Second-order Church-Rosser modulo, without normalization

Thiago Felicissimo

Université Paris-Saclay, INRIA, Deducteam, Laboratoire de Méthodes Formelles, ENS Paris-Saclay
thiago.felicissimo@inria.fr

Abstract

We investigate criteria for proving Church-Rosser modulo of second-order rewrite systems without relying on normalization.

1 Introduction

Rewriting modulo is an alternative to standard rewriting in which one considers not only rewriting rules $l \longmapsto r \in \mathcal{R}$ but also undirected equations $t \approx u \in \mathcal{E}$, allowing to handle theories defined by axioms that cannot be oriented in a well-behaved manner, such as commutativity. In this setting, the Church-Rosser property must be adapted into *Church-Rosser modulo*, stating that $t\ (\longrightarrow \cup \longleftarrow \cup \simeq)^*\ u$ implies $t \stackrel{\sim}{\longrightarrow}^* \circ \simeq \circ\ {}^*\!\stackrel{\sim}{\longleftarrow} u$, where $\simeq$ is the congruence generated by $\mathcal{E}$, $\longrightarrow$ is the rewrite relation generated by $\mathcal{R}$, and $\stackrel{\sim}{\longrightarrow}$ is a relation that can be $\longrightarrow$ [9], or $\simeq \circ \longrightarrow$, or something in between [10] depending on the considered variant of this definition.

Unfortunately, most criteria for Church-Rosser modulo rely on normalization [9, 10, 13, 6], posing a challenge in an ongoing line of study [2] to extend Dedukti [5], a rewriting-based framework for defining type theories, with rewriting modulo. Indeed, confluence proofs for dependent type theories are usually carried out on untyped terms, for which normalization does not hold due to rules such as β-reduction. The situation is made worse by the fact that type theories rely not on first- but second-order rewriting, for which criteria for Church-Rosser modulo are much rarer.

Example 1. Consider the following second-order rewrite system modulo, defining (a fragment of) the conversion of a type theory with an addition satisfying commutativity and assocativity. Function symbols are written in blue, and metavariables in `typewriter font`. We would like to show this example (or a variant of it) to be Church-Rosser modulo.[1]

$$+(\mathtt{t}, 0) \approx \mathtt{t} \qquad +(\mathtt{t}, S(\mathtt{u})) \approx S(+(\mathtt{t}, \mathtt{u})) \qquad +(\mathtt{t}, \mathtt{u}) \approx +(\mathtt{u}, \mathtt{t}) \qquad +(+(\mathtt{t}, \mathtt{u}), \mathtt{v}) \approx +(\mathtt{t}, +(\mathtt{u}, \mathtt{v}))$$

$$@(\lambda(x.\mathtt{t}\{x\}), \mathtt{u}) \longmapsto \mathtt{t}\{\mathtt{u}\} \qquad\qquad \mathbb{N}_{\mathsf{rec}}(0, \mathtt{p0}, xy.\mathtt{pS}\{x, y\}) \longmapsto \mathtt{p0}$$

$$\mathbb{N}_{\mathsf{rec}}(S(\mathtt{n}), \mathtt{p0}, xy.\mathtt{pS}\{x, y\}) \longmapsto \mathtt{pS}\{\mathtt{n}, \mathbb{N}_{\mathsf{rec}}(\mathtt{n}, \mathtt{p0}, xy.\mathtt{pS}\{x, y\})\}$$

In this work, we investigate criteria for proving Church-Rosser modulo of second-order rewrite systems without relying on normalization. We start by proposing a first criterion, which relies on a notion of *unblocked* term. We then discuss a second criterion, which can be shown almost directly from a well-known result. The proofs not given here can be found in a technical report [7].

2 Preliminaries

We work in the setting of (untyped) second-order rewriting.[2] An *arity* is a natural number n and a *binding arity* is a list of natural numbers $(n_1, \dots, n_k)$. Given a set $\mathcal{V}$ of variables $x, y, \dots,$

[1] Among other things, this is needed to establish the *injectivity of* Π*-types*: $\Pi(A_1, x.A_2) \equiv \Pi(A'_1, x.A'_2)$ should imply $A_i \equiv A'_i$. This is then used to establish subject reduction of β-reduction.

[2] This can be seen as Hamana's Second-order Computational Systems [8], or a simply-typed version of Klop's Combinatory Reduction Systems (CRSs) [12] with a single base type, or Nipkow's Pattern Rewrite

a set $\mathcal{M}$ of metavariables $\mathsf{t}, \mathsf{u}, \mathsf{x}, \ldots$ equipped with arities, and a set $\mathcal{F}$ of (function) symbols $f, g, \ldots$ equipped with binding arities, we define the terms by the following grammar, where we write $|\vec{x}|$ for the number k of variables in a list of variables $\vec{x} = x_1 \ldots x_k$. Here, the (simple) arity $\mathsf{arity}(\mathsf{x}) = k$ of x specifies that it takes k arguments, and the binding arity $\mathsf{arity}(f) = (n_1, \ldots, n_k)$ of f specifies that it takes k arguments and binds n_i variables $\vec{x}_i$ in its i-th argument t_i. Given $\mathcal{F}' \subseteq \mathcal{F}$, we write $\mathcal{T}(\mathcal{F}')$ for the set of terms containing only symbols in $\mathcal{F}'$.

$$\begin{array}{llll} t, u, v ::= & \mid x & x \in \mathcal{V} & \\ & \mid \mathsf{x}\{t_1, \ldots, t_k\} & \mathsf{x} \in \mathcal{M} & \text{with } \mathsf{arity}(\mathsf{x}) = k \\ & \mid f(\vec{x}_1.t_1, \ldots, \vec{x}_k.t_k) & f \in \mathcal{F} & \text{with } \mathsf{arity}(f) = (n_1, \ldots, n_k) \text{ and } |\vec{x}_i| = n_i \end{array}$$

We write $\mathsf{fv}(t)$ for the set of free variables of t and $\mathsf{mv}(t)$ for its set of metavariables. We often abbreviate $t_1, \ldots, t_k$ as $\vec{t}$, and $\vec{x}_1.t_1, \ldots, \vec{x}_k.t_k$ as $\mathbf{t}$. A *substitution* σ is a set of pairs either of the form t/x or $\vec{x}.t/\mathsf{x}$ where $\mathsf{arity}(\mathsf{x}) = |\vec{x}|$. We write $t[\sigma]$ for the application of σ to t, the interesting cases being $x[\sigma] = t$ if $t/x \in \sigma$ and $\mathsf{x}\{\vec{t}\}[\sigma] = u[\vec{t}[\sigma]/\vec{x}]$ if $\vec{x}.u/\mathsf{x} \in \sigma$.

A term t is said to be a *$\vec{x}$-pattern* if $\mathsf{fv}(t) \subseteq \vec{x}$ and all metavariables occurrences are of the form $\mathsf{x}\{\vec{x}, \vec{y}\}$ where $\vec{y}$ are the variables bound between the root of the term and this occurrence of x[3]. A *pattern* is then just a ε-pattern, where ε is the empty list.

A *rewrite system* $\mathcal{R}$ is a set of *rewrite rules* $l \longmapsto r$, where l is a pattern headed by a symbol and $\mathsf{mv}(r) \subseteq \mathsf{mv}(l)$ and $\mathsf{fv}(r) = \emptyset$ (we already have $\mathsf{fv}(l) = \emptyset$ from the definition of pattern). An *equational system* $\mathcal{E}$ is a set of *equations* $t \approx u$, where t, u are both patterns.[4] Given a rewrite system $\mathcal{R}$, we write $\longrightarrow$ for the rewrite relation generated by $\mathcal{R}$, and given an equational system $\mathcal{E}$ we write $\simeq$ for the congruence on terms generated by $\mathcal{E}$. We write $\mathcal{F}_{\mathcal{R}} \subseteq \mathcal{F}$ for the symbols appearing in some left-hand side of $\mathcal{R}$, and $\mathcal{F}_{\mathcal{E}} \subseteq \mathcal{F}$ for the symbols appearing in some equation of $\mathcal{E}$.

A *rewrite system modulo* is a pair $(\mathcal{R}, \mathcal{E})$, and we write $\equiv$ for the least equivalence relation containing $\longrightarrow$ and $\simeq$. As previously mentioned, there are many different definitions of Church-Rosser modulo in the literature, so here we will say that $(\mathcal{R}, \mathcal{E})$ is *weak* (resp. *strong*) *Church-Rosser modulo* when $t \equiv u$ implies $t \ (\simeq \circ \longrightarrow)^* \circ \simeq \circ \, ^*(\longleftarrow \circ \simeq) \ u$ (resp. $t \longrightarrow^* \circ \simeq \circ \, ^*\!\longleftarrow u$).

A *context* C is a linear pattern on distinguished metavariables $\Box_1, \Box_2, \ldots$ called *holes*. Given a context C with k holes and $\mathbf{t} = \vec{x}_1.t_1, \ldots, \vec{x}_k.t_k$ with $\mathsf{arity}(\Box_i) = |\vec{x}_i|$ for all i, we write $C[\mathbf{t}]$ for $C[\vec{x}_1.t_1/\Box_1, \ldots, \vec{x}_k.t_k/\Box_k]$.

Finally, we will also consider the definition of *orthogonal rewriting* $\Longrightarrow$ (also known as *developements*, or *simultaneous reduction* [3]), given by the following rules. Here we write $\vec{t_1} \Longrightarrow \vec{t_2}$ when $\vec{t_i} = t_{i,1}, \ldots, t_{i,k}$ and $t_{1,j} \Longrightarrow t_{2,j}$, and $\mathbf{t}_1 \Longrightarrow \mathbf{t}_2$ when $\mathbf{t}_i = \vec{x}_1.t_{i,1}, \ldots, \vec{x}_k.t_{i,k}$ and $t_{1,j} \Longrightarrow t_{2,j}$, and $\sigma_1 \Longrightarrow \sigma_2$ when $\mathsf{dom}(\sigma_1) = \mathsf{dom}(\sigma_2)$ and $t_1 \Longrightarrow t_2$ whenever $t_i/x \in \sigma_i$ or $\vec{x}.t_i/\mathsf{x} \in \sigma_i$.

$$\begin{array}{c} l \longmapsto r \in \mathcal{R} \\ \mathsf{mv}(l) = \mathsf{dom}(\sigma) \end{array} \frac{\sigma \Longrightarrow \sigma'}{l[\sigma] \Longrightarrow r[\sigma']} \qquad \frac{\mathbf{t} \Longrightarrow \mathbf{t}'}{f(\mathbf{t}) \Longrightarrow f(\mathbf{t}')} \qquad \frac{\vec{t} \Longrightarrow \vec{t'}}{\mathsf{x}\{\vec{t}\} \Longrightarrow \mathsf{x}\{\vec{t'}\}} \qquad \frac{}{x \Longrightarrow x}$$

3 The first criterion

In order to explain our criterion and the intuition behind it, it is instructive to start with the following simple criterion for abstract rewriting. Recall that an abstract rewrite system modulo is given by a set $\mathcal{A}$ equipped with a binary relation $\succ$ and an equivalence relation $\sim$.

Systems (PRSs) [13] over a single base type but with only function symbols of order at most two and variables of order at most one. In particular, this allows us to use results developed for any of these formalisms.

[3] Compared with Miller's original definition, we require patterns to be fully applied.

[4] Note that we allow equations such as $+(\mathsf{n}, 0) \approx \mathsf{n}$, in which one of the sides is a metavariable.

Definition 1 (Unblocking subset of $\mathcal{A}$)**.** Given an abstract rewrite system modulo, we say that a subset $\mathcal{U} \subseteq \mathcal{A}$ is *unblocking* for it if:

(A) For all $a \in \mathcal{A}$ there is some $b \in \mathcal{U}$ with $a \sim b$.

(B) For all $a, a' \in \mathcal{A}$ and $b \in \mathcal{U}$ with $b \sim a \succ a'$ we have $b \succ b' \sim a'$ for some $b' \in \mathcal{A}$.

Condition **(B)** intuitively states that in elements $b \in \mathcal{U}$ redexes are maximally unblocked with respect to $\sim$, so that if $b \sim a$, then any redex that is available in a is also available in b. **(A)** then imposes that for every $\sim$ equivalence class one can always find an element in $\mathcal{U}$.

An interesting consequence of having an unblocking subset $\mathcal{U}$ is that we do not need to search the whole $\sim$ equivalence class for redexes, but instead we can just appeal to **(A)** to obtain a term in which all redexes are available. This motivates us to define the relation $\rhd_{\mathcal{U}}$ by $a \rhd_{\mathcal{U}} b$ iff $a \sim c \succ b$ for some $c \in \mathcal{U}$. We then have the following easy result — in the statement, we think of $\succ$ as orthogonal rewriting, which is why supposing the diamond property is reasonable.

Proposition 1. *Suppose that $\succ$ satisfies the diamond property and that we have an unblocking subset $\mathcal{U} \subseteq \mathcal{A}$. Then $a\ (\succ \cup \prec \cup \sim)^*\ b$ implies $a \rhd^*_{\mathcal{U}} \circ \sim \circ\ {}^*_{\mathcal{U}}\!\lhd\ b$.*

The main insight of our criterion is then that, under suitable conditions (satisfied for instance by Example 1), we can find an unblocking subset of terms. The intuition is that the only two ways that a redex can be blocked in Example 1 is if (1) some collapsable term is inserted in the middle of the redex (as in $@(+(\lambda(x.t), 0), u)$, where we have $+(x, 0) \simeq x$), or (2) some symbol in $\mathcal{E}$ matched by a rule left-hand side is not maximally exposed (as in $\mathbb{N}_{\mathsf{rec}}(+(x, \mathrm{S}(y)), p, xy.q)$, where S could be exposed using $+(x, \mathrm{S}(y)) \simeq \mathrm{S}(+(x, y))$). This motivates the following definition:

Definition 2 (Unblocked terms)**.** A context E is an *$\mathcal{E}$-fragment* of t if $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ and $E[\mathbf{u}]$ is a subterm of t for some $\mathbf{u}$. A term t is said to be *unblocked* if, for all $\mathcal{E}$-fragments E of t:

(1) $E \simeq \square_i$ implies $E = \square_i$.

(2) $E \simeq f(\mathbf{t})$ with $f \in \mathcal{F}_{\mathcal{E}} \cap \mathcal{F}_{\mathcal{R}}$ implies $E = f(\mathbf{t}')$ with $\mathbf{t} \simeq \mathbf{t}'$.

Let us now state the assumptions of our criterion:

(i) Equations $t_1 \approx t_2 \in \mathcal{E}$ are linear, and we have $\mathsf{mv}(t_1) = \mathsf{mv}(t_2)$.

(ii) Symbols in $\mathcal{F}_{\mathcal{E}}$ have a binding arity of the form $(0, \dots, 0)$, the list being possibly empty.

(iii) For every context $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$, there is some unblocked $E' \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ with $E \simeq E'$.

(iv) $\mathcal{R}$ is left-linear and no left-hand side is headed by a symbol in $\mathcal{F}_{\mathcal{E}} \cap \mathcal{F}_{\mathcal{R}}$.

(v) Orthogonal rewriting ($\Longrightarrow$) with $\mathcal{R}$ satisfies the diamond property.

The goal of the rest of this section is then to show the following theorem, where we write $\tilde{\longrightarrow}$ for the relation defined by $t \mathrel{\tilde{\longrightarrow}} t'$ iff $t \simeq u \longrightarrow t'$ for some unblocked u.

Theorem 1. *Suppose* **(i)**-**(v)**. *Then $t \equiv u$ implies $t \mathrel{\tilde{\longrightarrow}}^* \circ \simeq \circ\ {}^*\!\tilde{\longleftarrow}\ u$ for all t, u. In particular, $(\mathcal{R}, \mathcal{E})$ is weak Church-Rosser modulo.*

Before showing the proof of Theorem 1, let us see how it can be applied to Example 1. Conditions **(i)**, **(ii)** and **(iv)** can be directly verified, whereas **(v)** follows from the fact that $\mathcal{R}$ is *orthogonal* [14, Theorem 4.8]. To show **(iii)**, let us first note that each context $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ can be put in a normal-form. Indeed, writing $\langle \vec{t} \rangle$ for $+(t_1, \dots +(t_{k-1}, t_k) \dots)$ or 0 when $\vec{t}$ is empty, then for each context $E \in \mathcal{T}(\mathcal{F}_{\mathcal{E}})$ we have $E \simeq \mathrm{S}^k(\langle \square_1, \dots, \square_n \rangle)$ for some unique k when E has n holes. We can easily see that this normal form is unblocked, showing **(iii)**.

Proof of Theorem 1

To prove Theorem 1, we set out to show that unblocked terms satisfy properties **(A)** and **(B)** of Definition 1 for the abstract rewrite system modulo defined by $\Longrightarrow$ and $\simeq$, which will be achieved by Propositions 2 and 3 respectively, and then apply Proposition 1.

A central tool of our proof is the fact that every term t can be decomposed as $t = \overline{E}[\vec{t}]$ where $\overline{E}$ is a context with $\overline{E} \in \mathcal{T}(\mathcal{F}_\mathcal{E})$, and none of the terms in $\vec{t}$ is headed by a symbol in $\mathcal{F}_\mathcal{E}$. We call $\overline{E}[\vec{t}]$ the $\mathcal{E}$-*decomposition* of t, which is unique modulo renaming of $\overline{E}$. A main property of $\mathcal{E}$-decompositions is that $\mathcal{E}$-conversions can be split along them, in the sense of the following lemma. Let us write $t_1 \cong t_2$ when we have $t_i = x$ or $t_i = \mathsf{x}\{\vec{v}_i\}$ and $\vec{v}_1 \simeq \vec{v}_2$ or $t_i = f(\mathbf{v}_i)$ and $\mathbf{v}_1 \simeq \mathbf{v}_2$. Let us then write $\vec{t_1} \cong \vec{t_2}$ for its pointwise extension to the elements of $\vec{t_i}$.

Lemma 1 (Splitting of an $\mathcal{E}$-conversion)**.** *Suppose* **(i)**, **(ii)**, *and $t_1 \simeq t_2$ for some t_1, t_2. Writing $\overline{E}_i[\vec{u}_i]$ for the $\mathcal{E}$-decomposition of t_i, we then must have $\overline{E}_1 \simeq \overline{E}_2$ and $\vec{u}_1 \cong \vec{u}_2$.*

Proof. By induction on $t_1 \simeq t_2$. For the case $t_i = u_i[\sigma]$ with $u_1 \approx u_2 \in \mathcal{E}$ we crucially rely on the fact that equations are linear, which ensures that matching is completely local. □

Lemma 2. *Suppose* **(i)**, **(ii)** *and that we have $t_1 \simeq t_2$ with t_1 an unblocked term and t_2 a term not headed by a symbol in $\mathcal{F}_\mathcal{E}$. Then we have $t_1 \cong t_2$.*

Proof. We consider the $\mathcal{E}$-decompositions $t_i = \overline{E}_i[\vec{u}_i]$ and apply Lemma 1 to get $\overline{E}_1 \simeq \overline{E}_2$ and $\vec{u}_1 \cong \vec{u}_2$. But because t_2 is not of the form $f(\mathbf{t})$ for some $f \in \mathcal{F}_\mathcal{E}$, we must have $\overline{E}_2 = \square$, and because t_1 is unblocked we get $\overline{E}_1 = \square$, so we conclude $\vec{u}_i = t_i$ and thus $t_1 \cong t_2$. □

We can now show that the set of unblocking terms satisfies property **(A)** of Definition 1.

Proposition 2. *Suppose* **(i)**-**(iii)**. *For each t, there is some unblocked term u with $t \simeq u$.*

Proof. By induction on t. Case $t = x$ is trivial. Cases $t = \mathsf{x}\{\vec{t}\}$ and $t = f(\mathbf{t})$ with $f \notin \mathcal{F}_\mathcal{E}$ follow directly by the ih. For t headed by a symbol in $\mathcal{E}$, consider its decomposition $t = \overline{E}[\vec{t}]$. By ih we have $\vec{u}$ unblocked with $\vec{t} \simeq \vec{u}$, so by Lemma 2 we have $\vec{t} \cong \vec{u}$. Finally, by **(iii)** we get $\overline{E}' \in \mathcal{T}(\mathcal{F}_\mathcal{E})$ unblocked with $\overline{E} \simeq \overline{E}'$, and so $\overline{E}'[\vec{u}]$ is unblocked and $\overline{E}'[\vec{u}] \simeq t$. □

To show that the set of unblocking terms satisfies property **(B)** of Definition 1 we now only need the following technical lemma, shown by induction on t_1 and using Lemma 2.

Lemma 3. *Suppose* **(i)**-**(iv)**, *and $t_1[\sigma] \simeq t_2$ with t_2 unblocked and $t_1 \in \mathcal{T}(\mathcal{F}_\mathcal{R})$ a linear $\vec{x}$-pattern and $\mathsf{dom}(\sigma) = \mathsf{mv}(t_1)$. Then we have $t_2 = t_1[\sigma']$ for some $\sigma' \simeq \sigma$.*

In the following, let us write $\rho(t \Longrightarrow u)$ for the number of redexes contracted in $t \Longrightarrow u$ (even if there might be many derivations of $t \Longrightarrow u$, the relevant one can be inferred from the context).

Proposition 3. *Suppose* **(i)**-**(v)**. *If u is unblocked and $u \simeq t \Longrightarrow t'$ then $u \Longrightarrow u' \simeq t'$ and $\rho(t \Longrightarrow t') = \rho(u \Longrightarrow u')$.*

Proof. By induction on $t \Longrightarrow t'$. Almost all cases are either trivial or follow directly by applying Lemma 2 and the ih, and case $l[\sigma] \Longrightarrow r[\sigma']$ also uses Lemma 3. The case $f(\mathbf{t}) \Longrightarrow f(\mathbf{t}')$ is more interesting, and follows using Lemma 2 when $f \notin \mathcal{F}_\mathcal{E}$, or using Lemma 1 when $f \in \mathcal{F}_\mathcal{E}$. □

Corollary 1. *Suppose* **(i)**-**(v)**. *If u is unblocked and $u \simeq t \longrightarrow t'$ then $u \longrightarrow u' \simeq t'$.*

We can now prove Theorem 1. Let us write $t \stackrel{\sim}{\Longrightarrow} u$ when $t \simeq t' \Longrightarrow u$ with some t' unblocked.

Proof of Theorem 1. By Propositions 2 and 3, the set of unblocked terms is unblocking for $\Longrightarrow$ and $\simeq$. So by Proposition 1, and the fact that $\equiv$ equals $(\Longrightarrow \cup \Longleftarrow \cup \simeq)^*$, we get that $\equiv$ is included in $\tilde{\Longrightarrow}^* \circ \simeq \circ {}^*\tilde{\Longleftarrow}$. To conclude it now suffices to replace the $\tilde{\Longrightarrow}$ by $\tilde{\longrightarrow}$. To do this, we first show that $\tilde{\Longrightarrow}$ is included in $\tilde{\longrightarrow}^* \circ \simeq$ using Corollary 1, and then we show that $\tilde{\Longrightarrow}^* \circ \simeq$ is included in $\tilde{\longrightarrow}^* \circ \simeq$ by induction on $\tilde{\Longrightarrow}^*$. □

Before concluding this section, let us mention that Theorem 1 can probably be strengthen. More precisely, we think the requirement that $\mathsf{mv}(t_1) = \mathsf{mv}(t_2)$ in **(i)** can be dropped, and that it might be possible to weaken **(v)** to only require $\mathcal{R}$ to be confluent. Assumption **(ii)** also does not seem to be essential, and was made here to simplify proofs, because all our use cases satisfy it. On the other hand, all linearity assumptions are essential in our proof.

4 The second criterion

We now discuss an alternative and much easier criterion, which follows almost directly from a well-known result. In the following, let us write $\mathsf{CP}^{\pm}(\mathcal{R}_1, \mathcal{R}_2)$ for the set of *critical pairs* between rules of $\mathcal{R}_1$ and $\mathcal{R}_2$ (see for instance [13] for a definition), and $\mathsf{CP}(\mathcal{R})$ for $\mathsf{CP}^{\pm}(\mathcal{R}, \mathcal{R})$. Moreover, given $\mathcal{E}$ for which both sides of all equations are headed by symbols and have the same metavariables[5], let us write $\mathcal{E}^{\pm}$ for the rewrite system $\mathcal{E} \cup \mathcal{E}^{-1}$, and note that we have $\simeq_{\mathcal{E}} = \longrightarrow^*_{\mathcal{E}^{\pm}}$. Then, given a second-order rewrite system modulo $(\mathcal{R} \cup \mathcal{S}, \mathcal{E})$, consider the assumptions:

- **(a)** $\mathcal{R} \cup \mathcal{S}$ is left-linear
- **(b)** For all equations $t \approx u \in \mathcal{E}$, we have t, u linear and headed by symbols, and $\mathsf{mv}(t) = \mathsf{mv}(u)$
- **(c)** $\mathcal{R}$ is confluent
- **(d)** $(\mathcal{S}, \mathcal{E})$ is strong Church-Rosser modulo
- **(e)** $\mathsf{CP}^{\pm}(\mathcal{R}, \mathcal{S}) = \emptyset$ and $\mathsf{CP}^{\pm}(\mathcal{R}, \mathcal{E}^{\pm}) = \emptyset$

Theorem 2. *Suppose* **(a)**-**(e)**. *Then* $(\mathcal{R} \cup \mathcal{S}, \mathcal{E})$ *is strong Church-Rosser modulo.*

So to apply Theorem 2 we still have to prove strong Church-Rosser modulo of a smaller system. The point is that in some cases of interest this smaller system can be strongly-normalizing, enabling the use of criteria that rely on this property. Let us see an example of this.

Example 2. Consider a version of Example 1 in which equations $+(\mathsf{t}, 0) \approx \mathsf{t}$ and $+(\mathsf{t}, \mathrm{S}(\mathsf{u})) \approx \mathrm{S}(+(\mathsf{t}, \mathsf{u}))$ are removed from $\mathcal{E}$, and in which we consider an additional rewrite system $\mathcal{S}$ given by

$$\mathcal{S} := \quad +(\mathsf{t}, 0) \longmapsto \mathsf{t}, \quad +(\mathsf{t}, \mathrm{S}(\mathsf{u})) \longmapsto \mathrm{S}(+(\mathsf{t}, \mathsf{u})), \quad +(0, \mathsf{t}) \longmapsto \mathsf{t}, \quad +(\mathrm{S}(\mathsf{u}), \mathsf{t}) \longmapsto \mathrm{S}(+(\mathsf{t}, \mathsf{u}))$$

Then conditions **(a)**, **(b)** and **(e)** can be directly verified, while **(c)** follows by orthogonality and **(d)** follows by [13, Theorem 5.11][6], using the fact that $\longrightarrow_{\mathcal{S}} \circ \simeq$ is strongly normalizing and that $\mathsf{CP}^{\pm}(\mathcal{E}^{\pm}, \mathcal{S}) \cup \mathsf{CP}(\mathcal{S}) \subseteq \longrightarrow^!_{\mathcal{S}} \circ \simeq_{\mathcal{E}} \circ {}^!_{\mathcal{S}}\longleftarrow$, where $\longrightarrow^!$ denotes reduction to a normal form.

Let us now move to the proof of Theorem 2. As previously mentioned, it can be shown almost directly from a well-known result, more precisely the following:

Theorem 3 (Shown locally in the proof of Theorem 6.8 in [15])**.** *If $\mathcal{R}$ and $\mathcal{S}$ are left-linear Pattern Rewrite Systems (PRSs) with* $\mathsf{CP}^{\pm}(\mathcal{R}, \mathcal{S}) = \emptyset$ *then they commute.*

[5]This extra condition on $\mathcal{E}$ is important for the definition to make sense. For instance, if $\mathcal{E} := \{+(\mathsf{x}, 0) \approx \mathsf{x}\}$, then $\mathcal{E} \cup \mathcal{E}^{-1}$ does *not* define a rewrite system, as left-hand sides of rewrite rules should be headed by symbols.

[6]Actually, [13, Theorem 5.11] is a criterion for *confluence modulo*, but by [3, Exercise 14.3.7] in this case this is equivalent to strong Church-Rosser modulo, given that $\mathcal{S}$ is strongly normalizing.

Proof of Theorem 2. Let us start with the following claim:

Claim 1. *We have* $\simeq_{\mathcal{E}} \circ {}^{*}_{\mathcal{RS}}\!\longleftarrow \circ \longrightarrow^{*}_{\mathcal{S}} \circ \simeq_{\mathcal{E}} \subseteq \longrightarrow^{*}_{\mathcal{S}} \circ \simeq_{\mathcal{E}} \circ {}^{*}_{\mathcal{RS}}\!\longleftarrow$.

Proof of Claim 1. First of all, because $(\mathcal{S}, \mathcal{E})$ is strong Church-Rosser modulo, it is easy to see that it suffices to prove ${}^{*}_{\mathcal{RS}}\!\longleftarrow \circ \longrightarrow^{*}_{\mathcal{S}} \circ \simeq_{\mathcal{E}} \subseteq \longrightarrow^{*}_{\mathcal{S}} \circ \simeq_{\mathcal{E}} \circ {}^{*}_{\mathcal{RS}}\!\longleftarrow$. To do this, we now show that $t \; {}^{n}_{\mathcal{RS}}\!\longleftarrow \circ \longrightarrow^{*}_{\mathcal{S}} \circ \simeq_{\mathcal{E}} u$ implies $t \longrightarrow^{*}_{\mathcal{S}} \circ \simeq_{\mathcal{E}} \circ {}^{*}_{\mathcal{RS}}\!\longleftarrow u$ by induction on n, the base case being trivial. For the induction step, we have $t \; {}_{\mathcal{RS}}\!\longleftarrow t' \; {}^{n}_{\mathcal{RS}}\!\longleftarrow \circ \longrightarrow^{*}_{\mathcal{S}} \circ \simeq_{\mathcal{E}} u$, so by ih we get $t \; {}_{\mathcal{RS}}\!\longleftarrow t' \longrightarrow^{*}_{\mathcal{S}} \circ \simeq_{\mathcal{E}} \circ {}^{*}_{\mathcal{RS}}\!\longleftarrow u$. We now do a case analysis on $t \; {}_{\mathcal{RS}}\!\longleftarrow t'$. For the case $t \; {}_{\mathcal{R}}\!\longleftarrow t'$ this follows because $\mathcal{R}$ commutes with $\mathcal{S}$ and $\mathcal{E}^{\pm}$ (by Theorem 3) and the fact that $\simeq = \longrightarrow^{*}_{\mathcal{E}^{\pm}}$. For the case $t \; {}_{\mathcal{S}}\!\longleftarrow t'$ this follows because $(\mathcal{S}, \mathcal{E})$ is strong Church-Rosser modulo. ☐

We now proceed with the proof of Theorem 2. We have $\equiv$ equal to $(\longrightarrow_{\mathcal{RS}} \cup {}_{\mathcal{RS}}\!\longleftarrow \cup \simeq_{\mathcal{E}})^{*}$, so we prove the theorem by showing that $t \; (\longrightarrow_{\mathcal{RS}} \cup {}_{\mathcal{RS}}\!\longleftarrow \cup \simeq_{\mathcal{E}})^{n} \; u$ implies $t \longrightarrow^{*}_{\mathcal{RS}} \circ \simeq_{\mathcal{E}} \circ {}^{*}_{\mathcal{RS}}\!\longleftarrow u$ by induction on n. The base case is trivial, and for the induction step we have $t \; (\longrightarrow_{\mathcal{RS}} \cup {}_{\mathcal{RS}}\!\longleftarrow \cup \simeq_{\mathcal{E}})^{n} \; u' \; (\longrightarrow_{\mathcal{RS}} \cup {}_{\mathcal{RS}}\!\longleftarrow \cup \simeq_{\mathcal{E}}) \; u$, and by ih we have $t \longrightarrow^{*}_{\mathcal{RS}} \circ \simeq_{\mathcal{E}} \circ {}^{*}_{\mathcal{RS}}\!\longleftarrow u'$. We conclude by a case analysis on $u' \; (\longrightarrow_{\mathcal{RS}} \cup {}_{\mathcal{RS}}\!\longleftarrow \cup \simeq_{\mathcal{E}}) \; u$. Case $u' \; {}_{\mathcal{RS}}\!\longleftarrow u$ is trivial. Cases $u' \longrightarrow_{\mathcal{S}} u$ and $u' \simeq_{\mathcal{E}} u$ follow by Claim 1, and case $u' \longrightarrow_{\mathcal{R}} u$ follows because $\mathcal{R}$ commutes with $\mathcal{S}$ and $\mathcal{E}^{\pm}$ (by Theorem 3) and with itself (by confluence of $\mathcal{R}$). ☐

5 Discussion

In this work, we discussed two criteria for proving Church-Rosser modulo without normalization.

As previously mentioned, Theorem 2 can be shown almost directly from the fact that two left-linear PRSs with no critical pairs between them commute, so it might not be original (maybe it was already clear for others that it could be derived)[7]. However, until finding Theorems 1 and 2, it was unclear for us how to prove Church-Rosser modulo for second-order systems with non-terminating rules, and we think that this problem should be more discussed in the literature. With Theorem 2 in hand, showing this property can be possible by isolating a terminating subsystem $(\mathcal{S}, \mathcal{E})$, proving it strong Church-Rosser modulo with the criteria available in the literature (such as [13, Theorem 5.11]), and trying to verify the other hypotheses of Theorem 2 (as illustrated in Example 2). Because of this, we consider important to document here the existence of Theorem 2 and the strategy of how it can be applied, which will certainly be useful in the future for showing Church-Rosser modulo in an upcoming version of Dedukti with rewriting modulo [2].

A natural question is then how the two criteria compare. First of all, both of them require equations to be linear and rewrite rules to be left-linear, two important limitations, but which seem reasonable: indeed, non-terminating higher-order rules (such as β-reduction) are known to interact badly with non-left-linearity (see Klop's countexample [11])[8]. Then, some of the other hypotheses seem difficult to compare, and indeed each of our examples (Examples 1 and 2) only works with one of the two criteria. However, looking closer at the examples, we remark an interesting point: the unblocked terms in Example 1 turn out to be exactly the normal forms for the system $\mathcal{S}$ in Example 2, so the move from Example 1 to Example 2 replaces the search for an unblocked term by rewriting with $\mathcal{S}$. The latter option seems more desirable, as it yields the strong variant of Church-Rosser modulo, instead of just the weak. It is an open question for us whether there are interesting examples that can be covered by Theorem 1, but which do not admit a variant covered by Theorem 2, or if the second criterion is always more useful in practice.

[7] Let us mention that a similar result is given by Blanqui in [4, Theorem 15], yet it is neither stronger nor weaker than ours (e.g., it only shows confluence modulo, which is weaker than strong Church-Rosser modulo).

[8] An alternative is to consider a setting with *confinement* to avoid interactions between the higher-order rules and the equations, as done in [1]. Unfortunately, this would forbid interesting examples like Examples 1 and 2.

Acknowledgements The author would like to thank Bruno Barras, Théo Winterhalter, Jean-Pierre Jouannaud, Vincent van Oostrom and the anonymous reviewers of IWC 2024.

A Missing definitions

$\boxed{t \longrightarrow u}$

$$\frac{l \longmapsto r \in \mathcal{R} \qquad \mathsf{dom}(\sigma) = \mathsf{mv}(l)}{l[\sigma] \longrightarrow r[\sigma]} \qquad \frac{t_i \longrightarrow t_i' \quad \text{for some } i}{\mathsf{x}\{t_1, \dots, t_i, \dots, t_k\} \longrightarrow \mathsf{x}\{t_1, \dots, t_i', \dots, t_k\}}$$

$$\frac{t_i \longrightarrow t_i' \quad \text{for some } i}{f(\vec{x}_1.t_1, \dots, \vec{x}_i.t_i, \dots, \vec{x}_k.t_k) \longrightarrow f(\vec{x}_1.t_1, \dots, \vec{x}_i.t_i', \dots, \vec{x}_k.t_k)}$$

$\boxed{t \simeq u}$

$$\frac{t \approx u \in \mathcal{E} \qquad \mathsf{dom}(\sigma) = \mathsf{mv}(t) \cup \mathsf{mv}(u)}{t[\sigma] \simeq u[\sigma]} \qquad \frac{t_i \simeq t_i' \quad \text{for all } i}{f(\vec{x}_1.t_1, \dots, \vec{x}_k.t_k) \simeq f(\vec{x}_1.t_1', \dots, \vec{x}_k.t_k')}$$

$$\frac{t_i \simeq t_i' \quad \text{for all } i}{\mathsf{x}\{t_1, \dots, t_k\} \simeq \mathsf{x}\{t_1', \dots, t_k'\}} \qquad \frac{}{x \simeq x} \qquad \frac{t \simeq u}{u \simeq t} \qquad \frac{t \simeq u \qquad u \simeq v}{t \simeq v}$$

Figure 1: Definitions of $\longrightarrow$ and $\simeq$ for some given $\mathcal{R}$ and $\mathcal{E}$

B Complete Proofs

Proposition 1. *Suppose that $\succ$ satisfies the diamond property and that we have an unblocking subset $\mathcal{U} \subseteq \mathcal{A}$. Then $a\ (\succ \cup \prec \cup \sim)^*\ b$ implies $a \rhd_{\mathcal{U}}^* \circ \sim \circ\ {}_{\mathcal{U}}^*\!\lhd b$.*

Proof. First note that we have the following basic facts, that can be easily shown using **(A)** and **(B)**: if $a \sim \circ \rhd_{\mathcal{U}}\ b$ then $a \rhd_{\mathcal{U}}\ b$, and if $a \succ b$ then $a \rhd_{\mathcal{U}} \circ \sim b$. We will also need the following claims.

Claim 2. *If $a\ {}_{\mathcal{U}}\!\lhd \circ \rhd_{\mathcal{U}}\ b$ then $a \rhd_{\mathcal{U}} \circ \sim \circ\ {}_{\mathcal{U}}\!\lhd b$.*

Proof of Claim 2. We have $a \prec a' \sim b' \succ b$ with $a', b' \in \mathcal{U}$. By **(B)** we have $b' \succ b'' \sim a$ for some b'', and by the diamond property we have $b'' \succ \circ \prec b$. We thus have $a \sim b'' \rhd_{\mathcal{U}} \circ \sim \circ\ {}_{\mathcal{U}}\!\lhd b$, and hence $a \rhd_{\mathcal{U}} \circ \sim \circ\ {}_{\mathcal{U}}\!\lhd b$. ☐

Claim 3. *If $a\ {}_{\mathcal{U}}\!\lhd \circ \rhd_{\mathcal{U}}^*\ b$ then $a \rhd_{\mathcal{U}}^* \circ \sim \circ\ {}_{\mathcal{U}}\!\lhd b$.*

Proof of Claim 3. We have $a\ {}_{\mathcal{U}}\!\lhd \circ \rhd_{\mathcal{U}}^n\ b$ for some $n \in \mathbb{N}$, so let us show the result by induction on n, the case $n = 0$ being trivial. For the induction step, we have $a\ {}_{\mathcal{U}}\!\lhd \circ \rhd_{\mathcal{U}} \circ \rhd_{\mathcal{U}}^n\ b$, so by Claim 2 we get $a \rhd_{\mathcal{U}} \circ \sim \circ\ {}_{\mathcal{U}}\!\lhd \circ \rhd_{\mathcal{U}}^n\ b$. By the ih we then get $a \rhd_{\mathcal{U}} \circ \sim \circ \rhd_{\mathcal{U}}^* \circ \sim \circ\ {}_{\mathcal{U}}\!\lhd b$, allowing us to conclude $a \rhd_{\mathcal{U}}^* \circ \sim \circ\ {}_{\mathcal{U}}\!\lhd b$. ☐

Now let us move to the proof of the theorem. We have $a\ (\succ \cup \prec \cup \sim)^n\ b$ for some n, so let us show the result by induction on n, the base case being trivial. For the induction step, we have $a\ (\succ \cup \prec \cup \sim)^n\ c\ (\succ \cup \prec \cup \sim)\ b$, and by i.h. we have $a \rhd^*_{\mathcal{U}} a' \sim c'\ {}^*_{\mathcal{U}}\!\lhd\ c$ for some a', c'. We now proceed by case analysis on $c\ (\succ \cup \prec \cup \sim)\ b$. Cases $c \sim b$ and $c \prec b$ are trivial, and the case $c \succ b$ follows by noting $a \rhd^*_{\mathcal{U}} a' \sim c'\ {}^*_{\mathcal{U}}\!\lhd \circ \rhd_{\mathcal{U}} \circ \sim b$ and then applying Claim 3 to get $a \rhd^*_{\mathcal{U}} a' \sim c' \rhd_{\mathcal{U}} \circ \sim \circ\ {}^*_{\mathcal{U}}\!\lhd \circ \sim b$, which implies the result. $\square$

Lemma 1 (Splitting of an $\mathcal{E}$-conversion)**.** *Suppose* **(i)**, **(ii)**, *and $t_1 \simeq t_2$ for some t_1, t_2. Writing $\overline{E}_i[\vec{u}_i]$ for the $\mathcal{E}$-decomposition of t_i, we then must have $\overline{E}_1 \simeq \overline{E}_2$ and $\vec{u}_1 \cong \vec{u}_2$.*

Proof. By induction on $t_1 \simeq t_2$. The cases when $t_1 \simeq t_2$ follows by an application of reflexivity, symmetry or transitivity are either trivial of follow directly by the ih.

- Case $t_i = e_i[\sigma]$ for some $e_1 \approx e_2 \in \mathcal{E}$. Then because each e_i is fully contained in $\overline{E}_i$, we have $\overline{E}_1 \simeq \overline{E}_2$ and $\vec{u}_1 = \vec{u}_2$. Note that this crucially relies on the fact that equations in $\mathcal{E}$ are linear, so that matching is completely local and does not depend on subterms.
- Case $t_1 = \mathsf{x}\{\vec{v}_1\} \simeq \mathsf{x}\{\vec{v}_2\} = t_2$ with $\vec{v}_1 \simeq \vec{v}_2$. Then we have $\overline{E}_i = \square$, so the result follows.
- Case $t_1 = f(\mathbf{v}_1) \simeq f(\mathbf{v}_2) = t_2$ with $\mathbf{v}_1 \simeq \mathbf{v}_2$. If $f \notin \mathcal{F}_{\mathcal{E}}$ then we have $\overline{E}_i = \square$ so the result follows trivially. For the case $f \in \mathcal{F}_{\mathcal{E}}$, because of **(ii)** we know that f binds no variables, so we have $\mathbf{v}_i = v_i^1, \ldots, v_i^k$. Let us now consider the $\mathcal{E}$-decompositions $v_i^j = \overline{E}_i^j[\vec{u}_{i,j}]$. By applying the ih to each $v_1^j \simeq v_2^j$ we get $\overline{E}_1^j \simeq \overline{E}_2^j$ and $\vec{u}_{1,j} \cong \vec{u}_{2,j}$. Writing $t_i = \overline{E}_i[\vec{u}_i]$ for the decomposition of t_i, we now conclude by noting that we must have $\overline{E}_i = f(\overline{E}_i^1, \ldots, \overline{E}_i^k)$ and $\vec{u}_i = \vec{u}_{i,1}, \ldots, \vec{u}_{1,k}$. $\square$

Lemma 3. *Suppose* **(i)**-**(iv)**, *and $t_1[\sigma] \simeq t_2$ with t_2 unblocked and $t_1 \in \mathcal{T}(\mathcal{F}_{\mathcal{R}})$ a linear $\vec{x}$-pattern and $\mathsf{dom}(\sigma) = \mathsf{mv}(t_1)$. Then we have $t_2 = t_1[\sigma']$ for some $\sigma' \simeq \sigma$.*

Proof. By induction on t_1.

- Case $t_1 = x$. We have $\sigma = \emptyset$ and by Lemma 2 we get $t_2 = x$, so we can take $\sigma' = \emptyset$.
- Case $t_1 = \mathsf{x}\{\vec{x}\}$. Then we have $\sigma = \vec{x}.u/\mathsf{x}$ for some u. Defining $\sigma' := \vec{x}.t_2/\mathsf{x}$ we then get $t_1[\sigma'] = t_2$ and $\sigma \simeq \sigma'$.
- Case $t_1 = f(\mathbf{v}_1)$. First note that we must have $t_2 = f(\mathbf{v}_2)$ for some $\mathbf{v}_2 \simeq \mathbf{v}_1[\sigma]$. Indeed, we have either $f \notin \mathcal{F}_{\mathcal{E}}$, in which case this claim follows by Lemma 2, or $f \in \mathcal{F}_{\mathcal{E}}$, in which case the claim directly follows from the fact that t_2 is unblocked. Now write $\mathbf{v}_i = \vec{x}_1.v_{i,1}, \ldots, \vec{x}_k.v_{i,k}$, and note that because t_1 is linear we must have $\mathsf{mv}(v_{1,j}) \cap \mathsf{mv}(v_{1,j'}) = \emptyset$ for $j \neq j'$. Let us then consider the decomposition $\sigma = \sigma_1 \cup \cdots \cup \sigma_k$ given by the decomposition $\mathsf{mv}(t_1) = \mathsf{mv}(v_{1,1}) \cup \cdots \cup \mathsf{mv}(v_{1,k})$. By applying the ih to each $v_{1,j}[\sigma_j] \simeq v_{2,j}$ we get some σ'_j satisfying $\sigma_j \simeq \sigma'_j$ and $v_{2,j} = v_{1,j}[\sigma'_j]$. Defining $\sigma' := \sigma'_1 \cup \cdots \cup \sigma'_k$, we conclude $t_2 = t_1[\sigma']$ and $\sigma \simeq \sigma'$. $\square$

Proposition 3. *Suppose* **(i)**-**(v)**. *If u is unblocked and $u \simeq t \Longrightarrow t'$ then $u \Longrightarrow u' \simeq t'$ and $\rho(t \Longrightarrow t') = \rho(u \Longrightarrow u')$.*

Proof. By induction on $t \Longrightarrow t'$. All cases are either trivial or follow directly by applying Lemma 2 and then the ih, except for the following two:

- Case $t = l[\sigma]$ and $t' = r[\sigma']$ with $\sigma \Longrightarrow \sigma'$. By Lemma 3 we have $u = l[\theta]$ with $\theta \simeq \sigma$. By the ih we have $\theta \Longrightarrow \theta' \simeq \sigma'$ and $\rho(\sigma \Longrightarrow \sigma') = \rho(\theta \Longrightarrow \theta')$. Hence we get $u = l[\theta] \Longrightarrow r[\theta'] \simeq r[\sigma'] = t'$ and $\rho(l[\sigma] \Longrightarrow r[\sigma']) = 1 + \rho(\sigma \Longrightarrow \sigma') = 1 + \rho(\theta \Longrightarrow \theta') = \rho(l[\theta'] \Longrightarrow r[\theta'])$.

- Case $t = f(\mathbf{t}) \Longrightarrow f(\mathbf{t}') = t'$. If $f \notin \mathcal{F}_{\mathcal{E}}$ then the result follows directly by applying Lemma 2 and then the ih. So let us now suppose $f \in \mathcal{F}_{\mathcal{E}}$, and consider the decompositions $t = \overline{E}_t[\vec{t}]$ and $u = \overline{E}_u[\vec{u}]$. By Lemma 1 we have $\overline{E}_t \simeq \overline{E}_u$ and $\vec{t} \simeq \vec{u}$. Now note that, because no symbol in $\mathcal{E}$ appears in the head of a rewrite rule, then $\overline{E}_t[\vec{t}] \Longrightarrow t'$ implies $t' = \overline{E}_t[\vec{t'}]$ with $\vec{t} \Longrightarrow \vec{t'}$. Moreover, because t is headed by a symbol in $\mathcal{E}$, it follows that the proof of $\vec{t} \Longrightarrow \vec{t'}$ is smaller than the one of $t \Longrightarrow t'$ we started with. Therefore, by the ih we get $\vec{u} \Longrightarrow \vec{u'} \simeq \vec{t'}$ and $\rho(\vec{t} \Longrightarrow \vec{t'}) = \rho(\vec{u} \Longrightarrow \vec{u'})$. We conclude $u = \overline{E}_u[\vec{u}] \Longrightarrow \overline{E}_u[\vec{u}'] \simeq \overline{E}_t[\vec{t'}] = t'$ and $\rho(t \Longrightarrow t') = \rho(\vec{t} \Longrightarrow \vec{t'}) = \rho(\vec{u} \Longrightarrow \vec{u}') = \rho(u \Longrightarrow u')$. $\square$

Corollary 1. *Suppose* (i)-(v)*. If u is unblocked and $u \simeq t \longrightarrow t'$ then $u \longrightarrow u' \simeq t'$.*

Proof. We have $u \simeq t \Longrightarrow t'$, so Proposition 3 gives $u \Longrightarrow u' \simeq t'$ for some u'. But because $\rho(u \Longrightarrow u') = \rho(t \Longrightarrow t') = 1$, then we have $u \longrightarrow u'$. $\square$

Theorem 1. *Suppose* (i)-(v)*. Then $t \equiv u$ implies $t \overset{\sim}{\longrightarrow}{}^* \circ \simeq \circ {}^*\overset{\sim}{\longleftarrow} u$ for all t, u. In particular, $(\mathcal{R}, \mathcal{E})$ is weak Church-Rosser modulo.*

Proof. By Propositions 2 and 3, the set of unblocked terms is unblocking for $\Longrightarrow$ and $\simeq$. So by Proposition 1, and the fact that $\equiv$ equals $(\Longrightarrow \cup \Longleftarrow \cup \simeq)^*$, we get that $\equiv$ is included in $\overset{\sim}{\Longrightarrow}{}^* \circ \simeq \circ {}^*\overset{\sim}{\Longleftarrow}$. To conclude it now suffices to replace the $\overset{\sim}{\Longrightarrow}$ by $\overset{\sim}{\longrightarrow}$. To do this, we will need the following claims.

Claim 4. *If $t \overset{\sim}{\Longrightarrow} u$ then $t \overset{\sim}{\longrightarrow}{}^* \circ \simeq u$.*

Proof. Because $\Longrightarrow \subseteq \longrightarrow^*$, we have $t \simeq \circ \longrightarrow^n u$ for some $n \in \mathbb{N}$, so let us show the result by induction on n, the base case being trivial. For the induction step, we write $t \simeq \circ \longrightarrow^n u' \longrightarrow u$, and by ih we have $t \overset{\sim}{\longrightarrow}{}^* t' \simeq u' \longrightarrow u$ for some t'. By Proposition 2 we have some t'' unblocked with $t'' \simeq u'$, so by Corollary 1 we get $t'' \longrightarrow \circ \simeq u$. We thus have $t' \overset{\sim}{\longrightarrow} \circ \simeq u$, so we conclude $t \overset{\sim}{\longrightarrow}{}^* \circ \simeq u$. $\square$

Claim 5. *If $t \overset{\sim}{\Longrightarrow}{}^* \circ \simeq u$ then $t \overset{\sim}{\longrightarrow}{}^* \circ \simeq u$.*

Proof. We have $t \overset{\sim}{\Longrightarrow}{}^n \circ \simeq u$ for some n, so we show the result by induction on n, the base case being trivial. For the induction step, we write $t \overset{\sim}{\Longrightarrow} \circ \overset{\sim}{\Longrightarrow}{}^n \circ \simeq u$, and by ih we have $t \overset{\sim}{\Longrightarrow} \circ \overset{\sim}{\longrightarrow}{}^* \circ \simeq u$. By Claim 4 we then get $t \overset{\sim}{\longrightarrow}{}^* \circ \simeq \circ \overset{\sim}{\longrightarrow}{}^* \circ \simeq u$ and thus $t \overset{\sim}{\longrightarrow}{}^* \circ \simeq u$ $\square$

By applying Claim 5 two times, we then obtain that $\overset{\sim}{\Longrightarrow}{}^* \circ \simeq \circ {}^*\overset{\sim}{\Longleftarrow}$ is included in $\overset{\sim}{\longrightarrow}{}^* \circ \simeq \circ {}^*\overset{\sim}{\longleftarrow}$, concluding the proof. $\square$

References

[1] Ali Assaf, Gilles Dowek, Jean-Pierre Jouannaud, and Jiaxiang Liu. Untyped Confluence In Dependent Type Theories. working paper or preprint, April 2017.

[2] Bruno Barras, Thiago Felicissimo, and Theo Winterhalter. Towards a logical framework modulo rewriting and equational theories. In *30th International Conference on Types for Proofs and Programs (TYPES 2024)*. https://types2024.itu.dk/abstracts.pdf#section.0.40.

[3] Marc Bezem, Jan Willem Klop, and Roel de Vrijer. *Term rewriting systems*. 2003.

[4] Frédéric Blanqui. Rewriting modulo in deduction modulo. In Robert Nieuwenhuis, editor, *Rewriting Techniques and Applications*, pages 395–409, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[5] Frédéric Blanqui, Gilles Dowek, Emilie Grienenberger, Gabriel Hondet, and François Thiré. A modular construction of type theories. *Logical Methods in Computer Science*, 2023.

[6] Alexandre Boudet and Evelyne Contejean. About the confluence of equational pattern rewrite systems. In Claude Kirchner and Hélène Kirchner, editors, *Automated Deduction — CADE-15*, pages 88–102, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg.

[7] Thiago Felicissimo. Second-order church-rosser modulo, without normalization. Technical report, 2024. Can be found at http://www.lsv.fr/~felicissimo/.

[8] Makoto Hamana. Complete algebraic semantics for second-order rewriting systems based on abstract syntax with variable binding. *Mathematical Structures in Computer Science*, 32(4):542–573, 2022.

[9] Gérard Huet. Confluent reductions: Abstract properties and applications to term rewriting systems: Abstract properties and applications to term rewriting systems. *Journal of the ACM (JACM)*, 1980.

[10] Jean-Pierre Jouannaud and Hélene Kirchner. Completion of a set of rules modulo a set of equations. In *11th ACM SIGACT-SIGPLAN symposium on Principles of programming languages*, 1984.

[11] Jan Willem Klop. *Combinatory reduction systems*. PhD thesis, Rijksuniversiteit Utrecht, 1963.

[12] Jan Willem Klop, Vincent Van Oostrom, and Femke Van Raamsdonk. Combinatory reduction systems: introduction and survey. *Theoretical computer science*, 121(1-2):279–308, 1993.

[13] Richard Mayr and Tobias Nipkow. Higher-order rewrite systems and their confluence. *Theoretical computer science*, 192(1):3–29, 1998.

[14] Tobias Nipkow. Orthogonal higher-order rewrite systems are confluent. In *International Conference on Typed Lambda Calculi and Applications*, pages 306–317. Springer, 1993.

[15] Vincent van Oostrom and Femke van Raamsdonk. Weak orthogonality implies confluence: The higher-order case. Technical report, 1994. http://www.javakade.nl/research/ps/ISRL-94-5.ps.