JP, Toyama Y. Modular church-rosser modulo: The complete picture. *Int J Software Informatics*, **2008, 2(1): 61–75. http://www.ijsi.org/1673-7288/2/61.pdf**

1 Introduction

Let R and S be two rewrite systems over disjoint signatures. Our goal is to prove that confluence is a modular property of their *disjoint union*, that is that $R \cup S$ inherits the confluence properties of R and S, a result known as Toyama's theorem. In the case of rewriting modulo an equational theory also considered in this paper, confluence must be generalized as a Church-Rosser property.

Our main contribution is a new comprehensive proof of Toyama's theorem for (almost) arbitrary plain rewrite systems. It is organized around the notion of *stable equalizers*, which are heterogeneous terms in which collapsing reductions have been anticipated. We call *cleaning* the process of rewriting a term to a stable equalizer. Confluence of the set $R^\infty \cup S^\infty$ obtained from $R \cup S$ by ordered completion implies

* The present paper is an improved version of Ref.[5] in which proofs have been greatly simplified and results made as general as it could possibly be.

Corresponding author: Jean-Pierre Jouannaud, Email: jouannaud@lix.polytechnique.fr
Manuscript received Jul. 19, 2008; revised Jun. 21, 2008; accepted Jun. 23, 2008; published online Aug.25, 2008.

that equivalent stable equalizers have the same structure, made of a homogeneous *cap* which cannot collapse, and a stable equalizer substitution for the aliens. This makes it possible to prove Toyama's theorem by induction on the structure of stable equalizers.

Because ordered completion allows for arbitrary sets of equations, this proof method allows for rewrite systems with *creation rules* whose righthand side contains extra variables, as in $0 \to x \times 0$, or even *expansion rules* whose lefthand side is a variable as in $x \to x + 0$. Toyama's proofs ruled out creation and expansion rules explicitely, but the former restriction was argued to be superfluous in Ref.[10]. Since the absence of expansion rules is only a sufficient condition for modularity, we give a more complete characterization of the cases where modularity is satisfied or not satisfied when one of the two systems contains expansions. Various counter-examples illustrate why and how modularity of confluence may fail in presence of expansion rules.

Our second contribution is a study of modularity of the Church-Rosser property when rewriting with a set of rules R modulo a set of equations E. We prove that all rewrite relations introduced in the litterature, class rewriting, plain rewriting modulo, rewriting modulo, normal rewriting and normalized rewriting enjoy a modular Church-Rosser property by showing a more general generic result which covers all these cases. The proof is obtained by generalizing the cleaning process under the assumption that variables are in normal form for rewriting modulo (or belong to a cycle), therefore generalizing[5].

Recently, yet another, constructive proof of Toyama's theorem was given by van Oostrom[17]. Assuming that both systems R and S are *constructively confluent*, that is, there is a procedure to transform an arbitrary proof into a valley proof, van Oostrom shows that their union is constructively confluent. To be constructive, our proof requires an additionnal assumption, that the equivalence between a term and any one of its variables is decidable.

We introduce the basics of term rewriting systems in Section 2, and our main tool, ordered rewriting and completion, in Section 3. The notions of caps and aliens are recalled in Section 4 before to carry out the new, abstract proof of Toyama's theorem in the general case where extra variables are allowed in righthand sides of rules. Section 5 describes the various ingredients that make the proof concrete. Modularity of rewriting modulo is then adressed in Section 6. Concluding remarks come in Section 7. We assume familiarity with the basic concepts and notations of term rewriting systems and refer to Refs.[2,12] for supplementary definitions and examples.

2 Preliminaries

Given a *signature* $\mathcal{F}$ of *functionsymbols*, and a set $\mathcal{X}$ of *variables*, $T(\mathcal{F}, \mathcal{X})$ denotes the set of *terms* built up from $\mathcal{F}$ and $\mathcal{X}$.

Terms are identified with finite labelled trees as usual. *Positions* are strings of positive integers, identifying the empty string Λ with the root position. We use $\mathcal{P}os(t)$ (resp. $\mathcal{FP}os(t)$) to denote the set of positions (resp. non-variable positions) of t, $t(p)$ for the symbol at position p in t, $t|_p$ for the *subterm* of t at position p, and $t[u]_p$ for the result of replacing $t|_p$ with u at position p in t. We may sometimes omit the position p, writing $t[u]$ for simplicity. We use the notation $u[\;]_p$ for a term with a hole at position $p \in \mathcal{P}os(t)$, called a *context*. $\mathcal{V}ar(t)$ is the set of variables occuring in t. A term is *ground* if $\mathcal{V}ar(t) = \emptyset$.

Substitutions are mappings from variables to terms. The *domain* of a substitution σ is the set $\mathcal{D}om(\sigma) = \{x \in \mathcal{X} \mid \sigma(\S) \neq \S\}$. A substitution of finite domain $\{x_1, \ldots, x_n\}$ is written as in $\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$. A *variable renaming* is a bijective substitution mapping variables onto variables. We use greek letters for substitutions and postfix notation for their application.

Given two terms s, t, computing the substitution σ such that $t = s\sigma$ whenever it exists is called *matching*, and s is then said to be *more general* than t. This quasi-ordering is naturally extended to substitutions. Given two terms s, t their *most general unifier* whenever it exists is the most general substitution σ (unique up to variable renaming) such that $s\sigma = t\sigma$.

An ordering $\succ$ on terms is *monotonic* if $s \succ t$ implies $u[s] \succ u[t]$ for all terms u, and *stable* if $s \succ t$ implies $s\sigma \succ t\sigma$ for all substitutions σ. A *reduction ordering* is a well-founded, monotonic, stable ordering on terms. Lexicographic path orderings[1] are particular reduction orderings $\succ_{\mathcal{F}}$ generated from a precedence $>_{\mathcal{F}}$ on the signature $\mathcal{F}$, which have two important additional properties: *regularity*: if $x \in \mathcal{V}ar(l)$ then $u[l\sigma]_p \succ_{\mathcal{F}} u[x\sigma]_p$ for arbitrary ground substitution σ and ground context $u[\;]_p$; *totality*: if $>_F$ is total on $\mathcal{F}$, then $\succ_{\mathcal{F}}$ is total on $T(\mathcal{F})$. Total reduction orderings are always regular.

A (*plain*) *rewrite rule* is an arbitrary pair of terms, written $l \to r$. Plain rewriting uses plain pattern-matching for firing rules: a term t *rewrites* to a term u at position p with the rule $l \to r \in R$ and the substitution σ, written $t \xrightarrow[l\to r]{p} u$ if $t|_p = l\sigma$ and $u = t[r\sigma]_p$. A (*plain*) *term rewriting system* is a set of rewrite rules $R = \{l_i \to r_i\}_i$. We use $\leftrightarrow_E$ for rewriting with a set E of equations, that is, containing $s \to t$ if it contains $t \to s$.

The inverse of a relation $\to$ is denoted by $\leftarrow$, its reflexive transitive closure, denoted by $\to^*$, is called *derivation*, while its symmetric, reflexive, transitive closure is denoted by $\leftrightarrow^*$, or $\leftrightarrow^*_R$ or $=_R$ when the relation is generated by a rewrite system R. A pair (s, t) of terms is said to be *divergent* if $s \longleftarrow^* u \longrightarrow^* t$ for some term u, *convertible* (or *equivalent*) if $s \leftrightarrow^* t$ and *joinable* if $s \longrightarrow^* v \longleftarrow^* t$ for some v. A relation $\to$ is *confluent* (resp. *Church-Rosser*) if every divergent (resp. convertible) pair of terms (s, t) is joinable. For plain rewriting, the Church-Rosser property coincides with confluence. This is no more true for rewriting modulo equations, which explains why we insist on the Church-Rosser property instead of confluence.

The *equational theory* generated by a set E of equations is the set of *provably equal* pairs s, t, that is such that $s \leftrightarrow^*_E t$. We say that E is *degenerated* if any two terms are provably equal in E. In case the equational theory is given by a confluent rewrite system R, this implies the existence of a derivation $x \longrightarrow^+_R s$ where $x \in \mathcal{X}$ (since two different variables must be joinable). It follows that a confluent rewrite system for which variables are in normal form cannot have a degenerated equational theory.

3 Ordered Rewriting

Ordered rewriting, defined as rewriting with the ordered instances of a given set of equations[3], is the main technical tool used in this paper. Order-rewriting uses a reduction ordering total on ground terms, hence regular.

Given a set of equations E and a well-founded regular ordering $\succ$ total on ground terms, *ordered rewriting* with the pair $(E, \succ)$ is defined as plain rewriting with the infinite system $R = \{l\sigma \to r\sigma \mid l = r \in E, l\sigma \succ r\sigma, \text{ for some ground substitution } \sigma\}$. Regularity of the ordering $\succ$ is used to ensure that no equation $x = s$ with $x \in \mathcal{V}ar(s)$ can be used from left to right.

When R is not confluent, the pair $(E, \succ)$ can be completed into a pair $(E^\infty, \succ)$ such that the associated rewrite system R^∞ is confluent, a process called *ordered completion*: given two equations $g = d \in E$, $l = r \in E$ such that (i) the substitution σ is the most general unifier of the equation $g = l|_p$ and (ii) $g\sigma\gamma \succ d\sigma\gamma$ for some ground context $u[\ ]_p$, then, the so-called *ordered critical pair* $l[d\sigma]_p = r\sigma$ is added to E if it is not trivial. In this process, we assume that neither g nor $l|_p$ are variables. It follows that E^∞ contains an equation $x = y$ between two variables x and y iff the theory E is degenerated.

Given two sets of equations E and S sharing absolutely no function symbol, a key observation is that $(E \cup S)^\infty = E^\infty \cup S^\infty$ for any reduction ordering $\succ$ total on ground terms. Because, if the signatures are disjoint, there are no critical pairs between E and S. Therefore, ordered completion is *modular* for disjoint unions. Note that the result of completion is not changed by adding an arbitrary set of free variables provided the ordering is extended so as to satisfy the required properties for terms in the extended signature, which is possible with the lexicographic path ordering. As a consequence, $(E \cup S)$-equivalent terms become joinable by ordered rewriting with $E^\infty \cup S^\infty$.

4 Modularity of Plain Rewriting

Let R and S be two rewrite systems operating on sets of terms defined over the respective vocabularies $\mathcal{F}_\mathcal{R} \cup \mathcal{X}$ and $\mathcal{F}_\mathcal{S} \cup \mathcal{X}$. We will often write $s \longrightarrow^* t$ for $s \longrightarrow^*_{R \cup S} t$ operating on terms defined over the vocabulary $\mathcal{F}_\mathcal{R} \cup \mathcal{F}_\mathcal{S} \cup \mathcal{X}$.

4.1 Assumptions

Following Toyama[19], our first assumption is that we are given two disjoint vocabularies $\mathcal{F}_R$ and $\mathcal{F}_S$:

$$\mathcal{F}_R \cap \mathcal{F}_S = \emptyset. \tag{1}$$

Assumption (1) is used throughout this paper, but is slightly relaxed in Section 5.5 and in conclusion.

Examples will help us understand our second assumption, which has to do with *expansions*, that is, rules of the form $x \to r$, for which the lefthand side is a variable.

Assume first that the rewrite system R contains an expansion rule $x \to r$ such that $x \notin \mathcal{V}ar(r)$. Then, the equational theory generated by R is degenerated and confluence is trivial, independently of the other rules. Therefore, modularity of the Church-Rosser property becomes a straightforward property in this case.

We now consider expansion rules $x \to r$ such that $x \in \mathcal{V}ar(r)$.

Example 1. Consider the two Church-Rosser rewrite systems $R = \{x \to f(x)\}$ and $S = \{g(a) \to b\}$. Then $b \longleftarrow_S g(a) \longrightarrow_R g(f(a))$. The set of reducts of b is

$\{f^p(b) \mid p \geqslant 0\}$, while the set of reducts of $g(f(a))$ is $\{f^m(g(f^{n+1}(a))) \mid m, n \geqslant 0\}$. Since both sets have no term in common, the union $R \cup S$ is not Church-Rosser.

Consider now the trivially confluent rewrite system $R' = \{x \to f(x), f(x) \to x\}$, defining the same equational theory as R. It is easy to see that the union $R' \cup S$ is confluent. □

The next example shows that we cannot expect to recover the Church-Rosser property by simply adding the inverse rules of the expansion rules as in the example above:

Example 2. Consider $R = \{x \to f(x), f(x) \to h(x)\}$ and $S = \{g(a) \to a\}$, which are both confluent, and let $R' = \{x \to f(x), f(x) \to x, f(x) \to h(x)\}$. R' is confluent, since $f(x) \to x$ is an equational consequence of R, but the union $R' \cup S$ is not confluent, since $g(a) \to a$ and $g(a) \to g(f(a)) \to g(h(a))$. Now, the set of reducts of a is the regular set $(f^*h^*)^*(a)$ while all reducts of $g(h(a))$ contain g. □

Our second assumption is therefore that there are no expansion rules in R or S. An equivalent, robust formulation of this assumption is that

$$\text{Variables are in normal form for } R \cup S. \tag{2}$$

Assumption (2) is used throughout the paper except in Section 5.5, this shall become important in Section 6 when time comes for our generalization to rewriting modulo. Assumption (2) is weakened in Section 5.7.

From assumption (2) and confluence, we can now easily prove that there are no rules $l \to x$ with $x \notin \mathcal{V}ar(l)$. This is so because such a rule would imply the equational consequence $x = y$ for two different variables x, y, in which case the equational theory generated by R must be degenerated. Then, by confluence, one of these variables would be rewritable, contradicting assumption (2). More generally, by the same token, no equation $s = x$ with $x \notin \mathcal{V}ar(s)$ can be generated by ordered completion of R (or of S). Using the remark that $(R \cup S)^\infty = R^\infty \cup S^\infty$ under assumption (1), it follows that no such equation can be generated by ordered completion of $R \cup S$. As a consequence, variables are in normal form for $R^\infty \cup S^\infty$ under our assumptions (1,2), a property which shall be important later on.

While our assumptions rule out the case where a confluent rewrite system defines a degenerated equational theory, modularity holds trivially in this case as we have pointed out already. Therefore. our restrictions do not prevent us to give a *complete* characterization of modular confluence. On the other hand, ruling out rules of the form $x \to s$ with $x \in \mathcal{V}ar(s)$ is not entirely satisfactory. We should seek for a syntactic criterion subdividing this case into two, one for which modularity is preserved and one for which this is not be the case. We will come back to this question in Section 5.7 and give a partial answer there.

4.2 Caps and aliens

We assume without loss of generality a fixed bijective mapping ξ from a denumerable set of variables $\mathcal{Y}$ disjoint from $\mathcal{X}$, to the set of terms $\mathcal{T}(\mathcal{F}_R \cup \mathcal{F}_S, \mathcal{X})$.

We proceed by slicing terms into homogeneous subparts:

Definition 1. *A term in* $\mathcal{T}(\mathcal{F}_R \cup \mathcal{F}_S, \mathcal{X})$ *is* heterogeneous *if it does not belong to the union* $\mathcal{T}(\mathcal{F}_R, \mathcal{X}) \cup \mathcal{T}(\mathcal{F}_S, \mathcal{X})$, *otherwise it is* homogeneous.

A heterogeneous term can be decomposed into a topmost maximal homogeneous part, its *cap*, and a multiset of remaining subterms, its *aliens*. Thanks to assumption (1), there is only one way of slicing a term by separating its homogeneous cap from its aliens rooted by symbols of the other signature.

Definition 2 (Cap and alien positions). *Given a term t, a position*

(i) $q \in \mathcal{P}os(t)$ is a cap position *if and only if $\forall p \leqslant q$, $t(p) \in \mathcal{F}_R \cup \mathcal{X}$ (resp. $\mathcal{F}_S \cup \mathcal{X}$) iff $t(\Lambda) \in \mathcal{F}_R \cup \mathcal{X}$ (resp. $\mathcal{F}_S \cup \mathcal{X}$). In particular, Λ is a cap position;*

(ii) $q \in \mathcal{P}os(t) \setminus \{\Lambda\}$ is an alien position*, and the subterm $t|_q$ is an* alien *if and only if $t(q) \in \mathcal{F}_S$ (resp. $\mathcal{F}_R$) iff $\forall p < q$, $t(p) \in \mathcal{F}_R$ (resp. $\mathcal{F}_S$).*

We use $\mathcal{CP}os(t)$ for the set of cap positions in t, $\mathcal{AP}os(t)$ for its set of alien positions, and $Aliens(t)$ for the multiset of aliens in t.

The rank *of a term t is 1 if t is homogeneous and the maximal rank of its aliens plus 1 otherwise.*

Definition 3 (Cap term and alien substitution). *Given a term t, its* cap $\widehat{t}$ *and* alien substitution γ_t *are defined as follows:*

(i) $\mathcal{P}os(\widehat{t}) = \mathcal{CP}os(t) \cup \mathcal{AP}os(t)$;

(ii) $\forall p \in \mathcal{CP}os(t)$ $\widehat{t}(p) = t(p)$;

(iii) $\forall q \in \mathcal{AP}os(t)$ $\widehat{t}(q) = \xi^{-1}(t|_q) \in \mathcal{Y}$

(iv) γ_t is the restriction of ξ to the variables in $\mathcal{V}ar(\widehat{t}) \cap \mathcal{Y}$.

The following result is straightforward:

Lemma 1. *Given a term t, its cap $\widehat{t}$ and alien substitution γ_t are uniquely defined and satisfy $t = \widehat{t}\gamma_t$. Moreover $\mathcal{AP}os(t) = \emptyset$ and $\widehat{t} = t$ iff t is homogeneous.*

4.3 Modularity proof

Our modularity proof is entirely described below. Its various ingredients are studied in detail in the next section.

Definition 4. *An alien-closed subset Σ of $T(\mathcal{F}_R \cup \mathcal{F}_S, \mathcal{X})$ is said to be*

(i) conservative *iff for every terms $s, t \in T(\mathcal{F}_R, \mathcal{X}) \cap \Sigma$ (resp. $s, t \in T(\mathcal{F}_S, \mathcal{X}) \cap \Sigma$) such that $s \leftrightarrow^*_{R\cup S} t$, then $s \leftrightarrow^*_R t$ (resp. $s \leftrightarrow^*_S t$).*

(ii) reachable *iff for every term $s \in T(\mathcal{F}_R \cup \mathcal{F}_S, \mathcal{X})$, there exists a term $u \in \Sigma$ such that $s \longrightarrow^*_{R\cup S} u$.*

(iii) structural *iff for any two terms $s, t \in \Sigma$ such that $s \leftrightarrow^*_{R\cup S} t$ then $\widehat{s}$ and $\widehat{t}$ belong both to either $T(\mathcal{F}_R, \mathcal{X})$ or to $T(\mathcal{F}_S, \mathcal{X})$, and there exists some variable-renaming $\eta : \mathcal{V}ar(\widehat{s}) \to \mathcal{V}ar(\widehat{t})$ such that $\widehat{s}\eta \leftrightarrow^*_{R\cup S} \widehat{t}$ and $\gamma_s \leftrightarrow^*_{R\cup S} \eta\gamma_t$.*

The property that any two equivalent aliens of s (resp. of s, t) are joinable is an assumption for conservativity, reachability and structurality.

Conservativity, reachability and structurality of Σ together are enough to show Toyama's theorem.

Theorem 1. *Assume that R and S satisfy assumptions (1,2), and that there exists a conservative, reachable and structural set Σ of alien-closed terms. Then the Church-Rosser property of $R \cup S$ is modular.*

Proof: We show the Church-Rosser property for arbitrary terms s, t: $s \leftrightarrow^*_{R\cup S} t$ iff $s \longrightarrow^*_{R\cup S} \longleftarrow^*_{R\cup S} t$. The if direction is straightforward. The proof of the converse proceeds by induction on the maximum of the ranks of s, t. By induction hypothesis, the Church-Rosser property is therefore satisfied for any pair of equivalent aliens of

s, t, allowing us to use the conservativity, reachability and structurality assumptions in this case.

1. By reachability, there exists $u, v \in \Sigma$ such that $s \longrightarrow^*_{R\cup S} u$ and $t \longrightarrow^*_{R\cup S} v$.

2. By structurality, $\widehat{u}$ and $\widehat{v}$ belong to the same signature, $\widehat{u}\eta \leftrightarrow^*_{R\cup S} \widehat{v}$ and $\gamma_u \leftrightarrow^*_{R\cup S} \eta\gamma_v$.

3. By conservativity, $\widehat{u}\eta \leftrightarrow^*_{R} \widehat{v}$ or $\widehat{u}\eta \leftrightarrow^*_{S} \widehat{v}$.

4. By the Church-Rosser assumption for homogeneous terms, $\widehat{u}\eta \longrightarrow^* w \longleftarrow^* \widehat{v}$ for some w.

5. By induction hypothesis, for all $x \in \mathcal{V}ar(\widehat{u})$, there exists a term w_x such that $x\gamma_u \longrightarrow^*_{R\cup S} w_x$ and $x\eta\gamma_v \longrightarrow^*_{R\cup S} w_x$. Let γ be the substitution of domain $\mathcal{V}ar(\widehat{u})$ such that $x\gamma = w_x$. Then $\gamma_u \longrightarrow^*_{R\cup S} \gamma$ and $\eta\gamma_v \longrightarrow^*_{R\cup S} \gamma$.

6. Putting steps together, we get

$$\begin{array}{r}
s \longrightarrow^* u = \widehat{u}\gamma_u = \widehat{u}\eta\eta^{-1}\gamma_u \longrightarrow^* w\eta^{-1}\gamma_u \longrightarrow^* w\eta^{-1}\gamma \\
\| \\
t \longrightarrow^* v = \widehat{v}\gamma_v = \widehat{v}\eta^{-1}\eta\gamma_v \longrightarrow^* \widehat{v}\eta^{-1}\gamma \longrightarrow^* w\eta^{-1}\gamma
\end{array}$$

and we are done. □

Note that the proof is constructive, in the sense that the rewrite proof can be constructed from the initial equivalent terms, provided reachability is constructive. We are left exhibiting a set of terms Σ that satisfies the required properties. This task is carried out in the next section. It first uses both assumptions (1,2) before to relax assumption (2).

5 Stable Equalizers

5.1 The set Σ of stable equalizers

We call *stable equalizers* terms for which the evolution of caps along derivations has been anticipated.

Definition 5. *A non-variable term s is an* equalizer *if it is homogeneous or otherwise if any two equivalent aliens of s are identical equalizers.*

An equalizer s is stable *if it is* alien-stable*, that is, its aliens are themselves stable, and* cap-stable*, that is, $\forall x \in \mathcal{V}ar(\widehat{s})$, $\widehat{s} \not\leftrightarrow^*_{R\cup S} x$.*

A substitution γ is an equalizer *(resp., a* stable equalizer*) if $\forall x \in \mathcal{D}om(\gamma)$, $x\gamma$ is an equalizer (resp., a stable equalizer), and $\forall x, y \in \mathcal{D}om(\gamma)$, $x\gamma \leftrightarrow^*_{R\cup S} y\gamma$ iff $x = y$.*

Let Σ be the set of stable equalizers. This set is clearly *alien-closed*, that is aliens of terms in Σ are in Σ. We are now going to investigate all properties of stable equalizers.

Most properties of stable equalizers become rather easy to prove under Toyama's hypotheses[19], that is, in the absence of rules with extra variables in their righthand side. On the other hand, some of them become wrong in presence of expansion rules, showing that our assumptions are necessary.

5.2 Normal forms for ordered completion

Most coming proofs use ordered completion as introduced in Section 3, for which the only important assumptions are that the signatures are disjoint and the theories are not degenerated, a property implied by assumption (2) and confluence. As already remarked, the result of ordered completion is a set of homogeneous equations $R^\infty \cup S^\infty$ for which ordered rewriting is Church-Rosser. We will further assume an ordering $\succ$ for which variables are minimal, ensuring that variables are in normal-form for ordered rewriting under the assumption that theories are not degenerated. It turns then out that normal forms with respect to $R^\infty \cup S^\infty$ have a key property:

Lemma 2. Let $s \in T(\mathcal{F}_R, \mathcal{X})$. Then, $s \downarrow_{R^\infty \cup S^\infty} \in T(\mathcal{F}_R, \mathcal{X})$. Further, the computation of $s \downarrow_{R^\infty \cup S^\infty}$ involves terms of $T(\mathcal{F}_R, \mathcal{X})$ only.

Proof: We proceed by induction on $\succ$. If s is in normal form, we are done. Otherwise, $s = u[l\theta] \longrightarrow_{l \to r \in R^\infty} u[r\theta]$. There is of course no garantee that the substitution θ is made of terms in $T(\mathcal{F}_R, \mathcal{X})$, and that the obtained reduct $u[r\theta]$ is again homogeneous, since r may contain variables which do not occur in l. We therefore introduce a new substitution θ' satisfying $\theta'(x) = y \in \mathcal{X}$ for all $x \in \mathcal{V}ar(r) \setminus \mathcal{V}ar(l)$ such that $\theta(x) \notin T(\mathcal{F}_R, \mathcal{X})$ and $\theta'(x) = \theta(x)$ otherwise. Clearly, $s = u[l\theta] = u[l\theta'] \longrightarrow_{l \to r \in R^\infty} u[r\theta'] \in T(\mathcal{F}_R, \mathcal{X})$. Besides, $u[r\theta] \leftrightarrow^*_{R \cup S} u[r\theta']$, and therefore both terms have the same normal form with respect to $R^\infty \cup S^\infty$. Further, by properties of the ordering $\succ$, we have $s = u[l\theta] \succ u[r\theta] \succeq u[r\theta']$. We conclude by induction hypothesis applied to $u[r\theta']$. □

5.3 *Conservativity*

Conservativity is of course violated when R or S define a degenerated equational theory, that is, under assumption (1), if they contain rules of the form $x \to s$ or $s \to x$ such that $x \notin \mathcal{V}ar(s)$. As previously, this is our only assumption besides (1), ensuring that we can use Lemma 2.

Lemma 3 (Conservativity). *Let $s, t \in T(\mathcal{F}_R, \mathcal{X})$ such that $s \leftrightarrow^*_{R \cup S} t$. Then, $s \leftrightarrow^*_R t$, with a proof which involves terms in $T(\mathcal{F}_R, \mathcal{X})$ only.*

Proof: Simple consequence of Lemma 2 and confluence of $R^\infty \cup S^\infty$. □

Of course, the same result holds for homogeneous terms in $T(\mathcal{F}_S, \mathcal{X})$.

5.4 *Stability*

The following key technical lemma relies on the absence of expansion rules, that is, on assumption (2).

Lemma 4 (Stability). *Assume s is a stable equalizer such that $\gamma_s \longrightarrow^*_{R \cup S} \gamma$ for some stable equalizer substitution γ. Then $t = \widehat{s}\gamma$ is a stable equalizer such that $\widehat{t} = \widehat{s}\eta$ and $\gamma_t = \eta^{-1}\gamma$ for some variable renaming $\eta : \mathcal{V}ar(\widehat{s}) \cap \mathcal{Y} \to \mathcal{Y}$.*

Note the need for assuming that γ is a stable equalizer substitution.

Proof: By assumption, for each $x \in \mathcal{V}ar(\widehat{s}) \cap \mathcal{Y}$, $x\gamma$ is a stable term. Since there are no expansion rules, a straightforward induction on the rank shows that its cap $\widehat{x\gamma}$ is in the same signature as $\widehat{x\gamma_s}$. For each $x \in \mathcal{V}ar(\widehat{s}) \cap \mathcal{Y}$, let $\eta(x) = \xi^{-1}(x\gamma)$. It is easy to see that η satisfies the claim, implying that t is cap-stable. Since $\eta^{-1}\gamma$ is a stable equalizer substitution by assumption on γ, t is a stable equalizer. □

5.5 *Structurality*

The goal in this section is to show that equivalence proofs between non-homogenous stable equalizers can be decomposed into an homogeneous proof between their caps, and a proof between their aliens. To this end, we use a natural detour via ordered rewriting with $R^\infty \cup S^\infty$. Our assumptions (1,2) shall therefore apply to the infinite rewrite systems R^∞ and S^∞ instead of the rewrite system R and S when using the previous lemmas. Since R^∞ and S^∞ are Church-Rosser and terminating, these assumptions come for free, except for one: ordered completion may generate the equation $x = y$ in case R or S are degenerated. We therefore assume again here as our only additional assumption besides assumption (1), that neither R nor S are degenerated.

Note that our first assumption that vocabularies are disjoint can be easily relaxed in the case where there are shared constructors. Having rules with constructors on top of lefthand sides, however, is not possible in this framework since the modularity property of ordered completion would then be violated.

Lemma 5. *Assume that s is a stable equalizer. Then $\widehat{s\downarrow_{R^\infty\cup S^\infty}} = (\widehat{s}\rho)\downarrow_{R^\infty\cup S^\infty}$ for some variable renaming ρ such that $\mathcal{D}om(\rho^{-1}) = \mathcal{D}om(\gamma_{s\downarrow_{R^\infty\cup S^\infty}}) = Y$, and $\gamma_{s\downarrow_{R^\infty\cup S^\infty}} = (\gamma_s)\downarrow_{R^\infty\cup S^\infty}$ (restricted to the variables in Y).*

Example 3. Let $R = R^\infty = \{f(x) \to a\}, S = S\infty = \{A \to B\}$, and $s = f(A)$ be a stable equalizer with $s\downarrow_{R^\infty\cup S^\infty} = a$. Then $\widehat{s} = f(y)$, $\gamma_s = \{y \mapsto A\}$, $\widehat{s\downarrow_{R^\infty\cup S^\infty}} = a$ and $\gamma_{s\downarrow_{R^\infty\cup S^\infty}} = \emptyset$ (the didentity substitution), which implies that ρ^{-1} and ρ have an empty domain.

Proof: By induction on the rank of s. We normalize s with $R^\infty \cup S^\infty$, normalizing its alien substitution γ_s first, resulting in σ. By induction hypothesis, for each $x \in \mathcal{V}ar(\widehat{s})$, $x\gamma_s$ and $x\sigma$ have their caps in the same signature and therefore $\widehat{x\sigma}$ is not in the same signature as $\widehat{s}$. By Lemma 4 applied to $R^\infty \cup S^\infty$, $s = \widehat{s}\gamma_s \longrightarrow^*_{R^\infty\cup S^\infty} \widehat{s}\rho\sigma$ for some variable renaming ρ. We now normalize $\widehat{s}$, resulting in u, hence $\widehat{s}\rho\sigma \longrightarrow^*_{R^\infty\cup S^\infty} u\rho\sigma$. Since rules in $R^\infty \cup S^\infty$ are homogeneous, $u\rho\sigma$ is in normal form. By Lemma 2, $\widehat{s}$ and u are in the same signature, and since s is stable by assumption, hence cap-stable, u is not a variable, and therefore $u\rho$ and $\widehat{s}$ are in the same signature. It follows that for all $x \in \mathcal{V}ar(\widehat{s})$, $u\rho$ and $\widehat{x\sigma}$ are non-variable terms which are not in the same signature. The result follows. □

Lemma 6 (Structure).

Let $R\cup S$ be a disjoint union, and v and w be equivalent stable equalizers. Assume that terms in the set $Aliens(v)\cup Aliens(w)$ enjoy the Church-Rosser property. Then, $\widehat{v}$ and $\widehat{w}$ belong both to either $T(\mathcal{F}_R, \mathcal{X})$ or $T(\mathcal{F}_S, \mathcal{X})$ and there exists a variable renaming η such that $\mathcal{D}om(\eta) \cap \mathcal{X} = \emptyset$, such that $\widehat{v}\eta \leftrightarrow^*_{R\cup S} \widehat{w}$ and $\gamma_v \leftrightarrow^*_{R\cup S} \eta\gamma_w$.

Proof: By assumption, v and w are equivalent stable equalizers. Since we are interested in equivalence proofs, we use the rewrite system $R^\infty \cup S^\infty$ to establish the equivalences. We therefore normalize both v and w, and by confluence of $R^\infty \cup S^\infty$, $v\downarrow_{R^\infty\cup S^\infty} = w\downarrow_{R^\infty\cup S^\infty}$. By Lemma 5, $\widehat{v\downarrow_{R^\infty\cup S^\infty}} = (\widehat{v}\rho)\downarrow_{R^\infty\cup S^\infty}$ for some variable renaming ρ and $\gamma_{v\downarrow_{R^\infty\cup S^\infty}} = (\gamma_v)\downarrow_{R^\infty\cup S^\infty}$, and $\widehat{w\downarrow_{R^\infty\cup S^\infty}} = (\widehat{w}\theta)\downarrow_{R^\infty\cup S^\infty}$ for some variable renaming θ and $\gamma_{w\downarrow_{R^\infty\cup S^\infty}} = (\gamma_w)\downarrow_{R^\infty\cup S^\infty}$. The result follows by using the variable renaming $\eta = \rho\theta^{-1}$. □

5.6 Reachability

This section is the only one requiring both assumptions (1,2) besides confluence of R and S. The reason is that we do not work with R^∞ and S^∞ here, but directly with R and S.

Lemma 7 (Cleaning). *Let s be a term which set of aliens is Church-Rosser for $R\cup S$. Then, there is a stable equalizer u such that $s \longrightarrow^*_{R\cup S} u$.*

Proof: If s is homogeneous, we are done. Otherwise, let $s = \widehat{s}\gamma_s$.

If γ_s is not stable, then, by assumption, $\gamma_s \longrightarrow^*_{R\cup S} \gamma$, where, for all $x \in \mathcal{V}ar(\widehat{s})$, $x\gamma$ is a stable equalizer. Since $R \cup S$ is assumed Church-Rosser on aliens, we can further assume that γ is a stable equalizer substitution, hence $\widehat{t} = s\gamma$ is an alien-stable equalizer. If t is cap stable, we are done. Otherwise, by Lemma 4, $\widehat{t} = \widehat{s}\eta$ for some variable renaming η, hence, by definition of stability, $\widehat{s}\eta \leftrightarrow^*_{R\cup S} x$ for some variable $x \in \mathcal{V}ar(\widehat{s}\eta)$. By Lemma 3, $\widehat{s}\eta \leftrightarrow^*_R x$ or $\widehat{s}\eta \leftrightarrow^*_S x$. By the Church-Rosser property assumption of both R and S, $\widehat{s}\eta \longrightarrow^*_{R\cup S} u$ and $x \longrightarrow^*_{R\cup S} u$ for some u. By assumption (2), $u = x$. Therefore, $t \longrightarrow^*_{R\cup S} x\gamma$, a stable equalizer and we are done. □

It is easy to see that the only additional property needed for constructivity is the decidability of the property whether a homogeneous term is equivalent to one of its variables: under this assumption, stability becomes decidable and therefore stable equalizers are then constructively reachable.

This concludes our proof of Theorem 1 under the more liberal assumptions of Section 4.1, which we examplify by giving an example of modularity that does not fall under Toyama's assumptions[19]:

Example 4. Let $R = \{x \ \& \ false \rightarrow false, x \ \& \ true \rightarrow true, x \ \& \ y \rightarrow y \ \& \ x, false \rightarrow false \ \& \ x\}$. The Church-Rosser property of this system is left as an exercice. We can now add to R any Church-Rosser system S satisfying our assumptions to obtain a Church-Rosser union. □

5.7 Expansion rules

In this section, we assume as before that the rewrite systems R and S are both confluent and share no function symbol, but try to relax assumption (2) that variables are in normal form (or, equivalently, that there are no expansion rules). We also assume again that R, S do not have a degenerated equational theory, in which case confluence of $R \cup S$ becomes a trivial fact.

The proof of Lemma 7 requires that for any term $s[x]$ such that $s[x] \leftrightarrow^*_R x$, then $s[x] \longrightarrow^*_R x$, the latter following from the fact that $s[x] \longrightarrow^*_R u$ and $x \longrightarrow^*_R u$ for some u by the Church-Rosser assumption, and $u = x$ by assumption (2) that variables are in normal form. We can easily relax this assumption, yielding assumption (2') instead:

$$\forall x \in \mathcal{X} \text{ and } u \in \mathcal{T}(\mathcal{F}, \mathcal{X}) \text{ s.t. } x \xrightarrow[R]{+} u \text{ then } u \xrightarrow[R]{*} x \tag{2'}$$

Then, we would conclude by using assumption (2') applied to u. Note that $x \in \mathcal{V}ar(u)$ because of our assumption that R is not degenerated. Vincent van Oostrom pointed out to us that condition (2') appears in Luth's thesis[11].

Note that weakening assumption (2) into assumption (2') allows to take care of the trick used in Example 1 to force modularity of confluence. Example 2 is taken care of as well, since condition (2') is not satisfied by that example and modularity is not either. However, assumption (2') is not necessary, as shown by the following example:

Example 5. Consider $R = \{x \rightarrow f(x), f(x) \rightarrow h(x)\}$ and $S = \{a \rightarrow b\}$, which are both confluent, and which union is confluent as well, although R violates assumption (2'). This is so because a, b are constants, which forbids creating a counter-example for confluence as in Example 2. □

In order to prevent the counter-example to modularity given in Example 2 while taking care of Example 5, S must satisfy the following additional condition when R contains an expansion rule violating (2'):

$$\forall u[y]_p, v \text{ s.t. } y \text{is a fresh variable}, u[y], v \notin \mathcal{X} \text{ and } u[v] \to w \in S,$$
$$\exists u', v' \text{ s.t. } u \longrightarrow_S^* u',\ v \longrightarrow_S^* v' \text{ and } r \longrightarrow_S^* u'\{y \mapsto v'\} \qquad (2")$$

The idea here is that if a lefthand side of rule is not reduced to a constant, then inserting an R-derivation from x to s at an inner position will be innocuous since we will be able to insert it as well in the derivation originating in the righthand side.

Lemma 8. *$R \uplus S$ is non-modular if R, S are not degenerated, R does not satisfy (2') and S does not satisfy (2"), or vice-versa.*

Proof: Let $u[v] \to w$ a rule in S violating (2"). Then, consider the derivation $u[v] \longrightarrow_R^* t = u[s\{x \mapsto w\}]$ obtained from the derivation $x \longrightarrow_R^* s$ violating (2'). Since $s \not\longrightarrow_R^* x$, the set of $R \cup S$-reducts of t is of the form $t' = u'\{y \mapsto s'\{x \mapsto v'\}\}$, where u' and v' are S-reducts of respectively u and v and s' is a (non-variable) R-reduct of S. We show now by contradiction that t' is not reachable from w in $R \cup S$. Consider a smallest innermost derivation from w to t'. It must be of the form $w \longrightarrow_S^* w[v', \ldots, v']_{p_1,\ldots,p_n} \longrightarrow_S^* w[s'\{x \mapsto v'\}, \ldots, s'\{x \mapsto v'\}]_{p_1,\ldots,p_n} \longrightarrow_R^* u'[s'\{x \mapsto v'\}, \ldots, s'\{x \mapsto v'\}]_{p_1,\ldots,p_n} = t'$. Then, we can construct a derivation from w to $u'\{y \mapsto v'\}$, a contradiction. □

We believe that the converse holds. To show it, the previous proof tells us that it is enough to reduce the non-confluent diagrams to those of the form $u[v] \to w \in S$ and $u[v] \longrightarrow_R^+ u[s\{x \mapsto v\}]$, which are minimal in some sense. Van Oostrom's technique for showing confluence by using decreasing diagrams might help here, but we have not tried to settle the question.

6 Rewriting Modulo Equations

This new proof of Toyama's theorem appears to be quite simple and yet as general as it can be. We shall see that it is the key to our generalization to rewriting modulo.

We assume now given a set R of rewrite rules and a set E of equations used for equational reasoning, both built over the signature $\mathcal{F}_\mathcal{R}$. Orienting the equations of E from left-to-right and right-to-left respectively, we denote by $E^\rightarrow$ and $E^\leftarrow$ the obtained rewrite systems.

Note that $\leftrightarrow_E^* = \longrightarrow_{E^\rightarrow \cup E^\leftarrow}^*$, and that $E^\rightarrow \cup E^\leftarrow$ is trivially confluent.

Similarly, we are also given a set S of rewrite rules and a set D of equations built over the signature $\mathcal{F}_\mathcal{S}$.

6.1 The Zoo of rewrite relations modulo equations

We consider five different rewrite relations in the case of rewriting with the pair (R, E):

1. Class rewriting[9], defined as $u \longrightarrow_{RE} t$ if $\exists s$ such that $u \leftrightarrow_E^* s \longrightarrow_R t$;

2. Plain rewriting modulo[4], defined as plain rewriting $\longrightarrow_R$;

3. Rewriting modulo[18,6], assuming that E-matching is decidable, defined as $u \longrightarrow_{R_E}^p t$ if $u|_p =_E l\sigma$ and $t = u[r\sigma]_p$ for some $l \to r \in R$;

4. Normal rewriting[7], assuming E-matching is decidable and E admits normal forms (a modular property[15]), writing $u{\downarrow_E}$ for the normal form of u, defined as $u \longrightarrow^*_E u{\downarrow_E} \longrightarrow_{R_E} t$;

5. Normalized rewriting[13], for which $E = S \cup AC$ and S is AC-Church-Rosser in the sense of rewriting modulo defined at case 3, defined as $u \longrightarrow^*_{S_{AC}} u{\downarrow_{S_{AC}}} \longrightarrow_{R_{AC}} t$.

Note that all these relations reduce to plain rewriting when E is empty. One step class-rewriting requires searching the equivalence class of u until an equivalent term s is found that contains a redex for plain rewriting. Being the least efficient, class-rewriting has been replaced by the other more effective definitions. Normal rewriting has been introduced for modelling higher-order rewriting (using higher-order pattern matching). But our results *do not* apply directly to the case of higher-order rewriting in the sense of Nipkow[14] and its generalizations[17], since the E-equational part is then shared.

6.2 Modularity of class rewriting

Modularity of class-rewriting reduces easily to modularity of plain rewriting by using the fact that $R \cup E^{\rightarrow} \cup E^{\leftarrow}$ and $S \cup D^{\rightarrow} \cup D^{\leftarrow}$ are confluent rewrite systems over disjoint signatures whenever class-rewriting with (E, R) and (S, D) are confluent. All the rewrite systems involved here, that is, $R, S, E^{\rightarrow} \cup E^{\leftarrow}, D^{\rightarrow} \cup D^{\leftarrow}$ must of course satisfy assumption (2) given in Section 4.1.

Theorem 2. *Under assumption (1) and assumption (2) for all rewrite systems $R, S, E^{\rightarrow} \cup E^{\leftarrow}, D^{\rightarrow} \cup D^{\leftarrow}$, the Church-Rosser property is modular for class rewriting.*

Proof: Class rewriting relates to plain rewriting with $R \cup E^{\rightarrow} \cup E^{\leftarrow}$ as follows: $u \longrightarrow_{RE} w$ iff $u \leftrightarrow^*_E v \longrightarrow_R w$ iff $u \longrightarrow^*_{E^{\rightarrow} \cup E^{\leftarrow}} v \longrightarrow_R w$, and therefore $u \longrightarrow^*_{RE} \leftrightarrow^*_E w$ iff $u \longrightarrow^*_{R \cup E^{\rightarrow} \cup E^{\leftarrow}} w$. As a consequence, class rewriting with (R, E) is Church-Rosser iff plain rewriting with $\longrightarrow^*_{R \cup E^{\rightarrow} \cup E^{\leftarrow}}$ is Church-Rosser. Since the former is modular by Theorem 1, so is the latter. □

This simple proof does not scale up to the other relations for rewriting modulo. On the other hand, it assumes the unecessary restriction that E and R do not contain *collapsing equations* of the form $s \rightarrow x$ with $x \in \mathcal{V}ar(s)$, since orienting a collapsing equation yieds an expansion.

6.3 Modularity of rewriting modulo equations

In order to show modularity of all these relations at once, we adopt an abstract approach using a generic notation $\Longrightarrow_{R,E}$ (resp. $\Longrightarrow_{S,D}$) for rewriting modulo with the pair (R, E) (resp. (S, D)). Assumptions or notations given for (R, E) should be understood as generic, and apply to (S, D) as well. We define the Church-Rosser property as:

$$\forall s,t \text{ s.t. } s \underset{R\cup E}{\overset{*}{\leftrightarrow}} t \quad \exists v,w \text{ s.t. } s \underset{R,E}{\overset{*}{\Longrightarrow}} v, t \underset{R,E}{\overset{*}{\Longrightarrow}} w \text{ and } v \underset{E}{\overset{*}{\leftrightarrow}} w$$

and prove that any rewrite relations $\Longrightarrow_{R,E}$ and $\Longrightarrow_{S,D}$ satisfying

$$\Longrightarrow_{R,E} \subseteq \leftrightarrow^*_E \longrightarrow_R \leftrightarrow^*_E \subseteq \leftrightarrow^*_E \Longrightarrow_{R,E} \leftrightarrow^*_E \qquad (0)$$

$$F_R \cap \mathcal{F}_S = \emptyset \qquad (1)$$

$$\text{Variables are in normal form for } \Longrightarrow_{R,E} \tag{2}$$

enjoy a modular Church-Rosser property.

Again, we rule out here the trivial case where $R \cup E$ defines a degenerated equational theory, which, as before, becomes impossible under the Church-Rosser assumption and assumption (2).

Note that all concrete rewriting modulo relations considered in Section 6.1 satisfy the inclusions (0), including of course class-rewriting, and moreover that any rewriting modulo relation should satisfy these conditions to make sense, since the first inclusion can be seen as a soundeness condition for our encoding and the second as a completeness condition, therefore ensuring together that

$$(\underset{R,E}{\Longrightarrow} \cup \underset{R,E}{\Longleftarrow} \cup \underset{E}{\longleftrightarrow})^* = (\underset{R}{\longrightarrow} \cup \underset{R}{\longleftarrow} \cup \underset{E}{\longleftrightarrow})^*$$

Let us now give a counter-example to modularity when assumption (2) is violated without having an expansion in the set of rules (showing that the chosen formulation of assumption (2) is the right one):

Example 5. Consider $R = \{f(x) \to g(x)\}$ with $E = \{x = f(x)\}$, and $S = \{h(a) \to b\}$ with $D = \emptyset$. R is clearly Church-Rosser modulo E for class rewriting (g symbols can be inserted at any position in any quantitity in a term), while S is Church-Rosser modulo D (class rewriting reducing then to plain rewriting). Consider the diverging computation $h(a) \longrightarrow_{SD} b$ and $h(a) \longrightarrow_{RE} h(g(a))$. Then, the set of reducts of b is $\{g^n(b) \mid n \geqslant 0\}$, the set of reducts of $h(g(a))$ is the regular set $g^n h g^{m+1} a \mid n, m \geqslant 0\}$, and their intersection is empty. □

From now on, we consider two sets of pairs (R, E) and (S, D), and assume that the corresponding generic relations for rewriting modulo, $\Longrightarrow_{R,E}$ and $\Longrightarrow_{S,D}$, are both Church-Rosser. We shall use the abbreviation $\Longrightarrow$ for $\Longrightarrow_{R \cup S, E \cup D}$.

Our proof that the generic relation $\Longrightarrow$ is Church-Rosser for terms in $T(\mathcal{F}_R \cup \mathcal{F}_S, \mathcal{X})$ is essentially based on the same lemmas as before. Those based on the infinite system obtained by completion will be used without change, except that $R^\infty \cup S^\infty$ is replaced by $(R \cup E)^\infty \cup (S \cup D)^\infty$. Therefore, Lemmas 2, 5 and 6 are kept unchanged. We therefore need generalizing Lemmas 3, 4 and 7. Since their proofs can essentially be repeated verbatim, this is indeed a very easy task.

Lemma 9 (Conservativity). *Let $s, t \in T(\mathcal{F}_R, \mathcal{X})$ such that $s \leftrightarrow^*_{R \cup E \cup S \cup D} t$. Then, $s \leftrightarrow^*_{R \cup E} t$ with a proof which involves terms in $T(\mathcal{F}_R, \mathcal{X})$ only.*

The proof can be simply repeated as it is. Defining now stable terms as before, using this time (R, E) instead of simply R, we get:

Lemma 10 (Stability). *Assume s is a stable equalizer such that $\gamma_s \Longrightarrow^*_{R \cup S} \gamma$ for some stable equalizer substitution γ. Then $t = s\gamma$ is a stable equalizer such that $\widehat{t} = \widehat{s}\eta$ and $\gamma_t = \eta^{-1}\gamma$ for some variable renaming $\eta : \mathcal{V}ar(\widehat{s} \cap \mathcal{Y}) \to \mathcal{Y}$.*

We do not repeat the proof which is exactly the same.

Lemma 11 (Cleaning). *Let t be a term such that the set of its non-trivial aliens has the Church-Rosser property for $\Longrightarrow$, and variables are in normal form for $\Longrightarrow$. Then, there exists a stable equalizer e such that $t \Longrightarrow^* e$.*

The proof is the same as before, using rewriting modulo instead of plain rewriting. We are now ready for our main new result:

Theorem 3. *The Church-Rosser property is modular for any rewriting modulo relation satisfying assumptions (0,1,2).*

Proof: The proof mimics the proof of Theorem 1. Let v, w satisfying $v \leftrightarrow^*_{R\cup E\cup S\cup D} w$. The proof is by induction on the maximum rank of v, w. By induction hypothesis, the Church-Rosser property is therefore satisfied for the aliens of v, w.

1. By the reachability Lemma 11, $v \Longrightarrow^* v'$, $w \Longrightarrow^* w'$, v' and w' being stable equalizers for the theory generated by $R \cup E \cup S \cup D$.

2. By assumptions (1,2), $v' \leftrightarrow^*_{R\cup E\cup S\cup D} w'$.

3. By the structure Lemma 6, $\widehat{v'}\eta \leftrightarrow^*_{R\cup E\cup S\cup D} \widehat{w'}$ and $\gamma_{v'} \leftrightarrow^*_{R\cup E\cup S\cup D} \gamma_{w'}\eta$.

4. By conservativity, $\widehat{v'}\eta \leftrightarrow^*_{R\cup E} \widehat{w'}$.

5. By the Church-Rosser assumption for homogeneous terms, $\widehat{v'}\eta \Longrightarrow^* \ s =_{E\cup D} t \Longleftarrow^* \widehat{w'}$. Note that $E \cup D$ applies here to an homogeneous term, that is, we do not know which of E or D is used to relate s and t.

6. By the induction hypothesis applied to $\gamma_{v'}$ and $\gamma_{w'}\eta$ which ranks are strictly smaller than those of v, w, $\gamma_{v'} \Longrightarrow^* \ \sigma =_{E\cup D} \tau \ \Longleftarrow^* \gamma_{w'}\eta$.

7. Putting things together, we get

$$\begin{array}{r}
v \Longrightarrow^* v' = \widehat{v'}\gamma_{v'} = \widehat{v'}\eta\eta^{-1}\gamma_{v'} \Longrightarrow^* s\eta^{-1}\gamma_{v'} \Longrightarrow^* s\eta^{-1}\sigma \\
=_{E\cup D} \\
w \Longrightarrow^* w' = \widehat{w'}\gamma_{w'} = \widehat{w'}\eta^{-1}\eta\gamma_{w'} \Longrightarrow^* \widehat{w'}\eta^{-1}\tau \Longrightarrow^* t\eta^{-1}\tau
\end{array}$$

and we are done. □

As before, it is possible to relax assumption (2) by assumption (2').

7 Conclusions

We have given a comprehensive treatment of Toyama's theorem which should ease its understanding, and which allowed us to carry out two generalisations. The first is the case of rewriting with rules, the righthand sides of which may contain extra-variables. This is not that easy because these extra-variables may be instantiated by arbitrary terms in the union, resulting in rank increasing rewrite steps. The second is the case of rewriting modulo equations for all rewriting relations considered in the litterature (and for those not yet considered as well, if any, since they should satisfy our conditions to make sense).

We have shown that the presence of rewrite rules which lefthand side is a variable occuring in the righthand side may sometimes destroy modularity. This is related to the fact that the proof of the cleaning Lemma 7 fails in presence of such rules. From this observation, we have given a characterization of the cases for which modularity fails which we believe to be complete.

The question arises whether our proof method scales up to the constructor sharing case. This requires generalizing the result of modularity of ordered completion to cope with constructor sharing. This extension is straightforward, as we have seen in Section 5.5 when constructors cannot occur on top of righthand sides of rules, but we have failed to extend it when they do. A rule violating this assumption is called constructor lifting after Ohlebusch[16].

As a consequence, the modularity of the Church-Rosser property of higher-order rewriting cannot be derived from our results, except when the higher-order rewrite rules do not have a binder or an application at the root of their righthand sides. Extending our method to the constructor sharing case with constructor-lifting rules is therefore an important direction for further research.

On the other hand, we think that our proof method should yield a simpler proof of other modularity results, in particular for the existence of a normal form. We have not tried this direction.

Acknowledgements

To Nachum Dershowitz and Maribel Fernandez who shared with the first author an initial unsuccessful quest for simplifying Toyama's modularity proof, and to Vincent van Oostrom for his careful reading and useful discussions on this topic.

References

[1] Dershowitz N. Orderings for term rewriting systems. Theoretical Computer Science, 1982, 17(3): 279–301.

[2] Dershowitz N, Jouannaud JP. Rewrite systems. In: van Leeuwen J, ed. Handbook of Theoretical Computer Science, volume B, North-Holland, 1990: 243–309.

[3] Hsiang J, Rusinowitch M. On word problems in equational theories. In: Proc. 14th Int. Coll. on Automata, Languages and Programming. LNCS 372, 54–71.

[4] Huet G. Confluent reductions: Abstract properties and applications to term rewriting systems. Journal of the ACM, 1980, 27(4): 797–821.

[5] Jouannaud JP. Modular church-rosser modulo. In: Proc. Rewriting Techniques and Applications, Seattle. LNCS 4098, 2006.

[6] Jouannaud JP, Kirchner H. Completion of a set of rules modulo a set of equations. SIAM Journal on Computing, 1986, 15(4): 1155–1194.

[7] Jouannaud JP, van Raamsdonk F. Church-Rosser properties of terminating, higher-order rewriting relations. In: Mathematical Theories of Abstraction, Substitution and Naming in Computer Science. ICMS, Edimburgh, May 2007.

[8] Klop JW, Middeldorp A, Toyama Y, de Vrijer R. Modularity of confluence: A simplified proof. Information Processing Letters, 1994, 49(2): 101–109.

[9] Lankford DS, Ballantyne AM. Decision procedures for simple equational theories with permutative axioms: Complete sets of permutative reductions. Research Report Memo ATP-37, Department of Mathematics and Computer Science, University of Texas, Austin, Texas, USA, August 1977.

[10] Luth C. Compositional term rewriting: An algebraic proof of Toyama's theorm. In: Proc. Rewriting Techniques and Applications, New-Brunswick. LNCS 1103, 1996: 261–275.

[11] Luth C. Categorical term rewriting: Monads and modularity [Ph.D. Thesis]. University of Edinburgh, 1998.

[12] Klop JW, Bezem M, de Vrijer R. Term Rewriting Systems. Number 55 in Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, Cambridge, England, 2003.

[13] Marché C. Normalised rewriting and normalised completion. In: Proc. 9th IEEE Symp. Logic in Computer Science. 1994: 394–403.

[14] Mayr R, Nipkow T. Higher-Order rewrite systems and their confluence. Theoretical Computer Science, 1998, 192(1): 3–29.

[15] Middeldorp A. Modular aspects of properties of term rewriting systems related to normal forms. In: Proc. 3rd Rewriting Techniques and Applications, Chapel Hill. LNCS 355, Springer-Verlag, 1989: 263–277.

[16] Ohlebusch E. On the modularity of confluence of constructor-sharing term rewriting systems. In: Tison S, ed. Proceedings of the Nineteenth International Colloquium on Trees in Algebra and Programming (Edinburgh, UK). LNCS 787, Springer-Verlag, April 1994.

[17] van Oostrom V. Modularity of constructing confluence. 2006. Draft.

[18] Peterson GE, Stickel MK. Complete sets of reductions for some equational theories. Journal of the ACM, 1981, 28(2): 233–264.

[19] Toyama Y. On the Church-Rosser property for the direct sum of term rewriting systems. Journal of the ACM, 1987, 34(1): 128–143.