Modular Church-Rosser Modulo

Jean-Pierre Jouannaud*

École Polytechnique
LIX, UMR CNRS 7161
91400 Palaiseau, France
http://www.lix.polytechnique.fr/Labo/Jean-Pierre.Jouannaud/

Abstract. In [12], 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 [5, 11].
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 in two different properties: a cleaning lemma, whose goal is to anticipate the application of collapsing reductions; a modularity property of ordered completion, that allows to pairwise match the caps and alien substitutions of two equivalent terms.
We then show that Toyama's modularity result scales up to rewriting modulo equations in all considered cases.

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 equationnal theory also considered in this paper, confluence must be generalized as a Church-Rosser property. Toyama apparently anticipated this generalization by using the word Church-Rosser in his title.

A first contribution of this paper is a new comprehensive proof of Toyama's theorem, obtained by reducing modularity of the confluence property to modularity of ordered completion, the latter being a simple property of disjoint unions. It is organized around the notion of *stable equalizers*, which are heterogeneous terms in which collapsing reductions have been anticipated with respect to the rewrite system $R^\infty \cup S^\infty$ obtained by (modular) ordered completion of $R \cup S$. Confluence of $R^\infty \cup S^\infty$ implies that equivalent terms have the same stable equalizers, made of a homogeneous *cap* which cannot collapse, and an alien

* Project LogiCal, Pôle Commun de Recherche en Informatique du Plateau de Saclay, CNRS, École Polytechnique, INRIA, Université Paris-Sud.

stable substitution. This makes it possible to prove Toyama's theorem by induction on the structure of stable equalizers.

A 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-Roser property. We indeed show a more general generic result which covers all these cases. The proof is again obtained by applying selected results of the previous contribution to the rewrite system $R \cup E^{\rightarrow} \cup E^{\leftarrow}$, obtained by orienting the equations in E both ways, which results in a confluent system when the original rewrite relation is conluent.

We introduce terms in Section 2, and recall the basic notions of caps and aliens in Section 3. The new proof of Toyama's theorem is carried out in Section 4. Modularity of rewriting modulo is adressed in Section 5. Concluding remarks come in Section 6. We assume familiarity with the basic concepts and notations of term rewriting systems and refer to [1, 11] for supplementary definitions and examples.

2 Preliminaries

Given a *signature* $\mathcal{F}$ of *function symbols*, 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. $\mathcal{V}ar(t)$ is the set of variables occuring in t.

Substitutions are sets of pairs (x, t) where x is a variable and t is a term. The *domain* of a substitution σ is the set $\mathcal{D}om(\sigma) = \{x \in \mathcal{X} \mid \sigma(x) \neq x\}$. 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 substitution is *ground* if $\sigma(x)$ is a ground term for all $x \in \mathcal{X}$. We use greek letters for substitutions and postfix notation for their application to terms. Composition is denoted by juxtaposition. Bijective substitutions are called *variable renamings*.

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

A *(plain) rewrite rule* is a pair of terms, written $l \rightarrow r$, such that $l \notin \mathcal{X}$ and $\mathcal{V}ar(r) \subseteq \mathcal{V}ar(l)$. Plain rewriting uses plain pattern-matching for firing rules: a term t *rewrites* to a term u at position p with the rule $l \rightarrow r \in R$ and the substitution σ, written $t \longrightarrow^p_{l \rightarrow r} u$ if $t|_p = l\sigma$ and $u = t[r\sigma]_p$. A *(plain) term rewriting system* is a set of rewrite rules $R = \{l_i \rightarrow r_i\}_i$. An *equation* is a rule which can be used both ways. An equation $x = s$ with $x \in \mathcal{X}$ is *collapsing*. We use AC for associativity and commutativity, and $\leftrightarrow_E$ for rewriting with a set E of equations.

The reflexive transitive closure of a relation $\rightarrow$, denoted by $\rightarrow^*$, 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 term rewriting system R is *confluent* (resp. *Church-Rosser*) if $t \rightarrow^* u$ and $t \rightarrow^* v$ (resp. $u \leftrightarrow^* v$) implies $u \rightarrow^* s$ and $v \rightarrow^* s$ for some s. The Church-Rosser property shall sometimes be used for some subset $T \subset \mathcal{T}(\mathcal{F}, \mathcal{X})$, in which case u, v are assumed to belong to T.

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 *rewrite ordering* is a well-founded, monotonic, stable ordering on terms.

Given a set of equations E and a rewrite ordering $\succ$ total on ground terms, *ordered rewriting* with the pair $(E, \succ)$ is defined as plain rewriting with the infinite system $R = \{l\sigma \rightarrow r\sigma \mid l = r \in E, \gamma \text{ ground and } l\gamma \succ r\gamma\}$. 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) $g\sigma\gamma \succ d\sigma\gamma$ and $l\sigma\gamma \succ r\sigma\gamma$ for some ground substitution γ, then, the so-called *ordered critical pair* $l[d\sigma]_p = r\sigma$ is added to E if it is not already confluent.

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 rewrite ordering $\succeq$ 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 remain a total rewrite ordering for terms in the extended signature, which is possible with the recursive path ordering.

3 Caps and Aliens

Following Toyama, our main assumption throughout this paper is that we are given two disjoint vocabularies $\mathcal{F}_R$ and $\mathcal{F}_S$, that is, such that

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

We also 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 the union $\mathcal{T}(\mathcal{F}_R \cup \mathcal{F}_S, \mathcal{X})$ is* heterogeneous if it uses symbols of both $\mathcal{F}_R$ and $\mathcal{F}_S$, 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 our assumption, 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) $q \in \mathcal{D}om(t)$ is a cap position *if and only if $\forall p \leq q\ t(p) \in \mathcal{F}_R \cup \mathcal{X}$ iff $t(\Lambda) \in \mathcal{F}_R \cup \mathcal{X}$. In particular, Λ is a cap position;*

(ii) $q \in \mathcal{D}om(t) \setminus \{\Lambda\}$ 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.
A term is its own (trivial) alien at level 0. (Non-trivial) aliens at level $i > 0$ in t are the aliens of the aliens at level $i-1$. The rank of a term is the maximal level of its aliens.

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) $\forall q \in \mathcal{AP}os(t)\ \widehat{t}(q) = \xi^{-1}(t|_q)$
(iv) γ_t is the restriction of ξ to the variables in $\mathcal{V}ar(\widehat{t}) \cap \mathcal{Y}$.

We will often use ξ instead of γ_t. The following result is straithforward:

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

4 Plain rewriting

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

4.1 Cap reduction, Alien reductions, and Equalizers

The notion of an equalizer is the key original notion of this paper, which allows us to perform reductions in the cap independently of reductions in the aliens (even if the rewrite rules are not left-linear) by anticipating reductions in the aliens.

Definition 4 (Equalizer). *A term t is an* equalizer *if for any two non-trivial aliens u at level i and v at level j in t, $u \leftrightarrow^*_{R\cup S} v$ iff $u = v$.*

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

Example 1. Let $\mathcal{F}_R = \{f, c, +, a, b\}, \mathcal{F}_S = \{g, h\}$, $R = \{+(a, b) \rightarrow +(b, a)\}$ and $S = \{g(x) \rightarrow h(x)\}$. The term $c(f(g(+(b, a))), g(+(b, a)))$ is an $R \cup S$-equalizer, while the term $c(f(g(+(a, b))), h(+(b, a)))$ is not.

Definition 5. *We define a* cap reduction *$s \longrightarrow_C t$ if $s \xrightarrow[R\cup S]{p} t$ with $p \in \mathcal{CP}os(s)$, and an* alien reduction *$s \longrightarrow_A t$ if $s \xrightarrow[R\cup S]{p} t$ with $p \notin \mathcal{CP}os(s)$.*

Alien reductions take place inside an alien term, not necessarily at an alien position.

Lemma 2. *Let $s \longrightarrow_A t$. Then $\widehat{t}(p) = \widehat{s}(p)$ for all $p \in \mathcal{CP}os(s)$ while $Aliens(s)(\longrightarrow)_{mul}Aliens(t)$.*

Proof. Since the reduction takes place in the aliens, $\mathcal{CP}os(s) \subseteq \mathcal{CP}os(t)$ and $\widehat{t}(p) = t(p) = s(p) = \widehat{s}(p)$ for all $p \in \mathcal{CP}os(s)$. □

Note that $\mathcal{D}om(\widehat{t})$ and $\mathcal{D}om(\widehat{s})$ become different in case the rule has collapsed the cap of an alien of s to a subterm in the other signature, hence enlarging the cap of the whole term.

Lemma 3. *Let $s \longrightarrow^p_C t$ with rule $l \rightarrow r \in R$ and substitution σ. Then,*
(i) $\widehat{s} \xrightarrow[l\rightarrow r]{p} \widehat{t} \in T(\mathcal{F}_R, \mathcal{Y}) \setminus \mathcal{Y}$; or
(ii) $\widehat{s} \xrightarrow[l\rightarrow r]{p} y \in \mathcal{Y}$, $r \in \mathcal{V}ar(l)$ and $t = \xi(y)$ is an alien of s.
In both cases t is an equalizer if s is an equalizer.

Note that $\widehat{s}$ and $\widehat{t}$ belong to the same signature and s and t have the same rank in the first case, while they do not in the second case and the rank has decreased strictly from s to t.

Proof. Since $s = \widehat{s}\gamma_s$ by lemma 1, $p \in \mathcal{CP}os(s)$ and rules are homogeneous, $\sigma = \delta\gamma_s$ for some homogeneous substitution δ. Therefore, $s = s[s|_p]_p = \widehat{s}\gamma_s[l\delta\gamma_s]_p = (\widehat{s}[l\delta]_p)\gamma_s$ since $p \in \mathcal{FP}os(\widehat{s})$, and $t = (\widehat{s}[r\delta]_p)\gamma_s$. Assuming that s is an equalizer, then γ_s is an equalizer substitution and t is an equalizer as well.

Case (i) $\widehat{s}[r\delta]_p \notin \mathcal{Y}$, that is, $\widehat{s}[r\delta]_p \in T(\mathcal{F}_R, \mathcal{Y})\backslash\mathcal{Y}$. Then, $\widehat{s} \longrightarrow_{l \to r} \widehat{t} = \widehat{s}[r\delta]_p$ and $t = \widehat{t}\gamma_s$.

Case (ii) $\widehat{s}[r\delta]_p \in \mathcal{Y}$. Necessarily, $r\delta = y \in \mathcal{V}ar(\widehat{s}), r \in \mathcal{V}ar(l)$, and $t = y\gamma_s = y\xi$. □

4.2 Stable Equalizers

Due to the possible action of collapsing reductions, the cap and the aliens may grow or change signature along derivations. In particular, the cap may change signature if the term is equivalent to one of its aliens. Before introducing a stronger notion of equalizer, let us consider an example:

Example 2. Let $R = \{f(x,x) \to x, h(x) \to x\}$ and $S = \{a \to b\}$.
Then, $f(h(a), b) \longrightarrow f(h(b), b) \longrightarrow f(b, b) \longrightarrow b$.

Collapsing the cap here needs rewriting first an alien in order to transform the starting term into an equalizer, before applying the non-linear collapsing rules according to Lemma 3 (ii). Starting from the equalizer directly would not need any alien rewrite step. This suggests a stronger notion of equalizer.

Definition 6 (Stability). *A rewrite step $s \longrightarrow t$ is* cap-stable *if $\widehat{s}$ and $\widehat{t}$ belong to the same signature. A* cap-stable *derivation is a sequence of cap-stable rewrite steps. An equalizer s is* cap-collapsing *if there exists a cap-stable derivation $s \longrightarrow_C^* t$ and an alien u of t such that $t \longrightarrow_C u$.*

An equalizer s is cap-stable *if it is not cap-collapsing,* stable *if it is cap-stable and its aliens are themselves stable, and* alien-stable *if its aliens are stable.*

According to Lemma 2, alien rewrite steps are cap-stable. We proceed with a thorough investigation of the properties of stable equalizers, of which the first is straightforward.

Lemma 4. *Any alien of a stable equalizer is a stable equalizer.*

Lemma 5. *Assume that s is a stable equalizer such that $s \longrightarrow_C t$. Then s and t have their cap in the same signature and t is a stable equalizer.*

Proof. By stability assumption of s, the rewrite step $s \longrightarrow_C t$ must satisfy Lemma 3 case (i). It is therefore a cap-stable step, and $\widehat{s}, \widehat{t}$ are built from the same signature. By Lemma 3 (i) again, every alien u of t is an alien of s, hence is a stable equalizer, and therefore t is an alien-stable equalizer. We are left to show that t is cap-stable.

If it were not, then $t \longrightarrow_C^* u$ for some cap-stable derivation and $u \longrightarrow_C v$ for some alien v of u. The derivation $s \longrightarrow_C t \longrightarrow_C^* u \longrightarrow_C v$ now contradicts the stability assumption of s. □

Lemma 6. *Given an alien-stable equalizer s such that $s \longrightarrow_A^* t$, there exists a substitution θ from $\mathcal{V}ar(\widehat{t}) \cap \mathcal{Y}$ to $\mathcal{V}ar(\widehat{s}) \cap \mathcal{Y}$ such that $\widehat{s} = \widehat{t}\theta$ and $\theta\gamma_s \longrightarrow^* \gamma_t$. Moreover, θ is a bijection if t is an equalizer.*

Proof. By Lemma 2, $\widehat{s}$ and $\widehat{t}$ are in the same signature, and by Lemma 5 t is alien-stable. Hence, $\mathcal{CP}os(s) = \mathcal{CP}os(t)$, and $\forall p \in \mathcal{CP}os(s)\ s(p) = t(p)$, and $\widehat{s}$ and $\widehat{t}$ may only differ by the names of their variables in $\mathcal{Y}$. Let $p, q \in \mathcal{AP}os(t)$ such that $\widehat{t}|_p = \widehat{t}|_q \in \mathcal{Y}$. Then $t|_p = t|_q$, therefore $s|_p \leftrightarrow^* s|_q$ since $s \longrightarrow_A^* t$. Hence $s|_p = s|_q$ since s is an equalizer. Therefore $\widehat{s}|_p = \widehat{s}|_q$, and $\widehat{s} = \widehat{t}\theta$ for some θ from $\mathcal{V}ar(\widehat{t}) \cap \mathcal{Y}$ to $\mathcal{V}ar(\widehat{s}) \cap \mathcal{Y}$. Also $\theta\gamma_s \longrightarrow^* \gamma_t$ since $s \longrightarrow_A^* t$.

If t is an equalizer, then $\widehat{s}|_p = \widehat{s}|_q \in \mathcal{Y}$ implies $t|_p = t|_q$, hence $\widehat{t}|_p = \widehat{t}|_q$, and θ is bijective. □

Lemma 7. *Let s be an alien-stable equalizer such that $s \longrightarrow_A^* u \longrightarrow_C v$. Then there exists a term t such that $s \longrightarrow_C t$.*

Proof. By Lemma 6, $\widehat{u} = \widehat{s}\sigma$ for some substitution σ. By Lemma 3, $\widehat{u}$ is rewritable, and therefore $\widehat{s} \longrightarrow w$ for some w, hence $s \longrightarrow_C w\gamma_s = t$. □

Lemma 8. *Let e be an alien-stable equalizer. Then, e is* cap-collapsing *iff $\widehat{e} \longrightarrow^* y$ for some variable $y \in \mathcal{Y}$.*

Proof. The if part is clear, we show the converse. Assume that $e \longrightarrow_C^* u$ is a cap-stable derivation and that $u \longrightarrow_C v$ for some alien v of u. Since all rewrite steps from e to u are cap-stable cap-rewrite steps, they satisfy Lemma 3(i), and therefore $\widehat{e} \longrightarrow^* \widehat{u}$. Since v is an alien of u, their caps are not in the same signature, hence the rewrite step from u to v is not cap-stable. It therefore satisfies Lemma 3(ii), and $\widehat{u} \longrightarrow_{l \to x} y \in \mathcal{Y}$. It follows that $\widehat{s} \longrightarrow^* y \in \mathcal{Y}$. □

4.3 Structure Lemma

The goal of this section is to show that equivalence proofs between non-homogenous stable terms can be decomposed into a proof between their caps, and a proof between their aliens.

Lemma 9 (Cleaning). *Let t be a term such that the set of all its non-trivial aliens has the Church-Rosser property with respect to $R \cup S$. Then, there exists a stable equalizer e such that $t \longrightarrow^*_{R \cup S} e$.*

Proof. By induction on the rank of $t = \widehat{t}\gamma_t$. By confluence assumption on the aliens, $\gamma_t \longrightarrow^* \gamma'$ such that $\gamma_t(x) \leftrightarrow^*_{R \cup S} \gamma_t(y)$ iff $\gamma'(x) = \gamma'(y)$. Let $\mathcal{D}om(\gamma') = \{x_1, \ldots, x_m\}$ and $y \in \mathcal{D}om(\gamma')$. By induction hypothesis, $y\gamma' \longrightarrow^*_{R \cup S} y\gamma''$, a stable equalizer. Let $s = \widehat{t}\gamma''$, hence $t \longrightarrow^*_A s$. We now compute $\widehat{s}$ and γ_s, show that γ_s is a stable equalizer substitution, and that s rewrites to a stable equalizer e.

From Lemma 2, $\mathcal{P}os(\widehat{t}) \subseteq \mathcal{P}os(\widehat{s})$. Let $y \in \mathcal{V}ar(\widehat{t}) \setminus \mathcal{V}ar(t)$ occurring at position p in $\widehat{t}$ and $\theta(y) = \widehat{s}|_p$. By construction, $\widehat{s} = \widehat{t}\theta$ and $\gamma'' = \theta\gamma_s$. Since γ'' is a stable equalizer substitution, so is γ_s by Lemma 4, hence s is an alien-stable equalizer. If s is not cap-collapsing, it is a stable equalizer and we are done. Otherwise, $\widehat{s} \longrightarrow^* y$ by Lemma 8, hence $s \longrightarrow^* y\gamma_s$, which is a stable equalizer as already shown and we are done again. □

By property of ordered completion, let $R^\infty \cup S^\infty$ be a confluent rewrite system such that $\leftrightarrow^*_{R \cup S} = \leftrightarrow^*_{R^\infty \cup S^\infty}$. By definition, both presentations define the same notions of equalizers.

Lemma 10. *Let u be a stable equalizer with respect to $R \cup S$. Then, it is a stable equalizer with respect to $R^\infty \cup S^\infty$.* □

Proof. Since $R \cup S$ and $R^\infty \cup S^\infty$ define the same equationnal theory, they enjoy the same set of equalizers. We now prove that u is stable with respect to $R^\infty \cup S^\infty$ by induction on the rank. By induction hypothesis, u is alien-stable. We are left to show that it is cap-stable.

Assume it does not hold. By Lemma 8, $\widehat{u} \longrightarrow^*_{R^\infty \cup S^\infty} y$ for some variable $y \in \mathcal{Y}$, and therefore $\widehat{u} \leftrightarrow^*_{R \cup S} y$. Since $\widehat{u}$ is homogeneous, by confluence of $R \cup S$ on homogeneous terms, $\widehat{u} \longrightarrow^*_{R \cup S} y$. Lemma 8 now yields a contradiction. □

The fact that $R^\infty \cup S^\infty$ and $R \cup S$ define the same notions of stable equalizers is crucial in the coming structural property of equalizers.

Lemma 11 (Structure). *Let $R \cup S$ be a disjoint union, and v and w be stable equalizers such that $v \leftrightarrow^*_{R\cup S} w$. Then, there exists a variable renaming η such that (i) $\widehat{v} \leftrightarrow^*_{R\cup S} \widehat{w}\eta$ and (ii) $\gamma_v \leftrightarrow^*_{R\cup S} \eta^{-1}\gamma_w$.*

Proof. By assumption, v and w are stable equalizers with respect to $R \cup S$, hence to $R^\infty \cup S^\infty$ by Lemma 10. Let v' and w' be their respective normal forms with respect to cap-rewrites with $R^\infty \cup S^\infty$. By lemma 5 (applied repeatedly), v' and w' are stable equalizers with respect to $R^\infty \cup S^\infty$.

Therefore, $v' \leftrightarrow^*_{R^\infty \cup S^\infty} w'$, $v' \longrightarrow^*_{R^\infty \cup S^\infty} s$ and $w' \longrightarrow^*_{R^\infty \cup S^\infty} s$ for some s. Now, since v' and w' are in normal form for cap-rewrites, all rewrites from v' to s and w' to s must occur in the aliens by Lemma 7. Since $R^\infty \cup S^\infty$ is confluent, equivalent aliens of s are joinable, and therefore, we can assume without loss of generality than s is an equalizer.

Since v and w are stable, Lemma 3(i) shows that $\widehat{v} \longrightarrow^* \widehat{v'}$ and $\widehat{w} \longrightarrow^* \widehat{w'}$ and therefore $\mathcal{V}ar(\widehat{v'}) \subseteq \mathcal{V}ar(\widehat{v})$ and $\mathcal{V}ar(\widehat{w'}) \subseteq \mathcal{V}ar(\widehat{w})$. Since $v' \longrightarrow^*_A s$ and $w' \longrightarrow^*_A s$, Lemma 6 shows that $\widehat{v'} = \widehat{s}\mu$ and $\widehat{w'} = \widehat{s}\nu$ for some bijection μ from $\mathcal{V}ar(\widehat{s}) \cap \mathcal{Y}$ to $\mathcal{V}ar(\widehat{v'}) \cap \mathcal{Y}$ and ν from $\mathcal{V}ar(\widehat{s}) \cap \mathcal{Y}$ to $\mathcal{V}ar(\widehat{w'}) \cap \mathcal{Y}$. Therefore, $\widehat{v'} = \widehat{w'}\nu^{-1}\mu$, and $\widehat{v} \leftrightarrow^*_{R\cup S} \widehat{w}\eta$ where $\eta = \mu^{-1}\nu$ is a bijection from $\mathcal{V}ar(\widehat{v'}) \cap \mathcal{Y}$ to $\mathcal{V}ar(\widehat{w'}) \cap \mathcal{Y}$.

Using now Lemmas 3(i) and 6 to relate the alien substitutions of u, v, s, we get $\gamma_v = \gamma_{v'}$ and $\mu\gamma_{v'} \longrightarrow^*_{R^\infty \cup S^\infty} \gamma_s$, hence $\mu\gamma_v \leftrightarrow^* \gamma_s$. Similarly $\nu\gamma_w \leftrightarrow^* \gamma_s$, and therefore, $\mu\gamma_v \leftrightarrow^* \nu\gamma_w$ yielding (ii). □

4.4 Modularity

Theorem 1. *The union of two Church-Rosser rewrite systems R, S over disjoint signatures is Church-Rosser.*

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

1. By the cleaning Lemma 9, $v \longrightarrow^*_{R\cup S} v'$, $w \longrightarrow^*_{R\cup S} w'$, v' and w' being stable equalizers.
2. By the structure Lemma 11, $\widehat{v'} \leftrightarrow^*_{R\cup S} \widehat{w'}\eta$ and $\gamma_{v'} \leftrightarrow^*_{R\cup S} \eta^{-1}\gamma_{w'}$.
3. By the Church-Rosser assumption for homogeneous terms, $\widehat{v'} \longrightarrow^* s = t \longleftarrow^* \widehat{w'}\eta$.
4. By the induction hypothesis applied to $\gamma_{v'}$ and $\eta^{-1}\gamma_{w'}$ whose ranks are strictly smaller than those of v, w, $\gamma_{v'} \longrightarrow^* \sigma = \tau \longleftarrow^* \eta^{-1}\gamma_{w'}$.

5. Conclusion:

$$\begin{array}{r} v \longrightarrow^* v' = \widehat{v'}\gamma_{v'} \longrightarrow^* s\gamma_{v'} \longrightarrow^* s\sigma \\ = \\ w \longrightarrow^* w' = \widehat{w'}\gamma_{w'} = \widehat{w'}\eta\eta^{-1}\gamma_{w'} = t\eta^{-1}\gamma_{w'} \longleftarrow^* t\tau \end{array}$$

□

This new proof of Toyama's theorem appears to be much simpler and shorter than previous ones. We will see next that it is the key to our generalization to rewriting modulo.

5 Rewriting modulo equations

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. the notation $E^{\leftarrow}$ implies the assumption that no equation $x = t$ with $x \in \mathcal{X}$ can be in E.

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 $\mathcal{F}_{\mathcal{S}}$.

5.1 The Zoo of rewrite relations modulo equations

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

1. Class rewriting [6], defined as $u \longrightarrow_{RE} t$ if $\exists s$ such that $u \leftrightarrow_E^* s \longrightarrow_R^* t$;
2. Plain rewriting modulo [2], defined as plain rewriting $\longrightarrow_R$;
3. Rewriting modulo [10, 3], 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 $l \rightarrow r \in R$;
4. Normal rewriting [4], assuming E-matching is decidable and E admits normal forms (a modular property [9]), 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 [7], for which $E = S \cup AC$ and S is AC-Church-Rosser in the sense of rewriting modulo defined at case 3, defined as $u \longrightarrow_{S_{AC}}^* u{\downarrow_{S_{AC}}} \longrightarrow_{R_{AC}} t$.

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 [8] and its generalizations [4], since the E-equational part is then shared.

5.2 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.

Theorem 2. *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 Toyama's theorem, so is the latter. □

This proof does not scale up to the other relations for rewriting modulo, unfortunately.

5.3 Modularity of rewriting modulo equations

In order to show the modularity property of all these relations at once, we adopt an abstract approach using a generic notation $\Longrightarrow_{R,E}$ for rewriting modulo with the pair (R, E). More precisely, we prove that any rewrite relation $\Longrightarrow_{R,E}$ satisfying

(i) $\longrightarrow_R \subseteq (\Longrightarrow_{R,E} \leftrightarrow^*_E)^*$
(ii) $\Longrightarrow_{R,E} \subseteq (\leftrightarrow^*_E \longrightarrow_R \leftrightarrow^*_E)^*$
(iii) Variables are in normal form for $\Longrightarrow_{R,E}$
(iv) E does not admit collapsing equations

enjoys a modular Church-Rosser property defined as

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

Note that all concrete rewriting modulo relations considered in Section 5.1 satisfy conditions (i,ii), including of course class-rewriting, and moreover that any rewriting modulo relation should satisfy these conditions to make sense, since (i,ii) imply soundeness

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

For all these relations, one $\Longrightarrow_R$ step suffices in the righthand side of (i), while for (ii), one $\longrightarrow_R$ step suffices in the righthand side with no $\leftrightarrow_E$ step on its right. For rewriting modulo, no $\leftrightarrow_E$ steps are needed in (i). They are needed on the left of $\longrightarrow_R$ in (ii) for modulo, normal and normalized rewriting. Finally, note that (iv) implies (iii) for all our relations, but is a much stronger assumption.

Our coming generalization of Toyama's theorem makes an essential use of the rewrite system $R \cup E^{\rightarrow} \cup E^{\leftarrow}$. We therefore first need to precisely relate the rewrite relation $\Longrightarrow_{R,E}$ to the relation $\longrightarrow_{R \cup E^{\rightarrow} \cup E^{\leftarrow}}$ when the former is Church-Rosser.

Lemma 12. *Assume $\Longrightarrow_{R,E}$ is Church-Rosser. Then, plain rewriting with $R \cup E^{\rightarrow} \cup E^{\leftarrow}$ is Church-Rosser.*

Proof. Straightforward consequence of (ii). □

Form 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 structure Lemma 11 for the rewrite systems $R \cup E^{\rightarrow} \cup E^{\leftarrow}$ and $S \cup D^{\rightarrow} \cup D^{\leftarrow}$. By Lemma 12, both are Church-Rosser under our assumption that $\Longrightarrow_{R,E}$ and $\Longrightarrow_{S,D}$, are Church-Rosser.

To this end, we first need generalizing the cleaning lemma:

Lemma 13 (Cleaning). *Let t be a term such that the set of its non-trivial aliens has the Church-Rosser property for $\Longrightarrow$. Then, there exists a stable equalizer e such that $t \Longrightarrow^* e$.*

The proof uses the cleaning Lemma 9 for the rewrite relation $R \cup E^{\rightarrow} \cup E^{\leftarrow} \cup S \cup D^{\rightarrow} \cup D^{\leftarrow}$, which is Church-Rosser for the aliens of t by lemma 12, in order to dispense us with showing all intermediate properties needed in a direct proof of the lemma. This is possible since a stable equalizer does not depend upon the rewrite relation in use, but upon the equational theory itself.

Proof. The proof is by induction on the rank. By our assumptions, Lemmas 12 and 9 (we actually need a more precise statement extracted from its proof), there exists an alien-stable equalizer $s = \widehat{t}\gamma$ such that $\gamma_t \longrightarrow^*_{R \cup E^{\rightarrow} \cup E^{\leftarrow} \cup S \cup D^{\rightarrow} \cup D^{\leftarrow}} \gamma$ (hence, by induction hypothesis, $\gamma_t \Longrightarrow^* \gamma$), and an equalizer e such that

1. either s is cap-stable, in which case $e = \widehat{s}\gamma$ is stable and $t \Longrightarrow^* e$,
2. or s is cap-collapsing, in which case $\widehat{s} \longrightarrow^*_{R \cup E^{\rightarrow} \cup E^{\leftarrow} \cup S \cup D^{\rightarrow} \cup D^{\leftarrow}} x$ for some variable x and $e = x\gamma$. By the Church-Rosser property of $\Longrightarrow$ for homogeneous terms and assumption (iii), $\widehat{s} \Longrightarrow^* x$, hence $s \Longrightarrow^* e$ again. □

We now obtain our main new result:

Theorem 3. *The Church-Rosser property is modular for any rewriting modulo relation satisfying assumptions (i,ii,iii,iv).*

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 cleaning Lemma 13, $v \Longrightarrow^* v'$, $w \Longrightarrow^* w'$, v' and w' being stable equalizers for the theory generated by $R \cup E \cup S \cup D$.
2. By assumptions (i) and (ii), $v' \leftrightarrow^*_{R \cup E \cup S \cup D} w'$.
3. By the structure Lemma 11, $\widehat{v'} \leftrightarrow^*_{R \cup E \cup S \cup D} \widehat{w'}\eta$ and $\gamma_{v'} \leftrightarrow^*_{R \cup E \cup S \cup D} \eta^{-1}\gamma_{w'}$.
4. By the Church-Rosser assumption for homogeneous terms, $\widehat{v'} \Longrightarrow^* s =_{E \cup D} t \Longleftarrow^* \widehat{w'}\eta$. 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.
5. By the induction hypothesis applied to $\gamma_{v'}$ and $\eta^{-1}\gamma_{w'}$ whose ranks are strictly smaller than those of v, w, $\gamma_{v'} \Longrightarrow^* \sigma =_{E \cup D} \tau \Longleftarrow^* \eta^{-1}\gamma_{w'}$.
6. Conclusion:

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

□

We have not investigated whether this result extends to a theory E that does not satisfy assumption (iv). We suspect it does when assumption (iii) is satisfied, by generalizing the notion of collapsing reduction to $s \longrightarrow_R =_E t$ for some alien t of s, but have not tried.

6 Conclusion

We have given a comprehensive treatment of Toyama's theorem which should ease its understanding. Moreover, we have generalized Toyama's theorem to 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), under the assumption that the equations are non-collapsing.

The question arises whether our proof method scales up to the constructor sharing case. This requires extending the modularity of ordered completion to cope with constructor sharing. We have tried without succes, except for the trivial case where constructors cannot occur on top of righthand sides of rules (a rule violating this assumption is called constructor lifting in the litterature). This implies that 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. This shows that extending our method to the constructor sharing case is 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.

Acknowledgments: The author thanks Nachum Dershowitz and Maribel Fernandez for numerous discussions about modularity and Yoshito Toyama for suggesting the trick of orienting equations both ways instead of repeating the basic proof. An anonymous referee suggested a potential further simplification by stabilizing terms before equalization.

References

1. Nachum Dershowitz and Jean-Pierre Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, pages 243–309. North-Holland, 1990.
2. Gérard Huet. Confluent reductions: abstract properties and applications to term rewriting systems. *Journal of the ACM*, 27(4):797–821, October 1980.
3. Jean-Pierre Jouannaud and Hélène Kirchner. Completion of a set of rules modulo a set of equations. *SIAM Journal on Computing*, 15(4):1155–1194, 1986.
4. Jean-Pierre Jouannaud, Femke van Raasdon, and Albert Rubio. Rewriting with types and arities, 2005. available from the web.
5. Jan Willem Klop, Aart Middeldorp, Yoshihito Toyama, and Roel de Vrijer. Modularity of confluence: A simplified proof. *Information Processing Letters*, 49(2):101–109, 1994.

6. Dallas S. Lankford and A. M. Ballantyne. 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.
7. Claude Marché. Normalised rewriting and normalised completion. In *Proc. 9th IEEE Symp. Logic in Computer Science*, pages 394–403, 1994.
8. Richard Mayr and Tobias Nipkow. Higher-order rewrite systems and their confluence. *Theoretical Computer Science*, 192(1):3–29, February 1998.
9. A. Middeldorp. Modular aspects of properties of term rewriting systems related to normal forms. In *Proc. 3rd Rewriting Techniques and Applications, Chapel Hill, LNCS 355*, pages 263–277. Springer-Verlag, 1989.
10. Gerald E. Peterson and Mark E. Stickel. Complete sets of reductions for some equational theories. *Journal of the ACM*, 28(2):233–264, April 1981.
11. M. Bezem, J.W. Kop and R. de Vrijer eds. *Term Rewriting Systems*. Cambridge Tracts in Theoretical Computer Science 55, Cambridge University Press, 2003.
12. Y. Toyama. On the Church-Rosser property for the direct sum of term rewriting systems. *Journal of the ACM*, 34(1):128–143, April 1987.