Order-Sorted Equality Enrichments Modulo Axioms

Raúl Gutiérrez, José Meseguer, and Camilo Rocha

Department of Computer Science
University of Illinois at Urbana-Champaign
201 N. Goodwin Ave., Urbana, IL 61801-2302, USA

Abstract. Built-in equality and inequality predicates based on comparison of canonical forms in algebraic specifications are frequently used because they are handy and efficient. However, their use places algebraic specifications with initial algebra semantics beyond the pale of theorem proving tools based, for example, on explicit or inductionless induction techniques, and of other formal tools for checking key properties such as confluence, termination, and sufficient completeness. Such specifications would instead be amenable to formal analysis if an equationally-defined equality predicate enriching the algebraic data types were to be added to them. Furthermore, having an equationally-defined equality predicate is very useful in its own right, particularly in inductive theorem proving. Is it possible to *effectively* define a theory transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ that extends an algebraic specification $\mathcal{E}$ to a specification $\mathcal{E}^{\simeq}$ where equationally-defined equality predicates have been added? This paper answers this question in the affirmative for a broad class of order-sorted conditional specifications $\mathcal{E}$ that are sort-decreasing, ground confluent, and operationally terminating modulo axioms B and have subsignature of constructors. The axioms B can consist of associativity, or commutativity, or associativity-commutativity axioms, so that the constructors are *free modulo* B. We prove that the transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ preserves all the just-mentioned properties of $\mathcal{E}$. The transformation has been automated in Maude using reflection and it is used in Maude formal tools.

1 Introduction

It can be extremely useful, when reasoning about equational specifications with initial semantics, to have an explicit equational specification of the *equality predicate* as a binary Boolean-valued operator $\_ \simeq \_$. For example, in *theorem proving* where the logic of universal quantifier-free formulas is automatically reduced to unconditional equational logic, the formula $(u \neq v \vee w = r) \wedge q = t$ becomes equivalent to the equation $(not(u \simeq v)\ or\ w \simeq r)\ and\ q \simeq t = true$, and in *inductionless induction* where inductive proofs can be reduced to proofs by consistency because any equation not holding inductively makes $true = false$. An equationally-defined predicate can be useful in the *elimination of built-in equalities and inequalities* that often are introduced in algebraic specifications through built-in equality and inequality operators: such built-in equalities and

inequalities are not defined logically but operationally by comparison of canonical forms for both expressiveness and efficiency reasons, but their non-logical character renders any formal reasoning about specifications using them impossible. In particular, the *use of formal tools* such as those checking termination, local confluence, or sufficient completeness of an algebraic specification is impossible with built-in equalities and inequalities, but becomes possible when they are replaced by the equationally axiomatized equality predicate $\_ \simeq \_$.

In principle, the meta-theorem of Bergstra and Tucker [2] ensures that any computable data type can be axiomatized as an initial algebra defined by a finite number of Church-Rosser and terminating equations. This also means that such a computable data type *plus* its equality predicate is also finitely axiomatizable by a finite set of Church-Rosser and terminating equations. However, the Bergstra-Tucker result is *non-constructive* in the sense that it does not give an algorithm to actually obtain the equational specification of the data type with its equality predicate. Therefore, what would be highly desirable in practice is a general *constructive theory transformation* $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ that adds equationally-axiomatized equality predicates to an algebraic data type specification $\mathcal{E}$.

Such a transformation should be *as general as possible* for it to be useful in practice. For example, a transformation applying only to "vanilla-flavored" specifications without support for types and subtypes, or that excludes conditional equations and rewriting modulo axioms would be extremely limited. Such a transformation should also come with *strong preservation properties*. For example, if $\mathcal{E}$ is ground confluent, ground operationally terminating, and sufficiently complete, then $\mathcal{E}^{\simeq}$ should also enjoy these same properties that are often essential for both executability and for various forms of formal reasoning.

These generality and property-preservation requirements on the transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ are a tall order. For instance, if f is a free constructor symbol, then the equations $f(x_1, \ldots, x_n) \simeq f(y_1, \ldots, y_n) = x_1 \simeq y_1 \; and \ldots and \; x_n \simeq y_n$, and $f(x_1, \ldots, x_n) \simeq g(y_1, \ldots, y_m) = \mathit{false}$ for each constructor $g \neq f$ of same type give a perfectly good and straightforward axiomatization of equality for f. But how can the equality predicate be defined when f satisfies, e.g., associativity and commutativity axioms? Also, how should sorts and subsorts be dealt with? An even harder issue is the preservation of properties such as ground confluence, operational termination, and sufficient completeness. The difficulty is that for any given specification there are tools that can be used to prove such properties, but we need a proof that will work for *all* specifications in a very wide class. What we actually need are *metatheorems* that prove that the transformation itself preserves these properties for *any* equational specification in the input class.

We present in this paper an effective theory transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ that satisfies the above-mentioned preservation properties. The class of equational theories $\mathcal{E}$ accepted as inputs to the transformation is quite general. Modulo mild syntactic requirements, it consists of all order-sorted theories $\mathcal{E}$ of the form $(\Sigma, E \uplus B)$ having a subsignature Ω of constructors and such that: B is a set

of associativity, or commutativity, or associativity-commutativity axioms[1]; the equations E can be conditional and are sort-decreasing, ground confluent, and operationally terminating; and the constructors Ω are *free modulo* B, i.e., there is an isomorphism $\mathcal{T}_{\Sigma/E \uplus B}|_{\Omega} \cong \mathcal{T}_{\Omega/B}$ of initial algebras.

Outline. In Section 2 we present a summary on order-sorted equational specifications. Section 3 includes the definition and fundamental properties of an equality enrichment. In sections 4 and 5 we present the transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ and state its basic metatheorems. In Section 7 we summarize how the transformation has been implemented in Maude and some of its practical consequences. The implementation of the transformation, and some examples are all publicly available from `http://camilorocha.info`.

2 Preliminaries

We assume basic knowledge on term rewriting [14] and order-sorted algebra [6].

Order-Sorted Signatures and Terms. We assume an *order sorted signature* $\Sigma = (S, \leq, F)$ with a finite poset of sorts $(S, \leq)$ and a finite set of function symbols F. We also assume that the function symbols in F can be subsort overloaded and satisfy that if $f \in F_{w,s} \cap F_{w',s'}$ then $w \equiv_{\leq} w'$ implies $s \equiv_{\leq} s'$, where $\equiv_{\leq}$ denotes the equivalence relation generated by $\leq$ on S and $(w, s), (w', s') \in S^* \times S$. We say that $f : s_1 \cdots s_n \to s \in F$ is a maximal typing of f in Σ if there is no other $f : s'_1 \cdots s'_n \to s' \in F$ such that $s_i \leq s'_i$ and $s \leq s'$. We let $X = \{X_s\}_{s \in S}$ be an S-sorted family of disjoint sets of variables with each X_s countably infinite. The set of Σ-terms of sort s is denoted by $T_{\Sigma}(X)_s$ and the set of ground terms of sort s is denoted by $T_{\Sigma,s}$, which we assume nonempty for each s. We let $\mathcal{T}_{\Sigma}(X)$ and $\mathcal{T}_{\Sigma}$ denote the corresponding order-sorted term algebras. The set of variables of a term t is written $\mathcal{V}ar(t)$ and is extended to sets of terms in the natural way. A *substitution* σ is a sorted mapping from a finite subset $\mathcal{D}om(\sigma) \subseteq X$ to $T_{\Sigma}(X)$ and extends homomorphically in the natural way; $\mathcal{R}an(\sigma)$ denotes the set of variables introduced by σ. The application of a substitution σ to a term t is denoted by $t\sigma$ and the composition of two substitutions σ_1 and σ_2 is denoted by $\sigma_1\sigma_2$. A substitution σ is called *ground* iff $\mathcal{R}an(\sigma) = \varnothing$. Throughout this paper we will assume that all order-sorted signatures are *preregular* [6], so that each Σ-term t has a *least sort* $ls(t) \in S$ such that $t \in T_{\Sigma}(X)_{ls(t)}$.

Order-Sorted Equational Theories. A *Σ-equation* is an expression $t = t'$ with $t \in T_{\Sigma}(X)_s$, $t' \in T_{\Sigma}(X)_{s'}$ and $s \equiv_{\leq} s'$. A *conditional Σ-equation* is a Horn clause $t = t'$ if C with $t = t'$ a Σ-equation and $C = \bigwedge_i u_i = v_i$ a finite conjunction of Σ-equations. An *equational theory* is a tuple (Σ, E) with Σ an order-sorted signature and E a finite set of conditional Σ-equations. For φ a

[1] Identity axioms are excluded from our transformation. However, by using the transformation described in [4] and subsort-overloaded operators, one can often extend our transformation to specifications that also include identity axioms.

conditional Σ-equation, $(\Sigma, E) \vdash \varphi$ iff φ can be proved from (Σ, E) by the deduction rules in [10] iff φ is valid in all models of (Σ, E) [10]. An equational theory (Σ, E) induces the congruence relation $=_E$ on $T_\Sigma(X)$ defined for any $t, u \in T_\Sigma(X)$ by $t =_E u$ iff $(\Sigma, E) \vdash (\forall X)\, t = u$. We let $\mathcal{T}_{\Sigma/E}(X)$ and $\mathcal{T}_{\Sigma/E}$ denote the quotient algebras induced by $=_E$ on the algebras $\mathcal{T}_\Sigma(X)$ and $\mathcal{T}_\Sigma$, respectively. We call $\mathcal{T}_{\Sigma/E}$ the *initial algebra* of (Σ, E) and call a conditional Σ-equation φ an *inductive consequence* of (Σ, E) iff $\mathcal{T}_{\Sigma/E} \models \varphi$, i.e., iff $(\forall \sigma : X \longrightarrow T_\Sigma)(\Sigma, E) \vdash \varphi\sigma$. A theory inclusion $(\Sigma, E) \subseteq (\Sigma', E')$, where $\Sigma \subseteq \Sigma'$ and $E \subseteq E'$, is called *protecting* iff the unique Σ-homomorphism $\mathcal{T}_{\Sigma/E} \longrightarrow \mathcal{T}_{\Sigma'/E'|\Sigma}$ of the Σ-reduct of the initial algebra $\mathcal{T}_{\Sigma'/E'}$ is a Σ-isomorphism.

Executability Conditions. We assume that the set of equations of an equational theory can be decomposed into a disjoint union $E \uplus B$, with B a collection of axioms (such as associativity, and/or commutativity, and/or identity) for which there exists a *matching algorithm modulo* B producing a finite number of B-matching substitutions, or failing otherwise. Furthermore, we assume that all axioms in B are *sort-preserving*, i.e., for each $u = v \in B$ and substitution θ we have $ls(\theta(u)) = ls(\theta(v))$. The conditional equations E can be oriented into a set of (possibly conditional) *ground sort-decreasing*, *operationally terminating* [9], and *ground confluent conditional* rewrite rules $\overrightarrow{E}$ modulo B. We let $\rightarrow_{E/B}$ denote the one-step rewrite relation induced by $\overrightarrow{E}$ modulo B on $T_\Sigma(X)$, and let $\rightarrow^*_{E/B}$ denote its reflexive and transitive closure. A set of rewrite rules R modulo B is: (i) ground sort-decreasing iff for each $t = t'$ if $C \in E$, and ground substitution θ we have $ls(\theta(t)) \geq ls(\theta(t'))$; (ii) operationally terminating iff there is no infinite well-formed proof tree modulo B in R; and (iii) ground confluent if $t, t', t'' \in T_\Sigma$, $t \rightarrow^*_{R/B} t'$, and $t \rightarrow^*_{R/B} t''$, then there is $u \in T_\Sigma$ such that $t' \rightarrow^*_{R/B} u$ and $t'' \rightarrow^*_{R/B} u$. We let $\mathrm{can}_{\Sigma,E/B}(t) \in T_{\Sigma,s}$ denote the *E-canonical form* of t modulo B, i.e. $t \rightarrow^*_{R/B} \mathrm{can}_{\Sigma,E/B}(t)$ and $\mathrm{can}_{\Sigma,E/B}(t)$ cannot be further rewritten. Under the above assumptions $\mathrm{can}_{\Sigma,E/B}(t)$ is unique up to B-equality.

Free Constructors Modulo. Given $\mathcal{E} = (\Sigma, E \uplus B)$ ground sort-decreasing, ground confluent and operationally terminating modulo B, we say that $\Omega \subseteq \Sigma$ is a subsignature of *free constructors* modulo B iff Ω has the same poset of sorts of Σ and for each sort s in Σ and ground term $t \in T_{\Sigma,s}$ there is a $u \in T_{\Omega,s}$ satisfying $t =_{E \uplus B} u$ and, moreover, $\mathrm{can}_{\Sigma,E/B}(v) =_B v$ for each $v \in T_{\Omega,s}$.

3 Equality Enrichments

In this section, the notion of *equality enrichment* [11] for an equational theory is introduced. Intuitively, an equality enrichment of $\mathcal{E}$ is an equational theory that defines the equality in $\mathcal{T}_\mathcal{E}$ as a Boolean-valued function. An order-sorted signature $\Sigma = (S, \leq, F)$ and an order-sorted equational theory $\mathcal{E} = (\Sigma, E)$ with initial algebra $\mathcal{T}_\mathcal{E}$ are fixed in this section.

Definition 1 (Equality Enrichment). *An equational theory* $\mathcal{E}^{\simeq} = (\Sigma^{\simeq}, E^{\simeq})$ *is called an* equality enrichment *of* $\mathcal{E}$*, with* $\Sigma^{\simeq} = (S^{\simeq}, \leq^{\simeq}, F^{\simeq})$ *and* $\Sigma = (S, \leq, F)$*, iff*

- $\mathcal{E}^{\simeq}$ *is a protecting extension of* $\mathcal{E}$*;*
- *the poset of sorts of* $\Sigma^{\simeq}$ *extends* $(S, \leq)$ *by adding a new sort* Bool *that belongs to a new connected component, with constants* $\top$ *and* $\bot$ *such that* $\mathcal{T}_{\mathcal{E}^{\simeq},\mathrm{Bool}} = \{[\top], [\bot]\}$*, with* $\top \neq_{E^{\simeq}} \bot$*; and*
- *for each connected component in* $(S, \leq)$*, there is a top sort* $k \in S^{\simeq}$ *and a binary commutative operator* $\_ \simeq \_ : k\ k \longrightarrow \mathrm{Bool}$ *in* $\Sigma^{\simeq}$ *such that, for any ground terms* $t, u \in T_{\Sigma,k}$*, then the following hold*

$$\mathcal{E} \vdash t = u \iff \mathcal{E}^{\simeq} \vdash (t \simeq u) = \top, \tag{1}$$
$$\mathcal{E} \nvdash t = u \iff \mathcal{E}^{\simeq} \vdash (t \simeq u) = \bot. \tag{2}$$

An equality enrichment $\mathcal{E}^{\simeq}$ *of* $\mathcal{E}$ *is* Boolean *if it contains all the function symbols and equations making the elements of* $\mathcal{T}_{\mathcal{E}^{\simeq},\mathrm{Bool}}$ *a two-element Boolean algebra.*

The equality predicate $\simeq$ in $\mathcal{E}^{\simeq}$ is sound for inferring equalities and inequalities in the initial algebra $\mathcal{T}_{\mathcal{E}}$, even for terms with variables. The precise meaning of this claim is given by Proposition 1.

Proposition 1 (Equality Enrichment Properties). *Let* $\mathcal{E}^{\simeq} = (\Sigma^{\simeq}, E^{\simeq})$ *be an equality enrichment of* $\mathcal{E}$*. Then, for any* Σ*-equation* $t = u$ *with* $X = \mathcal{V}ar(t) \cup \mathcal{V}ar(u)$*:*

$$\mathcal{T}_{\mathcal{E}} \models (\forall X)\ t = u \iff \mathcal{T}_{\mathcal{E}^{\simeq}} \models (\forall X)\ (t \simeq u) = \top, \tag{3}$$
$$\mathcal{T}_{\mathcal{E}} \models (\exists X)\ \neg(t = u) \iff \mathcal{T}_{\mathcal{E}^{\simeq}} \models (\exists X)\ (t \simeq u) = \bot, \tag{4}$$
$$\mathcal{T}_{\mathcal{E}} \models (\forall X)\ \neg(t = u) \iff \mathcal{T}_{\mathcal{E}^{\simeq}} \models (\forall X)\ (t \simeq u) = \bot. \tag{5}$$

Proof. We prove Statement (3); a proof of statements (4) and (5) can be obtained in a similar way.

$\mathcal{T}_{\mathcal{E}} \models (\forall X)\ t = u$
$\iff$ { by definition of satisfaction in $\mathcal{T}_{\mathcal{E}}$ }
$(\forall \theta : X \longrightarrow T_{\Sigma})\ \mathcal{E} \vdash t\theta = u\theta$
$\iff$ { by (1) }
$(\forall \theta : X \longrightarrow T_{\Sigma})\ \mathcal{E}^{\simeq} \vdash (t\theta \simeq u\theta) = \top$
$\iff$ { by $\mathcal{E}^{\simeq}$ being a protecting theory extension of $\mathcal{E}$ and sorts of $t, u \in \Sigma$ }
$(\forall \theta : X \longrightarrow T_{\Sigma^{\simeq}})\ \mathcal{E}^{\simeq} \vdash (t\theta \simeq u\theta) = \top$
$\iff$ { by definition of satisfaction in $\mathcal{T}_{\mathcal{E}^{\simeq}}$ }
$\mathcal{T}_{\mathcal{E}^{\simeq}} \models (\forall X)\ (t \simeq u) = \top.$

□

Note that by using an equality enrichment $\mathcal{E}^{\simeq}$ of $\mathcal{E}$, the problem of reasoning in $\mathcal{T}_{\mathcal{E}}$ about a universally quantified inequality $\neg(t = u)$ (or simply $t \neq u$) can be reduced to reasoning in $\mathcal{T}_{\mathcal{E}^{\simeq}}$ about the universally quantified equality

$(t \simeq u) = \bot$. A considerably more general reduction, not just for inequalities but for *arbitrary quantifier-free first-order formulae*, can be obtained with Boolean equality enrichments, as stated by Corollary 1.

Corollary 1. *Let $\mathcal{E}^{\simeq} = (\Sigma^{\simeq}, E^{\simeq})$ be a Boolean equational enrichment of $\mathcal{E}$. Let $\varphi = \varphi(t_1 = u_1, \ldots, t_n = u_n)$ be a quantifier-free Boolean formula whose atoms are the Σ-equalities $t_i = u_i$ with variables in X, for $1 \leq i \leq n$, and whose Boolean connectives are $\neg$, $\vee$, and $\wedge$. Then, the following holds*

$$\mathcal{T}_{\mathcal{E}} \models (\forall X)\varphi \iff \mathcal{T}_{\mathcal{E}^{\simeq}} \models (\forall X)\ \varphi(t_1 \simeq u_1, \ldots, t_n \simeq u_n) = \top, \tag{6}$$

where $\varphi(t_1 \simeq u_1, \ldots, t_n \simeq u_n)$ is the $\Sigma^{\simeq}$-term with sort Bool *obtained from φ by replacing every occurrence of the logical connectives $\neg$, $\vee$, and $\wedge$ by, respectively, the function symbols $\sqsupset$, $\sqcup$, and $\sqcap$ in $\mathcal{E}^{\mathrm{Bool}}$, making $\mathcal{T}_{\mathcal{E},\mathrm{Bool}}$ a Boolean algebra, and every occurrence of an atom $t_i = u_i$ by the* Bool *term $t_i \simeq u_i$, for $1 \leq i \leq n$.*

Proof. It follows by considering all ground substitutions and reasoning by structural induction on the complexity of φ. Note that the base cases are covered by statements (1) and (2). □

A fundamental property of an equality enrichment $\mathcal{E}^{\simeq}$ of $\mathcal{E}$ is that, if $\mathcal{E}^{\simeq}$ is extended with any set E' of Σ-equations that are *not* satisfiable in $\mathcal{T}_{\mathcal{E}}$, then the resulting extension is inconsistent and can derive the *contradiction* $\top = \bot$. Conversely, if the set E' of Σ-equations extending $\mathcal{E}^{\simeq}$ is satisfiable in $\mathcal{T}_{\mathcal{E}}$, then the resulting extension is consistent and therefore cannot yield a proof of contradiction. Statements (7) and (8) in Corollary 2 account for these facts. We use the following auxiliar result.

Lemma 1. *Let E, E' be two sets of Σ-equations. Then $\mathcal{T}_{\Sigma/E} \models E'$ iff $\mathcal{T}_{\Sigma/E} \cong \mathcal{T}_{\Sigma/E \cup E'}$*

Proof. The ($\Leftarrow$) direction is clear, since we always have $\mathcal{T}_{\Sigma/E\cup E'} \models E'$, and therefore (since satisfaction is preserved by isomorphisms) $\mathcal{T}_{\Sigma/E} \models E'$. To see the ($\Rightarrow$) direction, note that, since $\mathcal{T}_{\Sigma/E} \models E$, we have $\mathcal{T}_{\Sigma/E} \models E \cup E'$. The initiality of $\mathcal{T}_{\Sigma/E\cup E'}$ then forces the existence of a unique Σ-homomorphism $h : \mathcal{T}_{\Sigma/E\cup E'} \to \mathcal{T}_{\Sigma/E}$, and the initiality of $\mathcal{T}_{\Sigma/E}$ and the fact that $\mathcal{T}_{\Sigma/E\cup E'} \models E$ forces likewise a unique Σ-homomorphism $q : \mathcal{T}_{\Sigma/E} \to \mathcal{T}_{\Sigma/E\cup E'}$. But then the initially of $\mathcal{T}_{\Sigma/E}$ forces $q; h = 1_{\mathcal{T}_{\Sigma/E}}$, and the initiality of $\mathcal{T}_{\Sigma/E\cup E'}$ forces $h; q = 1_{\mathcal{T}_{\Sigma/E\cup E'}}$. Therefore, $\mathcal{T}_{\Sigma/E} \cong \mathcal{T}_{\Sigma/E\cup E'}$, as desired. □

Corollary 2. *Let $\mathcal{E}^{\simeq} = (\Sigma^{\simeq}, E^{\simeq})$ be a equational enrichment of $\mathcal{E}$ and let E' be a collection of Σ-equalities. Then the following hold*

$$\mathcal{T}_{\mathcal{E}} \not\models E' \iff (\Sigma^{\simeq}, E^{\simeq} \cup E') \vdash \top = \bot, \tag{7}$$

$$\mathcal{T}_{\mathcal{E}} \models E' \iff (\Sigma^{\simeq}, E^{\simeq} \cup E') \not\vdash \top = \bot. \tag{8}$$

Proof. Note that statements (7) and (8) are logically equivalent. The following is a proof of (7). Without loss of generality assume that the Σ-equalities in E' are unconditional[2].

We first prove the ($\Rightarrow$) direction.

$$
\begin{array}{ll}
& \mathcal{T}_{\Sigma/E} \models E' \\
\iff & \{ \text{ by } \mathcal{E}^{\simeq} \text{ being a protecting theory extension of } \mathcal{E} \ \} \\
& \mathcal{T}_{\Sigma^{\simeq}/E^{\simeq}} \models E' \\
\iff & \{ \text{ by Lemma 1 } \} \\
& \mathcal{T}_{\Sigma^{\simeq}/E^{\simeq} \cup E'} \cong \mathcal{T}_{\Sigma^{\simeq}/E^{\simeq}} .
\end{array}
$$

Therefore $\mathcal{T}_{\Sigma^{\simeq}/E^{\simeq} \cup E', \mathrm{Bool}} = \{[\top], [\bot]\}$, and hence $(\Sigma^{\simeq}, E^{\simeq} \cup E') \not\vdash \top = \bot$.

To prove the ($\Leftarrow$) direction we reason by contradiction. Suppose that $(\Sigma^{\simeq}, E^{\simeq} \cup E') \vdash \top = \bot$. This means that $\mathcal{T}_{\Sigma^{\simeq}/E^{\simeq}} \ncong \mathcal{T}_{\Sigma^{\simeq}/E^{\simeq} \cup E'}$ and therefore by Lemma 1, $\mathcal{T}_{\Sigma^{\simeq}/E^{\simeq}} \not\models E'$, which by $\mathcal{E}^{\simeq}$ being a protecting extension of $\mathcal{E}$ forces $\mathcal{T}_{\Sigma/E} \not\models E'$. □

4 Equality Enrichments of Theories with Free Constructors Modulo

This section presents the effective theory transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ for enriching with an equality predicate order-sorted equational theories having free constructors modulo structural axioms (such as associativity, commutativity, and identity). Given an equational theory $\mathcal{E}$ as input, Definition 2 produces a Boolean equality enrichment $\mathcal{E}^{\simeq}$ of $\mathcal{E}$ with equality predicate $\simeq$. In this section, an order-sorted equational theory $\mathcal{E} = (\Sigma, E \uplus B)$, with $\Sigma = (S, \leq, F)$, is fixed. It is assumed that $\Omega \subseteq \Sigma$ is a signature of free constructors modulo B, where B is a union of associative (A), commutative (C) and associative-commutative (AC) axioms[3]. Furthermore, the following convention is adopted: for x a variable and s a sort, the expression x_s indicates that x has sort s, i.e., $x \in X_s$.

On input $\mathcal{E}$, a first transformation extends $\mathcal{E}$ with new sorts, the equational theory $\mathcal{E}^{\mathrm{Bool}}$ of Booleans with constructors $\top$ and $\bot$ (and with the other usual Boolean connectives equationally defined), some auxiliary functions, and the predicate $\simeq$ for each top sort in the input theory. A second transformation generates a set of equations defining $\simeq$ that depend on the structural axioms of the symbols in Ω. More precisely,

Transformation 1: extends the input theory $\mathcal{E}$ by:

[2] If the equations E' are conditional, we can replace them by the set $E'' = \{t = t' \mid E \cup E' \vdash t = t'\}$. It is then easy to prove that $\mathcal{T}_{\mathcal{E}} \models E'$ iff $\mathcal{T}_{\mathcal{E}} \models E''$.

[3] Note that combinations of the above axioms with identity axioms are excluded. However, using the variant-based semantic-preserving theory transformation presented in [4], and choosing carefully the sorts in Ω, one can associate an equality predicate to equational theories having any combination of axioms A and/or C and/or identity.

1. generating a fresh top sort for each connected component in Σ that does not have it;
2. adding the theory $\mathcal{E}^{\mathrm{Bool}}$ with sort Bool;
3. adding a Boolean-valued (binary) commutative operator $\simeq$ for the top sort of each conected component of $\mathcal{E}$;
4. adding the Boolean-valued unary operator root_f^k and the Boolean-valued binary operator in_f^k to the top sort of each $f \in \Omega$ with structural axioms A or AC.

Transformation 2: for each $f \in \Omega$, and depending on the structural axioms of f, generate a suitable set of equations defining $\simeq$, root_f^k, and in_f^k.

Auxiliary Boolean-valued operators root_f^k and in_f^k are useful for checking if terms are rooted by or contain the constructor symbol f, respectively.

Remark 1. This paper uses the Boolean theory $\mathcal{E}^{\mathrm{Bool}}$ in [3, Subsection 9.1]. The theory $\mathcal{E}^{\mathrm{Bool}}$ has free constructors modulo B^{Bool}, it is sort-decreasing, confluent, and operationally terminating modulo AC, and hence provides a Boolean decision procedure; its signature of free constructors is $\Omega^{\mathrm{Bool}} = \{\top, \bot\}$, its set of defined symbols is $\Sigma^{\mathrm{Bool}} \backslash \Omega^{\mathrm{Bool}} = \{\, \lrcorner\,, \sqcap\,, \sqcup\,, \oplus\,, \supset \,\}$, and also $\mathcal{T}_{\mathcal{E}^{\mathrm{Bool}}} \models \top \neq \bot$.

Definition 2 spells out in detail Transformation 1 and prepares the ground for Transformation 2.

Definition 2 (Enrich). *Given $\mathcal{E}$, the transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ obtains the smallest equational theory $\mathcal{E}^{\simeq} = (\Sigma^{\simeq}, E^{\simeq} \uplus B^{\simeq})$ satisfying:*

- $\mathcal{E} \uplus \mathcal{E}^{\mathrm{Bool}} \subseteq \mathcal{E}^{\simeq}$;
- *the poset of sorts of $\mathcal{E}^{\simeq}$ extends that of $\mathcal{E}$ by adding a new connected component* {Bool}*, and by adding a fresh top sort to any connected component of the poset of sorts of $\mathcal{E}$ lacking a top sort;*
- *for each k which is the top sort in $\Sigma^{\simeq}$ of a connected component of Σ we add an operator*

$$(\_ \simeq \_) : k\ k \to \mathrm{Bool},$$

  $B^{\simeq}$ contains the structural axiom

$$x_k \simeq y_k = y_k \simeq x_k,$$

  $E^{\simeq}$ contains the equation

$$x_k \simeq x_k = \top,$$

- *for each k which is the top sort in $\Sigma^{\simeq}$ of a connected component of Σ*
  - *if $f : s\ s' \to s'' \in \Omega$ has axioms A or AC, then $\Sigma^{\simeq}$ contains the symbol*

$$\mathrm{root}_f^k : k \to \mathrm{Bool},$$

  - *if $f : s\ s' \to s'' \in \Omega$ has axioms AC, then $\Sigma^{\simeq}$ contains the symbol*

$$\mathrm{in}_f^k : k\ k \to \mathrm{Bool},$$

– *for each function symbol* $f \in \Omega$, $E^{\simeq}$ *contains the equations* $\mathsf{enrich}_{\mathcal{E}}(f)$ *(see the upcomming definitions).*

Function $\mathsf{enrich}_{\mathcal{E}}$ in Definition 2 corresponds to the formal definition of Transformation 2 and is defined for each constructor symbol depending on its structural axioms. We start by giving the definition of $\mathsf{enrich}_{\mathcal{E}}$ for the case in which the constructor symbol has no structural axioms; we call such a symbol *absolutely free*. In the rest of the paper we use the acronyms C, A, and AC to qualify a function symbol whose structural axioms are commutativity, associativity, or associativity-commutativity, respectively.

Definition 3 (Absolutely Free Enrich). *Assume* $f \in \Omega$ *is an absolutely free symbol. Then, for each maximal typing* $f : s_1 \dots s_n \to s$ *of* $f \in \Omega$, $\mathsf{enrich}_{\mathcal{E}}(f)$ *adds the following equations:*

– *for* $g : s'_1 \dots s'_m \to s' \in \Omega$ *a maximal typing of* g *such that* $s \equiv_{\leq} s'$ *and* $f \neq g$

$$f(x^1_{s_1}, \dots, x^1_{s_n}) \simeq g(y^1_{s'_1}, \dots, y^m_{s'_m}) = \bot,$$

– *for* f *itself*

$$f(x^1_{s_1}, \dots, x^n_{s_n}) \simeq f(y^1_{s_1}, \dots, y^n_{s_n}) = \bigsqcap_{1 \leq i \leq n} x^i_{s_i} \simeq y^i_{s_i},$$

– *for each* $1 \leq i \leq n$

$$f(x^1_{s_1}, \dots, x^n_{s_n}) \simeq x^i_{s_i} = \bot.$$

In Definition 3, some equations use the Boolean operator $\sqcap$ in $\mathcal{E}^{\mathrm{Bool}}$ to obtain a recursive definition of $\simeq$. Example 1 illustrates Definition 2 and Definition 3.

Example 1. Consider the following equational theory $\mathcal{E}^{\texttt{NATURAL}}$ that represents the natural numbers in Peano notation:

```
fmod NATURAL is
  sort Nat .
  op 0    : -> Nat [ctor] .
  op s    : Nat -> Nat [ctor] .
endfm
```

An equality enrichment consist of $\mathcal{E}^{\texttt{NATURAL}}$ extended with the equational theory $\mathcal{E}^{\mathrm{Bool}}$ and an equational definition of $\simeq$. The following equational theory $\mathcal{E}^{\texttt{EQ-NATURAL}}$ is an equational enrichment of $\mathcal{E}^{\texttt{NATURAL}}$. The last equation is not essential, but it is useful for detecting a greater number of inequalities between terms with variables.

```
fmod EQ-NATURAL is
  protecting PEANO .
  protecting BOOL .

  op _==_ : Nat Nat -> Bool [comm] .
```

```
  vars N M : Nat .

  eq N == N    = true .
  eq 0 == s(N) = false .
  eq s(N) == s(M) = N == M .
  eq s(N) == N    = false .
endfm
```

Definition 4 presents the definition or $\mathsf{enrich}_{\mathcal{E}}$ for the case in which the input symbol is commutative.

Definition 4 (C-Enrich). *Assume $f \in \Omega$ is commutative. Then for each maximal typing $f : s\ s \to s'$ of $f \in \Omega$, $\mathsf{enrich}_{\mathcal{E}}(f)$ adds the following equations:*

- *for $g : s'_1 \dots s'_m \to s'$ a maximal typing of $g \in \Omega$ such that $f \neq g$*

$$f(x^1_s, x^2_s) \simeq g(y^1_{s'_1}, \dots, y^m_{s'_m}) = \bot,$$

- *for f itself*

$$f(x^1_s, x^2_s) \simeq f(y^1_s, y^2_s) = (x^1_s \simeq y^1_s \sqcap x^2_s \simeq y^2_s) \sqcup (x^1_s \simeq y^2_s \sqcap x^2_s \simeq y^1_s),$$

- *and*

$$f(x^1_s, x^2_s) \simeq x^1_s = \bot.$$

For the definition of $\mathsf{enrich}_{\mathcal{E}}$ in the case of an associative function symbol f with maximal typing of sort s, it is assumed that its two arguments have also sort s. Furthermore, a *top typing* for such an f is also assumed, i.e., a typing $f : s'\ s' \to s'$ satisfying that if $f : s\ s \to s$ is another typing with $s \equiv_< s'$, then $s' \geq s$ (note that a top typing of f may not belong to Ω, as in Example 2 below).

Definition 5 (A-Enrich). *Assume $f \in \Omega$ is associative. Then for each maximal typing $f : s\ s \to s$ of $f \in \Omega$, $\mathsf{enrich}_{\mathcal{E}}(f)$ adds the following equations:*

- *for f itself*

$$\mathrm{root}^k_f(f(x^1_s, x^n_s)) = \top,$$

- *for each $g : s'_1 \dots s'_m \to s'$ a maximal typing of $g \in \Omega$ such that $f \neq g$ and $s \equiv_\leq s'$:*

$$\mathrm{root}^k_f(g(x^1_{s'_1}, \dots, x^m_{s'_m})) = \bot \quad \textit{and} \quad f(x^1_s, x^2_s) \simeq g(y_{s'_1}, \dots, y^m_{s'_m}) = \bot,$$

- *for f itself*

$$\begin{array}{lll} f(x^1_s, x^2_s) \simeq f(x^1_s, y^2_s) = x^2_s \simeq y^2_s, & & \\ f(x^1_s, x^2_s) \simeq f(y^1_s, x^2_s) = x^1_s \simeq y^1_s, & & \\ f(x^1_s, x^2_s) \simeq f(y^1_s, y^2_s) = \bot & \textit{if} & \neg\,(\mathrm{root}^k_f(x^1_s)) \ \sqcap \\ & & \neg\,(\mathrm{root}^k_f(y^1_s)) \ \sqcap \\ & & \neg\,(x^1_s \simeq y^1_s) = \top, \end{array}$$

– *for each* $1 \leq i \leq 2$*:*

$$f(x_s^1, x_s^2) \simeq x_s^i = \bot.$$

Example 2. Consider the following equational theory $\mathcal{E}^{\mathtt{LIST}}$ that specifies the lists of natural numbers in Peano notation:

```
fmod LIST is
  protecting NATURAL .

  sorts NeNatList NatList .
  subsorts Nat < NeNatList < NatList .

  op nil : -> NatList [ctor] .
  op _;_ : NeNatList NeNatList -> NeNatList [ctor assoc] .
  op _;_ : NatList NatList -> NatList [assoc] .

  var L : NatList .

  eq L ; nil = L .
  eq nil ; L = L .
endfm
```

Note that _;_ is a constructor symbol only when its arguments are non-empty lists. Hence the signature of free constructors modulo B of $\mathcal{E}^{\mathtt{LIST}}$ is $\{$`nil : -> NatList`, `_;_ : NeNatList NeNatList -> NeNatList`$\}$. In order to have a recursive definition of equality for lists, $\mathsf{enrich}_{\mathcal{E}}(f)$ uses the auxiliar function root_f^k. This function checks if a term is rooted by constructor symbol f. In this case, a valid equality enrichment can be:

```
fmod EQ-LIST is
  protecting LIST .
  protecting BOOL .

  op ;-NeNatList-root : NatList -> Bool .
  op _==_  : NatList NatList -> Bool [comm] .

  vars P Q R S : NeNatList .
  var N : Nat .

  eq ;-NeNatList-root(0) = false .
  eq ;-NeNatList-root(s(N)) = false .
  eq ;-NeNatList-root(nil) = false .
  eq ;-NeNatList-root(P ; Q) = true .
  eq P == P = true .
  eq 0 == nil = false .
  eq s(N) == nil = false .
  eq (P ; Q) == 0 = false .
```

```
  eq (P ; Q) == s(N) = false .
  eq (P ; Q) == nil = false .
  eq (P ; Q) == P = false .
  eq (P ; Q) == Q = false .
  eq (P ; Q) == (P ; R) = Q == R .
  eq (P ; Q) == (R ; Q) = P == R .
  ceq (P ; Q) == (R ; S) = false
                           if (not(;-NeNatList-root(P)) and
                               not(;-NeNatList-root(R)) and
                               not(P == R)) = true .
endfm
```

In the case in which the input symbol of $\mathsf{enrich}_{\mathcal{E}}$ with maximal typing of sort s is associative-commutative, it is assumed that its two arguments also have sort s and there is a *top typing* for f, as in the associative case.

Definition 6 (AC-Enrich). *Assume $f \in \Omega$ is associative-commutative. Then for each maximal typing $f : s\ s \to s'$ of $f \in \Omega$, $\mathsf{enrich}_{\mathcal{E}}(f)$ adds the following equations:*

- *for f itself*
$$\mathrm{root}^k_f(f(x^1_s, x^2_s)) = \top,$$
- *for each $g : s'_1 \dots s'_m \to s'$ a maximal typing of $g \in \Omega$ such that $f \neq g$ and $s \equiv_{\leq} s'$:*
$$\mathrm{root}^k_f(g(x^1_{s'_1}, \dots, x^m_{s'_m})) = \bot,$$
- *and*
$$f(x^1_s, x^2_s) \simeq g(y^1_{s'_1}, \dots, y^m_{s'_m}) = \bot,$$
- *for f itself*
$$\begin{aligned}
\mathrm{in}^k_f(x_s, y_k) &= \bot && \text{if } \mathrm{root}^k_f(x_s) = \top,\\
\mathrm{in}^k_f(x_s, f(x_s, y_s)) &= \top && \text{if } \neg(\mathrm{root}^k_f(x_s)) = \top,\\
\mathrm{in}^k_f(x_k, f(y^1_s, y^2_s)) &= (x_k \simeq y^1_s) \sqcup \mathrm{in}^k_f(x_k, y^2_s) \\
& && \text{if } \neg(\mathrm{root}^k_f(x_k)) \sqcap \neg(\mathrm{root}^k_f(y^1_s)) = \top,\\
\mathrm{in}^k_f(x_k, y_k) &= x_k \simeq y_k && \text{if } \neg(\mathrm{root}^k_f(x_k)) \sqcap \neg(\mathrm{root}^k_f(y_k)) = \top,
\end{aligned}$$
- *and*
$$\begin{aligned}
&\mathsf{f}(x_s, y_s) \simeq \mathsf{f}(x_s, z_s) = y_s \simeq z_s,\\
&\mathsf{f}(x^1_s, x^2_s) \simeq \mathsf{f}(y^1_s, y^2_s) = \bot \qquad \text{if } \neg(\mathrm{root}^k_f(x^1_s))) \sqcap \\
&\qquad\qquad \neg(\mathrm{in}^k_f(x^1_s, f(y^1_s, y^2_s))) = \top,
\end{aligned}$$
- *and*
$$f(x^1_s, x^2_s) \simeq x^1_s = \bot.$$

Intuitively, if we identify a term rooted by an associative-commutative symbol f as a multiset with union operator f, the function in^k_f in Definition 6 helps in identifying the cases in which an element (a term not rooted by f) belongs to the multiset.

Example 3. Consider the following equational theory $\mathcal{E}^{\mathtt{MSET}}$, which represents multisets of natural numbers in Peano notation:

```
fmod MSET is
  protecting NATURAL .

  sorts NeNatMSet NatMSet .
  subsort Nat < NeNatMSet < NatMSet .

  op empty : -> NatMSet [ctor] .
  op __   : NeNatMSet NeNatMSet -> NeNatMSet [ctor assoc comm] .
  op __   : NatMSet NatMSet -> NatMSet [assoc comm] .

  var T : NatMSet .

  eq empty T = T .
endfm
```

Auxiliary functions root_f^k and in_f^k are used to give a recursive comparison of equality for constructors terms rooted by AC-symbols. In this case, the following is a valid equality enrichment for `MSET`:

```
fmod EQ-MSET is
  protecting MSET .
  protecting BOOL .

  op -NeNatMSet-root : NatMSet -> Bool .
  op in--NeNatMSet   : NatMSet NatMSet -> Bool .
  op _==_ : NatMSet NatMSet -> Bool [comm] .

  vars P Q R S : NeNatMSet .
  var N : Nat .
  vars T U : NatMSet .

  eq -NeNatMSet-root(0) = false .
  eq -NeNatMSet-root(s(N)) = false .
  eq -NeNatMSet-root(empty) = false .
  eq -NeNatMSet-root(P Q) = true .
  ceq in--NeNatMSet(P,Q) = false
                       if -NeNatMSet-root(P) = true .
  ceq in--NeNatMSet(P, (P Q)) = true
                            if not(-NeNatMSet-root(P)) = true .
  ceq in--NeNatMSet(T, (Q R)) = (T == Q) or in--NeNatMSet(T,R)
                            if (not(-NeNatMSet-root(T)) and
                                not(-NeNatMSet-root(Q))) = true .
  ceq in--NeNatMSet(T,U) = T == U
                       if (not(-NeNatMSet-root(T)) and
```

```
                              not(-NeNatMSet-root(U))) = true .

  eq P == P = true .
  eq 0 == empty = false .
  eq s(X5) == empty = false .
  eq (P Q) == 0 = false .
  eq (P Q) == empty = false .
  eq (P Q) == s(X5) = false .
  eq (P Q) == P = false .
  eq (P Q) == (P R) = Q == R .
  ceq (P Q) == (R S) = false
                    if (not(-NeNatMSet-root(P)) and
                        not(in--NeNatMSet(P, R S))) = true .

endfm
```

5 Executability Properties of $\mathcal{E}^{\simeq}$

From a theoretical and practical point of view, it is quite convenient that if our original theory satisfies some executability properties, the Boolean equality enrichment $\mathcal{E}^{\simeq}$ of $\mathcal{E}$ using the transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ inherits these executability properties. In particular, if the original theory $\mathcal{E}$ is ground sort-decreasing, ground confluent, and operationally terminating, then $\mathcal{E}^{\simeq}$ is so as well. Moreover, the subsignature of constructors of $\mathcal{E}^{\simeq}$ is an extension of the subsignature of constructors of $\mathcal{E}$ and its function symbols are free (modulo the structural axioms). Thus, the agreement between mathematical and operational semantics is preserved.

Note that the domain of the transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ includes exactly equational theories whose structural axioms are any combination of A and/or C axioms for some of its symbols. However, if the input theory $\mathcal{E}$ has symbols with identity axioms, one could use the results in [4] to remove them and instead add them as equations, provided that the constructors remain free after the transformation. Note that, as illustrated by the `LIST` and `MSET` examples, where identities for lists and multisets are specified as oriented equations and not as axioms, this is often possible in practice.

In what follows, $\mathcal{E} = (\Sigma, E \uplus B)$ is an order-sorted equational theory with signature of free constructors $\Omega \subseteq \Sigma$ modulo B and $\mathcal{E}^{\simeq} = (\Sigma^{\simeq}, E^{\simeq} \uplus B^{\simeq})$ is the Boolean equality enrichment $\mathcal{E}^{\simeq}$ obatined by using the transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$.

5.1 Preservation of Ground Sort-Decreasingness

Recall from Section 2 that the equational theory $\mathcal{E} = (\Sigma, E \uplus B)$ is ground sort-decreasing iff for each $t = t'$ if $C \in E$, and ground substitution θ we have $ls(\theta(t)) \geq ls(\theta(t'))$. The key observation here is that since Bool is a fresh sort in

a new connected component of $\mathcal{E}^{\simeq}$ and all the equations in $\bigcup_{f \in \Omega} \mathsf{enrich}_{\mathcal{E}}(f)$ are of sort Bool, it is imposible that the equations in $\mathcal{E}^{\mathrm{Bool}}$ or in $\bigcup_{f \in \Omega} \mathsf{enrich}_{\mathcal{E}}(f)$ can be applied to terms in T_{Σ}.

Theorem 1. *If $\mathcal{E}$ is ground sort-decreasing, then $\mathcal{E}^{\simeq}$ is ground sort-decreasing.*

Proof. Consider the following cases on the equations in $\mathcal{E}^{\simeq}$:

1. any equation in $\mathcal{E}$ is sort-decreasing by assumption,
2. if an equation is in $\mathcal{E}^{\simeq}$ but not in $\mathcal{E}$, then the left-hand and right-hand sides of such an equation have least sort Bool because Bool has no proper subsorts or supersorts.

□

5.2 Preservation of Operational Termination

The key idea here is to use the information that the input theory $\mathcal{E}$ of the transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ is operationally terminating to obtain a modular and much simpler proof of operational termination for $\mathcal{E}^{\simeq}$. The notion of reductive theory is key for proving $\mathcal{E}^{\simeq}$ operationally terminating.

Definition 7 (Reductive Theory Modulo Axioms). *An equational theory $\mathcal{E} = (\Sigma, E \uplus B)$ is* reductive modulo B *iff there exists a reduction ordering $\succ$ and a symetric, stable, and monotonic relation $\sim$ such that:*

1. *$l \notin X$ for each equation $l = r$ if $\bigwedge_{i=1..n} t_i = u_i \in E$.*
2. *$l \succ r$ for each equation $l = r$ if $\bigwedge_{i=1..n} t_i = u_i \in E$.*
3. *$l(\succ \cup \rhd)^+ t_i$ and $l(\succ \cup \rhd)^+ u_i$ for each equation $l = r$ if $\bigwedge_{i=1..n} t_i = u_i \in E$.*
4. *$u \sim v$ for each equation $u = v \in B$*
5. *$\sim \circ \succ \subseteq \succ$.*

Lemma 2. *If an equational theory $\mathcal{E} = (\Sigma, E \uplus B)$ is* reductive modulo B*, then it is operational terminating modulo B.*

Proof. Note that a reductive theory is quasi-decreasing, and quasi-decreasingness is equivalent to operational termination [9]. □

Lemma 3 states that the equational subtheory of $\mathcal{E}^{\simeq}$ that forgets the equations in $\mathcal{E}$ is reductive. Note that $\mathcal{E}^{\mathrm{Bool}}$ unconditional and terminating modulo B^{Bool} and therefore is reductive. The following proof includes another verification of this fact.

Lemma 3. *The equational theory $\mathcal{E}' = ((\Sigma^{\simeq} \setminus \Sigma) \cup \Omega, (E^{\simeq} \setminus E) \uplus (B^{\simeq} \setminus B^{\Sigma \setminus \Omega}))$ is reductive.*

Proof. It is enough to prove that $\mathcal{E}'$ is reductive regardless of the sort information. The symetric, stable, and monotonic relation $\sim$ is witnessed by $=_{B^{\simeq} \setminus B^{\Sigma \setminus \Omega}}$. The $(B^{\simeq} \setminus B^{\Sigma \setminus \Omega})$-compatible simplification ordering is witnessed by $\succ$ [1], that can be obtained using an AC-RPO [16] with the following order precedence $>$ among symbols of the signature[4]:

$$
\begin{array}{llll}
\supset & > \sqcap & > \oplus & > \bot \\
\supset & > \lrcorner & > \top & \\
\supset & > \lrcorner & > \oplus & > \bot \\
\{f\} & > \bot & & \\
\{f\} & > \top & & \\
\{\mathrm{in}_f^k\} & > \_ \simeq \_ > \lrcorner & & > \top \\
\{\mathrm{in}_f^k\} & > \_ \simeq \_ > \lrcorner & & > \oplus > \bot \\
\{\mathrm{in}_f^k\} & > \_ \simeq \_ > \sqcup & & > \sqcap > \oplus > \bot \\
\{\mathrm{in}_f^k\} & > \_ \simeq \_ > \{\mathrm{root}_f^k\} & > \top &
\end{array}
$$

where $f \in \Omega$ and $\succeq \, = \succ \cup =_{B^{\simeq} \setminus B^{\Sigma \setminus \Omega}}$. It is routine to check by inspection on the equations $(E^{\simeq} \setminus E)$ that $\mathcal{E}'$ is reductive modulo $(B^{\simeq} \setminus B^{\Sigma \setminus \Omega})$. □

We consider the following logic $\mathcal{L}$ (we can assume all rewrite systems are 3-CTRS):

$$
(Refl)\ \frac{}{t \to^*_{E/B} u} \quad \text{where } t =_B u
$$

$$
(Tran)\ \frac{t \to_{E/B} v \quad v \to^*_{E/B} u}{t \to^*_{E/B} u}
$$

$$
(Cong)\ \frac{t_i \to_{E/B} u_i}{f(t_1, \ldots, t_i, \ldots, t_n) \to_{E/B} f(t_1, \ldots, u_i, \ldots, t_n)} \quad \text{where } f \in \Sigma \text{ and } 1 \leq i \leq \mathsf{ar}(f)
$$

$$
(Repl)\ \frac{t_1\sigma \to^*_{E/B} u_1\sigma \cdots t_m \to^*_{E/B} u_m}{t\sigma \to_{E/B} u\sigma} \quad \text{where } t \to u \text{ if } t_1 \to^*_{E/B} u_1 \cdots t_m \to^*_{E/B} u_m \in \overrightarrow{E} \text{ and } \sigma \text{ is well-sorted}
$$

First, we prove that if $(\Sigma, E \uplus B)$ and $((\Sigma^{\simeq} \setminus \Sigma) \cup \Omega, (E^{\simeq} \setminus E) \uplus (B^{\simeq} \setminus B^{\Sigma \setminus \Omega}))$ are operationally terminating then, the extended theories $(\Sigma^{\simeq}, E \uplus B^{\simeq})$ and $(\Sigma^{\simeq}, (E^{\simeq} \setminus E) \uplus B^{\simeq})$ are so too.

Lemma 4 establishes some good properties of structural axioms in B. Note that the relation $\to_{E/B}$ is equivalent to $=_B \circ \to_E \circ =_B$. Let $=^1_B$ denote the one step relation induced by $=_B$.

[4] this ordering can be obtained by existing automated tools for proving termination of rewriting modulo AC. Simplification orderings imply $\rhd \subseteq \succ$.

Lemma 4 (Property of Axioms). *Let $\mathcal{E} = (\Sigma, E \uplus B)$ be an equational theory where B is a union of associative, commutative, and associative-commutative axioms, $u = v, u' = v' \in B$ and $t_1, t_2, t_2', t_3 \in T_\Sigma(X)$. If $t_1 =^1_{u=v} t_2 =^1_{u'=v'} t_3$ and $\mathsf{root}(u) \neq \mathsf{root}(v)$ then there exists a term t_2' such that $t_1 =^1_{u'=v'} t_2' =^1_{u=v} t_3$, where $\mathsf{root}(u)$ and $\mathsf{root}(v)$ denote the root symbols from u and v, respectively.*

Proof. Consider that $\mathsf{root}(u) = f$ and $\mathsf{root}(u') = g$. We reason by case analysis on the positions p, q of $t_1 \overset{p}{=}^1_{u=v} t_2 \overset{q}{=}^1_{u'=v'} t_3$:

1. if $p > q$, then we have two possibilities:
   (a) $u = v$ is a commutativity axiom so that $t_1 = D[f(t_1^1, t_1^2)]$ and $t_2 = D[f(t_1^2, t_1^1)]$ for a (possibly empty) context D. Since $f \neq g$ then $t_1^1 =^1_{u'=v'} t_3^1$ or $t_1^2 =^1_{u'=v'} t_3^2$ and $t_3 = D[f(t_1^2, t_3^1)]$ in the first case or $D[f(t_3^2, t_1^1)]$ in the second case. Since axioms are linear and regular then t_1^1 and t_1^2 also appear in t_1 once, we can apply $=^1_{u'=v'}$ to t_1, obtaining $t_1 =^1_{u'=v'} t_2'$ and $t_2' = D[f(t_3^1, t_1^2)]$ or $t_2' = D[f(t_1^1, t_3^2)]$. We can apply then $=^1_{u'=v'}$ to t_2' obtaining $t_3 = D[f(t_1^2, t_3^1)]$ in the first case or $D[f(t_3^2, t_1^1)]$ in the second case, as desired.
   (b) $u = v$ is an associativity axiom so that $t_1 = D[f(t_1^1, f(t_1^2, t_1^3))]$ or $t_1 = D[f(f(t_1^1, t_1^2), t_1^3)]$ and $t_2 = D[f(f(t_1^1, t_1^2), t_1^3)]$ or $t_2 = D[f(t_1^1, f(t_1^2, t_1^3))]$ for a (possible empty) context D. Then, we can reason as in the previous case since axioms are linear and regular.
2. The case $q > p$ is entirely symetric to the case $p > q$.
3. if $p || q$ then $t_1 = D[t_1^1, t_1^2]$, $t_2 = D[t_3^1, t_1^2]$ and $t_3 = D[t_3^1, t_3^2]$ for a non-empty context D. Then, we can get $t_1 = D[t_1^1, t_1^2]$, $t_2' = D[t_1^1, t_3^2]$ and $t_3 = D[t_3^1, t_3^2]$.

□

Lemma 5 establishes properties for terms in $T_{\Sigma^{\simeq}}(X)$.

Lemma 5 (Properties of Terms in $\mathcal{E}^{\simeq}$). *Let $\mathcal{E} = (\Sigma, E \uplus B)$, $\Sigma = (S, \leq, F)$ and $s \in S$. If $\mathcal{E}$ is ground sort-decreasing and operationally terminating, then the following statements hold:*

1. $(\forall t, t' \in T_{\Sigma^{\simeq}}(X)_s)\ t \to_{E^{\simeq}/B^{\simeq}} t' \iff t \to_{E/B} t'$,
2. $(\forall t, t' \in T_{(\Sigma^{\simeq} \setminus \Sigma) \cup \Omega}(X)_{\mathrm{Bool}})\ t \to_{E^{\simeq}/B^{\simeq}} t' \iff t \to_{(E^{\simeq} \setminus E)/(B^{\simeq} \setminus B^{\Sigma \setminus \Omega})} t'$,
3. $(\forall t, t' \in T_{\Sigma^{\simeq}}(X)_{\mathrm{Bool}})$
   (a) $t \to_{E/B^{\simeq}} t' \iff (\exists t_1 \in T_{\Sigma^{\simeq}}(X)_{\mathrm{Bool}})\, t \to_{E/B} t_1$ *and* $t_1 =_{B^{\simeq} \setminus B} t'$,
   (b) $(t \to_{(E^{\simeq} \setminus E)/B^{\simeq}} t' \iff (\exists t_1, t_2 \in T_{\Sigma^{\simeq}}(X)_{\mathrm{Bool}})\, t =_B t_1 \to_{(E^{\simeq} \setminus E)/(B^{\simeq} \setminus B^{\Sigma \setminus \Omega})} t_2 =_B t'$.

Proof. 1. If $t \in T_{\Sigma^{\simeq}}(X)_s$, it is trivial to prove by structural induction that $t \in T_\Sigma(X)_s$. Since $t \in T_\Sigma(X)_s$ this means that each $B^{\simeq}$ axiom applied belongs to B and the applied equation in $E^{\simeq}$ belongs to E. Hence, $t \to_{E/B} t'$.

2. If $t \in T_{(\Sigma^{\simeq} \setminus \Sigma) \cup \Omega}(X)_{\mathrm{Bool}}$, we can only apply axioms from $B^{\simeq} \setminus B^{\Sigma \setminus \Omega}$ and equation from $E^{\simeq} \setminus E$. Hence, $t \to_{(E^{\simeq} \setminus E)/(B^{\simeq} \setminus B^{\Sigma \setminus \Omega})} t'$.

3. For any well-defined term $t \in T_{\Sigma^{\simeq}}(X)_{\mathrm{Bool}}$, $t = D[t_1^1, \cdots, t_1^n]$ where D is a context such that $D \in T_{(\Sigma^{\simeq} \setminus \Sigma) \uplus \uplus \{\Box\}}(X)_{\mathrm{Bool}}$ and $t_1^i \in T_\Sigma(X)_{s_i}$.

(a) By multiple applications of Lemma 4, we have $t =_B t'_1 =_{B^{\simeq} \setminus B} \circ \to_E t'_2 =_B \circ =_{B^{\simeq} \setminus B} t'$. Consider the sequence $u_1 =^1_{B^{\simeq} \setminus B} u_2 \to_E u_3$, where $u_1 = D[u^1_1, \cdots, u^n_1]$, $D \in T_{(\Sigma^{\simeq} \setminus \Sigma) \uplus \{\Box\}}(X)_{\mathrm{Bool}}$ and $u^i_1 \in T_\Sigma(X)_{s_i}$. Since each axiom in $B^{\simeq} \setminus B$ is linear, regular and sort preserving, we get $D[u^1_1, \cdots, u^i_1, \cdots, u^n_1] =^1_{B^{\simeq} \setminus B} D'[u^1_1, \cdots, u^i_1, \cdots, u^n_1] \to_E D'[u^1_1, \cdots, u^i_2, \cdots, u^n_1]$. Therefore, we can change the order of application of the rule and the axiom obtaining $D[u^1_1, \cdots, u^i_1, \cdots, u^n_1] \to_E D[u^1_1, \cdots, u^i_2, \cdots, u^n_1] =^1_{B^{\simeq} \setminus B} D'[u^1_1, \cdots, u^i_2, \cdots, u^n_1]$. By multiple applications of this result and Lemma 4 to $t =_B t'_1 =_{B^{\simeq} \setminus B} \circ \to_E t'_2 =_B \circ =_{B^{\simeq} \setminus B} t'$, we get $t =_B \circ \to_E \circ =_B t_1 =_{B^{\simeq} \setminus B} t'$, that is, $t \to_{E/B} t_1 =_{B^{\simeq} \setminus B} t'$.

(b) By multiple applications of Lemma 4, we have $t =_B t_1 =_{(B^{\simeq} \setminus B^{\Sigma \setminus \Omega})} \circ \to_{E^{\simeq} \setminus E} \circ =_{(B^{\simeq} \setminus B^{\Sigma \setminus \Omega})} t_2 =_B t'$.

□

We assume that operational termination of $(\Sigma, E \uplus B)$ is Σ-extensible, i.e., if $(\Sigma, E \uplus B)$ is operationally terminating then $(\Sigma \cup \Delta, E \uplus B)$ is so too.

Lemma 6. *Let $(\Sigma, E \uplus B)$ be ground sort-decreasing, ground confluent and operationally terminating, then $(\Sigma^{\simeq}, E \uplus B^{\simeq})$ is operationally terminating and ground confluent.*

Proof. By contradiction, consider that there is an infinite well-formed proof tree for $t \to^*_{E/B^{\simeq}} u$ or $t \to^*_{E/B^{\simeq}} u$ with $t, u \in T_{\Sigma^{\simeq}}$.

1. It cannot be a well-formed proof tree of the form:

$$\frac{}{t \to^*_{E/B^{\simeq}} u}$$

obtained using $(Refl)$, since this proof tree is finite.

2. If the well-formed proof tree is of the form:

$$\frac{t_1\sigma \to^*_{E/B^{\simeq}} u_1\sigma \cdots t_m\sigma \to^*_{E/B^{\simeq}} u_m\sigma}{t\sigma \to_{E/B^{\simeq}} u\sigma}$$

we know that $t_i, u_i \in T_\Sigma(X)$ and $\sigma : X \mapsto T_\Sigma$. Therefore, we have:

$$\frac{t_1\sigma \to^*_{E/B} u_1\sigma \cdots t_m\sigma \to^*_{E/B} u_m\sigma}{t\sigma \to_{E/B^{\simeq}} u\sigma}$$

and every well-formed proof tree $t_i\sigma \to^*_{E/B} u_i\sigma$ is finite since $(\Sigma, E \uplus B)$ is operationally terminating. Hence, the well-formed proof tree is finite.

3. If the well-formed proof tree is of the form (let $t = f(t_1, \ldots, t_i, \ldots, t_n)$ and $u = f(t_1, \ldots, u_i, \ldots, t_n)$):

$$\frac{t_i \to_{E/B^{\simeq}} u_i}{f(t_1, \ldots, t_i, \ldots, t_n) \to_{E/B^{\simeq}} f(t_1, \ldots, u_i, \ldots, t_n)}$$

we have to consider two cases:

(a) If $t_i \to_{E/B} u_i$ is of the form presented in Item 2, the well-formed proof tree is finite.
(b) If $t_i \to_{E/B} u_i$ is of the form presented in Item 3, then $f(t_1, \ldots, t_i, \ldots, t_n) \rhd t_i$.

Hence, recursively, either we arrive at a subtree of the form presented in Item 2 or we have an infinite sequence $f(t_1, \ldots, t_i, \ldots) \rhd t_i \rhd \cdots$, leading to a contradiction with the well-foundedness of $\rhd$ on finite terms.

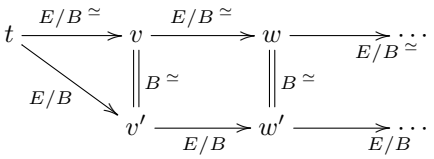
4. If the well-formed proof tree is of the form:

$$\frac{t \to_{E/B^{\simeq}} v \quad v \to^*_{E/B^{\simeq}} u}{t \to^*_{E/B^{\simeq}} u}$$

we have to prove that both branches are finite. The left branch only fits with Item 2 and Item 3, therefore the well-formed proof tree for $t \to_{E/B^{\simeq}} v$ is finite. Hence, if the well-formed proof tree is infinite, the unique possibility is an infinite application of Item 4 on the right branch, getting an infinite sequence:

$$t \to_{E/B^{\simeq}} v \to_{E/B^{\simeq}} w \to_{E/B^{\simeq}} \cdots$$

By applying recursively Lemma 5(3a) on the sequence, we get:



obtaining an infinite sequence over $\to_{E/B}$, which is a contradiction with the operational termination of $(\Sigma^{\simeq}, E \uplus B)$.
Local confluence is straightforward since all terms in E do not involve any of the new symbols in $B^{\simeq} \setminus B$ and therefore no new critial pairs appear.
□

Lemma 7. *Let* $((\Sigma^{\simeq} \setminus \Sigma) \cup \Omega, (E^{\simeq} \setminus E) \uplus (B^{\simeq} \setminus B^{\Sigma \setminus \Omega}))$ *be operationally terminating, then* $(\Sigma^{\simeq}, (E^{\simeq} \setminus E) \uplus B^{\simeq})$ *is operationally terminating.*

Proof. By Lemma 3, since AC-RPO proofs are Σ-extensible for AC-symbols. □

Now, we can prove the main theorem.

Theorem 2. *If* $\mathcal{E}$ *is ground sort-decreasing, ground confluent and operationally terminating, then* $\mathcal{E}^{\simeq}$ *is ground operationally terminating.*

Proof. Consider the following relation R, such that $t \; R \; u$ if:

$$\begin{array}{lll} t & \Rightarrow & u \\ t & \rhd & u \\ t & \to_{E/B^{\simeq}} & u \end{array}$$

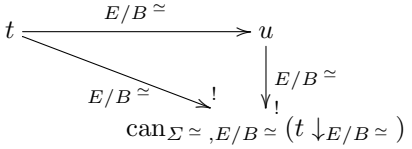
where we define $t \Rightarrow u$ if there is an oriented equation $l \to r$ if $v_1 \to_{E^{\simeq}/B^{\simeq}} w_1 \cdots v_n \to_{E^{\simeq}/B^{\simeq}} w_n \in \overrightarrow{(E^{\simeq} \setminus E)}$ and a substitution σ such that $t =_{B^{\simeq}} l\sigma$, and either $u = r\sigma$ or $u =_{B^{\simeq}} u_j\sigma$, where $1 \leq j \leq n$. We know that $\succ_1 = \to_{E/B^{\simeq}}$ is a well-founded ordering by Lemma 6 and $\rhd \subseteq \succ_2$ and $\Rightarrow \subseteq \succ_2$ by the *reductive* ordering obtained by Lemma 7. Therefore, we have that if $t \; R \; u$ then $t \succ_2 u$ or $t \succ_1 u$.

We prove that R is noetherian using the following result: if $t \; R \; u$ then $\mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(t \downarrow_{E/B^{\simeq}}) = \mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(u \downarrow_{E/B^{\simeq}})$ if $t \to_{E/B^{\simeq}} u$, and $\mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(t \downarrow_{E/B^{\simeq}}) \succ_2 \mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(u \downarrow_{E/B^{\simeq}})$, otherwise. We proceed by cases on a step $t \; R \; u$:

1. If $t \to_{E/B^{\simeq}} u$, then

$$\mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(t \downarrow_{E/B^{\simeq}}) = \mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(u \downarrow_{E/B^{\simeq}})$$

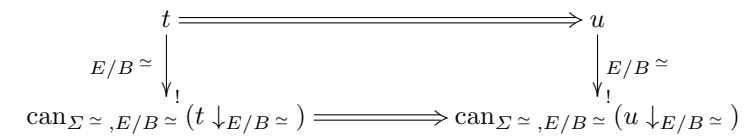
because $(\Sigma^{\simeq}, E \uplus B^{\simeq})$ is ground confluent and operationally terminating. We get the following schema:



2. If $t \Rightarrow u$, we know:
   (a) $t = D[t_1, \ldots, t_n]$ where $D \in T_{(\Sigma^{\simeq} \setminus \Sigma) \uplus \Omega \uplus \{\Box\}}(X)_{\mathrm{Bool}}$ and $\mathsf{root}(t_i) \in \Sigma \setminus \Omega$,
   (b) the redex $l \in T_{(\Sigma^{\simeq} \setminus \Sigma) \uplus \Omega}(X)_{\mathrm{Bool}}$, where $l \to r$ if $v_1 \to_{E^{\simeq}/B^{\simeq}} w_1 \cdots v_n \to_{E^{\simeq}/B^{\simeq}} w_n \in \overrightarrow{E^{\simeq} \setminus E}$ matches with a subterm in D,
   (c) $t = D[t_1, \ldots, t_m] =_{B^{\simeq}} l\sigma$ and either $u = r\sigma$ or $u = v_j\sigma$, where $u = D'[u_1, \ldots, u_{m'}]$, $1 \leq j \leq n$, $u_i =_B v \in \{t_1, \ldots, t_n\}$, $1 \leq i \leq m'$, and $D' \in T_{(\Sigma^{\simeq} \setminus \Sigma) \uplus \Omega \uplus \{\Box\}}(X)_{\mathrm{Bool}}$.

   Therefore,
   (a) $\mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(t \downarrow_{E/B^{\simeq}}) = \mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(D[t_1 \downarrow_{E/B^{\simeq}}, \ldots, t_m \downarrow_{E/B^{\simeq}}])$; and
   (b) $\mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(u \downarrow_{E/B^{\simeq}}) = \mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(D'[u_1 \downarrow_{E/B^{\simeq}}, \ldots, u_{m'} \downarrow_{E/B^{\simeq}}])$.

   We get the following schema:



3. If $t \rhd u$, we know:
   (a) $t = D[t_1, \ldots, t_n]$ where $D \in T_{(\Sigma^{\simeq} \setminus \Sigma) \uplus \Omega \uplus \{\Box\}}(X)_{\mathrm{Bool}}$ and $\mathsf{root}(t_i) \in \Sigma \setminus \Omega$,
   (b) either $u = D'[t_1, \ldots, t_n]$ and $D[t_1, \ldots, t_n] \rhd D'[t_1, \ldots, t_n]$ or $t_i \trianglerighteq u$ for some $1 \leq i \leq n$ (note that in the second case $u \in T_\Sigma$ and the term is operationally terminating by Lemma 5(1)).

Therefore, either

(a) $\mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(t\downarrow_{E/B^{\simeq}}) = \mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(D[t_1\downarrow_{E/B^{\simeq}},\ldots,t_n\downarrow_{E/B^{\simeq}}])$, and either
   i. $\mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(u\downarrow_{E/B^{\simeq}}) = \mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(D'[t_1\downarrow_{E/B^{\simeq}},\ldots,t_n\downarrow_{E/B^{\simeq}}])$ if $u = D'[t_1\downarrow_{E/B^{\simeq}},\ldots,t_n\downarrow_{E/B^{\simeq}}]$, or
   ii. $\mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(u\downarrow_{E/B^{\simeq}})$ if $t_i \trianglerighteq u$.

We get the following schema:

$$\begin{array}{ccc} t & \rhd & u \\ {\scriptstyle E/B^{\simeq}}\big\downarrow_{!} & & \big\downarrow_{!}{\scriptstyle E/B^{\simeq}} \\ \mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(t\downarrow_{E/B^{\simeq}}) & \rhd & \mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(u\downarrow_{E/B^{\simeq}}) \end{array}$$

By contradiction, if R is not noetherian, without loss of generality we can construct an infinite sequence of the form:

$$t_1 \succ_1^* t_2 \succ_2 t_3 \succ_1^* t_4 \succ_2 \cdots$$

and, by applying the previous result, we obtain an infinite sequence of the form:

$$\mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(t_1\downarrow_{E/B^{\simeq}}) \succ_2 \mathrm{can}_{\Sigma^{\simeq},E/B^{\simeq}}(t_3\downarrow_{E/B^{\simeq}}) \succ_2 \cdots$$

leading to a contradiction with the well-foundedness of $\succ_2$.

Now, we prove that $\mathcal{E}^{\simeq}$ is ground operationally terminating by contradiction. We assume that there is an infinite well-formed proof for $t \to_{E^{\simeq}/B^{\simeq}} u$ or $t \to^*_{E^{\simeq}/B^{\simeq}} u$ with $t, u \in T_{\Sigma^{\simeq}}$. We choose among all ground terms, a term t which is *minimal* in the R relation with the property of having the left-hand side at the root of an infinite well-formed proof tree. Such a t exists by the non-operational termination assumption and R being noetherian. We now reason by cases to reach a contradiction:

- if $t \in T_{\Sigma^{\simeq},s}$ and $s \in S$ then $t \in T_{\Sigma,s}$ and by Lemma 6 no such infinite well-formed proof tree can exist;
- if $t \in T_{(\Sigma^{\simeq}\setminus\Sigma)\cup\Omega,\mathrm{Bool}}$, by Lemma 7 no such infinite well-formed proof tree exist;
- otherwise, $t \in T_{\Sigma^{\simeq},\mathrm{Bool}}$ and its only possible shape is $t = D[t^1_{s_1},\cdots,t^n_{s_n}]$ where D is a context such that $D \in T_{(\Sigma^{\simeq}\setminus\Sigma)\uplus\Omega\uplus\{\Box\},\mathrm{Bool}}$ and each $t^i_{s_i} \in T_{\Sigma,s_i}$, $s_i \in S$, and $\mathsf{root}(t^i_{s_i}) \in \Sigma\setminus\Omega$. If the root of the infinite well-formed proof tree is of the form $t \to_{E^{\simeq}/B^{\simeq}} u$, then it cannot be an *unconditional replacement* step, so it must be either a *congruence* step or a *conditional replacement* step. For a *congruence* step we have $t = f(t_1,\ldots,t_i,\ldots,t_n)$, $u = f(t_1,\ldots,t'_i,\ldots,t_n)$ and there is an infinite well-formed proof tree rooted at $t_i \to_{E^{\simeq}/B^{\simeq}} t'_i$, which is impossible by the minimality of t and $t\ R\ t_i$. The only remaining case is a *conditional replacement* step, with a rule of the form $l \to r$ if $v_1 \to_{E^{\simeq}/B^{\simeq}} w_1 \cdots v_n \to_{E^{\simeq}/B^{\simeq}} w_n \in \overrightarrow{E^{\simeq}\setminus E}$ (if $l \to r$ if $v_1 \to_{E^{\simeq}/B^{\simeq}} w_1 \cdots v_n \to_{E^{\simeq}/B^{\simeq}} w_n \in \overrightarrow{E}$, there is no infinite well-formed proof tree rooted at $t \to_{E/B^{\simeq}} u$ since every $v_i\sigma \in T_\Sigma$), so that

there is an infinite well-formed proof tree rooted at $v_i\sigma \rightarrow_{E^{\simeq}/B^{\simeq}} w_i$ for σ the matching substitution. This is again imposible by the minimality of t, since $t\ R\ v_i\sigma$. If the infinite well-formed proof tree has a root of the form $t \rightarrow^*_{E^{\simeq}/B^{\simeq}} u$, it cannot be a *reflexive* step, so it must be *transitivity* step. We also have a well-formed proof tree t rooted at $t \rightarrow_{E^{\simeq}/B^{\simeq}} v$ with t an R-minimal left-hand side of an infinite well-formed proof tree. We have already shown that no infinite well-formed proof tree with root $t \rightarrow_{E^{\simeq}/B^{\simeq}} v$ exists. Therefore, there must be an infinite well-formed proof tree rooted at $v \rightarrow^*_{E^{\simeq}/B^{\simeq}} u$, but this is impossible, since $t\ R\ v$ and t is R-minimal.

□

5.3 Preservation of Ground Confluence

Recall from Section 2 that the equational theory $\mathcal{E} = (\Sigma, E \uplus B)$ is ground confluent modulo B iff for all terms $t, t', t'' \in T_\Sigma$, such that $t \rightarrow^*_{E/B} t'$ and $t \rightarrow^*_{E/B} t''$, there is $u \in T_\Sigma$ such that $t' \rightarrow^*_{E/B} u$ and $t'' \rightarrow^*_{E/B} u$. If $\mathcal{E}$ is operationally terminating, then it is enough to prove $\mathcal{E}$ ground locally confluent [5]. Namely, that for all terms $t, t', t'' \in T_\Sigma$, if $t \rightarrow_{E/B} t'$ and $t \rightarrow_{E/B} t''$, then there is $u \in T_\Sigma$ such that $t' \rightarrow^*_{E/B} u$ and $t'' \rightarrow^*_{E/B} u$.

Ground local confluence can be established via ground joinability of the so-called conditional critical pairs.

Definition 8 (Conditional Critical Pair). *Given $(\Sigma, E \uplus B)$ with Σ preregular, B sort-preserving and with $\overrightarrow{E}$ B-coherent, and given oriented conditional equations $l \rightarrow r$ if $C, l' \rightarrow r'$ if $C' \in \overrightarrow{E}$ such that $(\mathcal{V}ar(l) \cup \mathcal{V}ar(r) \cup \mathcal{V}ar(C)) \cap (\mathcal{V}ar(l') \cup \mathcal{V}ar(r') \cup \mathcal{V}ar(C')) = \varnothing$ and $l|_p\sigma =_B l'\sigma$, for some nonvariable position $p \in \mathcal{P}os(l)$ and B-unifier σ of $l|_p$ and l', then the triple*

$$C\sigma \wedge C'\sigma \Rightarrow l\sigma[r'\sigma]_p = r\sigma$$

is called a (conditional) critical pair.

Theorem 3. *If $\mathcal{E}$ is ground sort-decreasing, operationally terminating, ground confluent, then $\mathcal{E}^{\simeq}$ is ground confluent.*

Proof. First of all note that $\mathcal{E}^{\mathrm{Bool}}$ has been chosen to be confluent, sort-decreasing and operational terminating modulo B^{Bool}. Note also that $\mathcal{E}^{\simeq}$ is ground sort-decreasing by Theorem 1 and operationally terminating by Theorem 2. Hence, it is enough to prove that $\mathcal{E}^{\simeq}$ is locally ground confluent. Note that if $f \in \Omega$, then any equation $f(t_1, \ldots, t_n) = u$ if $C \in E$ is such that $f(t_1\theta, \ldots, t_n\theta) \notin T_{\Omega,s}$ for any $f : s_1 \ldots s_n \rightarrow s$ where $f \in \Omega$ and ground substitution θ satisfying $t_1\theta \in T_{\Omega,s_1}, \ldots t_n\theta \in T_{\Omega,s_n}$, since otherwise $\Omega \subseteq \Sigma$ would not be a subsignature of free constructors modulo B for $\mathcal{E}$ (e.g., as in examples 2 and 3). Therefore, the set of conditional critical pairs of $\mathcal{E}^{\simeq}$ is the union of the conditional critical pairs of the theories $\mathcal{E}$, $\mathcal{E}^{\mathrm{Bool}}$ and the theory with the rest of rules in $\mathcal{E}^{\simeq}$ that are not in $\mathcal{E}$ and $\mathcal{E}^{\mathrm{Bool}}$ in isolation. That is, the set of conditional critical pairs of $\mathcal{E}^{\simeq}$ consists of

- the conditional critical pairs of E, which are ground joinable by assumption
- the critical pairs of E^{Bool}, which are joinable by the choice of $\mathcal{E}^{\mathrm{Bool}}$, and
- the conditional critical pairs of $E^{\simeq} \setminus (E \cup E^{\mathrm{Bool}})$.

For the latter set of oriented equations the proof proceeds by case analysis on the structural axioms of the constructor symbols in Ω. Throughout the whole case analysis we need to worry about *possibly different maximal typings* of a constructor f, i.e., $f : s_1 \cdots s_n \to s$ and $f : s'_1 \cdots s'_n \to s'$.

- For the oriented equations defining $\_ \simeq \_$, if $f \in \Omega$ is an absolutely free symbol:
  1. for $x_{k_1} \simeq x_{k_1} \to \top$ and $f(x^1_{s_{1_2}}, \ldots, x^n_{s_{n_2}}) \simeq g(y^1_{s'_{1_2}}, \ldots, y^n_{s'_{n_2}}) \to \bot$ do not yield critical pairs;
  2. for $x_{k_1} \simeq x_{k_1} \to \top$ and $f(x^1_{s_{1_2}}, \ldots, x^n_{s_{n_2}}) \simeq x^i_{s_{i_2}} \to \bot$ do not yield critical pairs;
  3. for $f(x^1_{s_{1_1}}, \ldots, x^n_{s_{n_1}}) \simeq x^i_{s_{i_1}} \to \bot$ and $f(x^1_{s_{1_2}}, \ldots, x^n_{s_{n_2}}) \simeq g(y^1_{s'_{1_2}}, \ldots, y^m_{s'_{m_2}}) \to \bot$, for any $B^{\simeq}$-unifier σ we obtain the trivial critical pair $< \bot, \bot >$;
  4. for $f(x^1_{s_{1_1}}, \ldots, x^n_{s_{n_1}}) \simeq f(y^1_{s_{1_1}}, \ldots, y^n_{s_{n_1}}) \to \prod_{1 \le i \le n} x^i_{s_{i_1}} \simeq y^i_{s_{i_1}}$ and $x_{k_2} \simeq x_{k_2} \to \top$ we obtain the joinable critical pair $< \prod_{1 \le i \le n} z^i_{s_{i_3}} \simeq z^i_{s_{i_3}}, \top >$ from the $B^{\simeq}$-unifier $\sigma(x^i_{s_{i_1}}) = \sigma(y^i_{s_{i_1}}) = z^i_{s_{i_3}}$ and $\sigma(x_{k_2}) = f(z^1_{s_{1_3}}, \ldots, z^n_{s_{n_3}})$;
  5. for $f(x^1_{s_{1_1}}, \ldots, x^n_{s_{n_1}}) \simeq f(y^1_{s_{1_1}}, \ldots, y^n_{s_{n_1}}) \to \prod_{1 \le i \le n} x^i_{s_{i_1}} \simeq y^i_{s_{i_1}}$ and $f(x^1_{s_{1_2}}, \ldots, x^n_{s_{n_2}}) \simeq x^i_{s_{i_2}} \to \bot$ we obtain the critical pairs:
     (a) $< \prod_{1 \le j \le n, j \ne i} w^i_{s'_{i_3}} \simeq z^i_{s_{i_3}} \sqcap (f(z^1_{s_{1_3}}, \ldots, z^n_{s_{n_3}}) \simeq z^i_{s_{i_3}}), \bot >$ from the $B^{\simeq}$-unifiers satisfying $\sigma(x^i_{s_{i_1}}) = \sigma(x^i_{s_{i_2}}) = f(z^1_{s_{1_3}}, \ldots, z^n_{s_{n_3}})$, $\sigma(x^j_{s_{j_1}}) = \sigma(x^j_{s_{j_2}}) = w^j_{s'_{j_3}}$ for $j \ne i$ and $\sigma(y^i_{s_{i_1}}) = z^i_{s_{i_3}}$. By applying the rule $f(x^1_{s_{1_4}}, \ldots, x^n_{s_{n_4}}) \simeq x^i_{s_{i_4}} \to \bot$ to $f(z^1_{s_{1_3}}, \ldots, z^n_{s_{n_3}}) \simeq z^i_{s_{i_3}}$, the critical pair is joinable;
     (b) $< \prod_{1 \le j \le n, j \ne i} z^i_{s_{i_3}} \simeq w^i_{s'_{i_3}} \sqcap (z^i_{s_{i_3}} \simeq f(z^1_{s_{1_3}}, \ldots, z^n_{s_{n_3}})), \bot >$ from the $B^{\simeq}$-unifiers satisfying $\sigma(y^i_{s_{i_1}}) = \sigma(x^i_{s_{i_2}}) = f(z^1_{s_{1_3}}, \ldots, z^n_{s_{n_3}})$, $\sigma(y^j_{s_{j_1}}) = \sigma(x^j_{s_{j_2}}) = w^j_{s_{j_3}}$ for $j \ne i$ and $\sigma(x^i_{s_{i_1}}) = z^i_{s_{i_3}}$. By applying the rule $f(x^1_{s_{1_4}}, \ldots, x^n_{s_{n_4}}) \simeq x^i_{s_{i_4}} \to \bot$ to $f(z^1_{s_{1_3}}, \ldots, z^n_{s_{n_3}}) \simeq z^i_{s_{i_3}}$, the critical pair is joinable.
- For the oriented equations defining $\_ \simeq \_$, if $f \in \Omega$ is a C-symbol:
  1. for $x_{k_1} \simeq x_{k_1} \to \top$ and $f(x^1_{s_{1_2}}, x^2_{s_{2_2}}) \simeq g(y^1_{s'_{1_2}}, \ldots, y^m_{s'_{m_2}}) \to \bot$ do not yield critical pairs;
  2. for $x_{k_1} \simeq x_{k_1} \to \top$ and $f(x^1_{s_2}, x^1_{s_2}) \simeq x^1_{s_2} \to \bot$ do not yield critical pairs;

3. for $f(x^1_{s_1}, x^2_{s_1}) \simeq x^1_{s_1} \to \bot$ and $f(x^1_{s_2}, x^2_{s_2}) \simeq g(y^1_{s_{1_2}}, \ldots, y^m_{s_{m_2}}) \to \bot$, for any $B^{\simeq}$-unifier σ we obtain the trivial critical pair $< \bot, \bot >$;
4. for $f(x^1_{s_1}, x^2_{s_1}) \simeq f(y^1_{s_1}, y^2_{s_1}) \to (x^1_{s_1} \simeq y^1_{s_1} \sqcap x^2_{s_1} \simeq y^2_{s_1}) \sqcup (x^1_{s_1} \simeq y^2_{s_1} \sqcap x^2_{s_1} \simeq y^1_{s_1})$ and $x_{k_2} \simeq x_{k_2} \to \top$ we have the $B^{\simeq}$-unifiers:
   (a) $\sigma(x^i_{s_1}) = \sigma(y^i_{s_1}) = z^i_{s_3}$ and $\sigma(x_{k_2}) = f(z^2_{s_3}, z^1_{s_3})$, obtaining the joinable critical pair:
   $$< (z^1_{s_3} \simeq z^1_{s_3} \sqcap z^2_{s_3} \simeq z^2_{s_3}) \sqcup (z^1_{s_3} \simeq z^2_{s_3} \sqcap z^2_{s_3} \simeq z^1_{s_3}), \top >,$$
   (b) and $\sigma(x^1_{s_1}) = \sigma(y^2_{s_1}) = z^1_{s_3}$, $\sigma(x^2_{s_1}) = \sigma(y^1_{s_1}) = z^2_{s_3}$ and $\sigma(x_{k_2}) = f(z^2_{s_3}, z^1_{s_3})$, obtaining the joinable critical pair:
   $$< (z^1_{s_3} \simeq z^2_{s_3} \sqcap z^2_{s_3} \simeq z^1_{s_3}) \sqcup (z^1_{s_3} \simeq z^1_{s_3} \sqcap z^2_{s_3} \simeq z^2_{s_3}), \top >;$$
5. for $f(x^1_{s_1}, x^2_{s_1}) \simeq x^1_{s_1} \to \bot$ and $f(x^1_{s_2}, x^2_{s_2}) \simeq x^1_{s_2} \to \bot$, for any $B^{\simeq}$-unifier σ we obtain the trivial critical pair $< \bot, \bot >$;
6. for $f(x^1_{s_1}, x^2_{s_1}) \simeq f(y^1_{s_1}, y^2_{s_1}) \to (x^1_{s_1} \simeq y^1_{s_1} \sqcap x^2_{s_1} \simeq y^2_{s_1}) \sqcup (x^1_{s_1} \simeq y^2_{s_1} \sqcap x^2_{s_1} \simeq y^1_{s_1})$ and $f(x^1_{s_2}, x^2_{s_2}) \simeq x^1_{s_2} \to \bot$ we obtain the critical pairs:
   (a) $< (f(z^1_{s_3}, z^2_{s_3}) \simeq z^1_{s_3} \sqcap w_{s_4} \simeq z^2_{s_3}) \sqcup (f(z^1_{s_3}, z^2_{s_3}) \simeq z^2_{s_3} \sqcap w_{s_4} \simeq z^1_{s_3}), \bot >$ from the $B^{\simeq}$-unifier σ which must satisfy $\sigma(x^1_{s_1}) = \sigma(x^1_{s_2}) = f(z^1_{s_{1_3}}, z^2_{s_{2_3}})$, $\sigma(x^2_{s_1}) = \sigma(x^2_{s_2}) = w_{s_4}$ and $\sigma(y^i_{s_{i_1}}) = z^i_{s_{i_3}}$. By applying the rule $f(x^1_{s_{1_5}}, x^2_{s_{1_5}}) \simeq x^1_{s_{1_5}} \to \bot$ to $f(z^1_{s_{1_3}}, z^2_{s_{1_3}}) \simeq z^i_{s_{i_3}}$, the critical pair is joinable,
   (b) $< (w_{s_4} \simeq z^1_{s_3} \sqcap f(z^1_{s_3}, z^2_{s_3}) \simeq z^2_{s_3}) \sqcup (w^1_{s_4} \simeq z^2_{s_3} \sqcap f(z^1_{s_3}, z^2_{s_3}) \simeq z^1_{s_3}), \bot >$ from the $B^{\simeq}$-unifier σ which must satisfy $\sigma(x^2_{s_1}) = \sigma(x^1_{s_2}) = f(z^1_{s_3}, z^2_{s_3})$, $\sigma(x^1_{s_1}) = \sigma(x^2_{s_2}) = w_{s_4}$ and $\sigma(y^i_{s_1}) = z^i_{s_3}$. By applying the rule $f(x^1_{s_5}, x^2_{s_5}) \simeq x^1_{s_5} \to \bot$ to $f(z^1_{s_3}, z^2_{s_3}) \simeq z^i_{s_3}$, the critical pair is joinable,
   (c) $< (z^1_{s_3} \simeq f(z^1_{s_3}, z^2_{s_3}) \sqcap z^2_{s_3} \simeq w_{s_4}) \sqcup (z^2_{s_3} \simeq f(z^1_{s_3}, z^2_{s_3}) \sqcap z^1_{s_3} \simeq w_{s_4}), \bot >$ from the $B^{\simeq}$-unifier σ which must satisfy $\sigma(y^1_{s_1}) = \sigma(x^1_{s_2}) = f(z^1_{s_3}, z^2_{s_3})$, $\sigma(y^2_{s_1}) = \sigma(x^2_{s_2}) = w_{s_4}$ and $\sigma(x^1_{s_1}) = z^1_{s_3}$. By applying the rule $f(x^1_{s_{1_5}}, x^2_{s_{1_5}}) \simeq x^1_{s_{1_5}} \to \bot$ to $f(z^1_{s_3}, z^2_{s_3}) \simeq z^1_{s_3}$, the critical pair is joinable,
   (d) $< (z^1_{s_3} \simeq w_{s_4} \sqcap z^2_{s_3} \simeq f(z^1_{s_3}, z^2_{s_3})) \sqcup (z^2_{s_3} \simeq w_{s_4} \sqcap z^1_{s_3} \simeq f(z^1_{s_3}, z^2_{s_3})), \bot >$ from the $B^{\simeq}$-unifier σ which must satisfy $\sigma(y^2_{s_1}) = \sigma(x^1_{s_2}) = f(z^1_{s_3}, z^2_{s_3})$, $\sigma(y^1_{s_1}) = \sigma(x^2_{s_2}) = w_{s_4}$ and $\sigma(x^i_{s_1}) = z^i_{s_3}$. By applying the rule $f(x^1_{s_{1_5}}, x^2_{s_{1_5}}) \simeq x^1_{s_{1_5}} \to \bot$ to $f(z^1_{s_3}, z^2_{s_3}) \simeq z^i_{s_3}$, the critical pair is joinable;
7. for $f(x^1_{s_1}, x^2_{s_1}) \simeq f(y^1_{s_1}, y^2_{s_1}) \to (x^1_{s_1} \simeq y^1_{s_1} \sqcap x^2_{s_1} \simeq y^2_{s_1}) \sqcup (x^1_{s_1} \simeq y^2_{s_1} \sqcap x^2_{s_1} \simeq y^1_{s_1})$ and $f(x^1_{s_2}, x^2_{s_2}) \simeq f(y^1_{s_2}, y^2_{s_2}) \to (x^1_{s_2} \simeq y^1_{s_2} \sqcap x^2_{s_2} \simeq y^2_{s_2}) \sqcup (x^1_{s_2} \simeq y^2_{s_2} \sqcap x^2_{s_2} \simeq y^1_{s_2})$ we obtain the joinable critical pairs:
   (a) $< (w^1_{s_4} \simeq z^1_{s_3} \sqcap w^2_{s_4} \simeq z^2_{s_3}) \sqcup (z^1_{s_3} \simeq w^2_{s_4} \sqcap w^2_{s_4} \simeq z^1_{s_3}), (z^1_{s_3} \simeq w^1_{s_4} \sqcap z^2_{s_3} \simeq w^2_{s_4}) \sqcup (z^1_{s_3} \simeq w^2_{s_4} \sqcap z^2_{s_3} \simeq w^1_{s_4}) >$ from the $B^{\simeq}$-unifier σ which must satisfy $\sigma(x^1_{s_1}) = \sigma(y^1_{s_2}) = w^1_{s_4}$, $\sigma(x^2_{s_1}) = \sigma(y^2_{s_2}) = w^2_{s_4}$, $\sigma(y^1_{s_1}) = \sigma(x^1_{s_2}) = z^1_{s_3}$, and $\sigma(y^2_{s_1}) = \sigma(x^2_{s_2}) = z^2_{s_3}$,
   (b) $< (w^1_{s_4} \simeq z^1_{s_3} \sqcap w^2_{s_4} \simeq z^2_{s_3}) \sqcup (z^1_{s_3} \simeq w^2_{s_4} \sqcap w^2_{s_4} \simeq z^1_{s_3}), (z^2_{s_3} \simeq w^1_{s_4} \sqcap z^1_{s_3} \simeq w^2_{s_4}) \sqcup (z^2_{s_3} \simeq w^2_{s_4} \sqcap z^1_{s_3} \simeq w^1_{s_4}) >$ from the $B^{\simeq}$-unifier σ which

must satisfy $\sigma(x^1_{s_1}) = \sigma(y^1_{s_2}) = w^1_{s_4}$, $\sigma(x^2_{s_1}) = \sigma(y^2_{s_2}) = w^2_{s_4}$, $\sigma(y^1_{s_1}) = \sigma(x^2_{s_2}) = z^1_{s_3}$, and $\sigma(y^2_{s_1}) = \sigma(x^1_{s_2}) = z^2_{s_3}$,

(c) $< (w^1_{s_4} \simeq z^1_{s_3} \sqcap w^2_{s_4} \simeq z^2_{s_3}) \sqcup (z^1_{s_3} \simeq w^2_{s_4} \sqcap w^2_{s_4} \simeq z^1_{s_3}), (z^2_{s_3} \simeq w^2_{s_4} \sqcap z^1_{s_3} \simeq w^1_{s_4}) \sqcup (z^2_{s_3} \simeq w^1_{s_4} \sqcap z^1_{s_3} \simeq w^2_{s_4}) >$ from the $B^{\simeq}$-unifier σ which must satisfy $\sigma(x^1_{s_1}) = \sigma(y^2_{s_2}) = w^1_{s_4}$, $\sigma(x^2_{s_1}) = \sigma(y^1_{s_2}) = w^2_{s_4}$, $\sigma(y^1_{s_1}) = \sigma(x^2_{s_2}) = z^1_{s_3}$, and $\sigma(y^2_{s_1}) = \sigma(x^1_{s_2}) = z^2_{s_3}$,

(d) $< (w^1_{s_4} \simeq z^1_{s_3} \sqcap w^2_{s_4} \simeq z^2_{s_3}) \sqcup (z^1_{s_3} \simeq w^2_{s_4} \sqcap w^2_{s_4} \simeq z^1_{s_3}), (z^1_{s_3} \simeq w^2_{s_4} \sqcap z^2_{s_3} \simeq w^1_{s_4}) \sqcup (z^1_{s_3} \simeq w^1_{s_4} \sqcap z^2_{s_3} \simeq w^2_{s_4}) >$ from the $B^{\simeq}$-unifier σ which must satisfy $\sigma(x^1_{s_1}) = \sigma(y^2_{s_2}) = w^1_{s_4}$, $\sigma(x^2_{s_1}) = \sigma(y^1_{s_2}) = w^2_{s_4}$, $\sigma(y^1_{s_1}) = \sigma(x^1_{s_2}) = z^1_{s_3}$, and $\sigma(y^2_{s_1}) = \sigma(x^2_{s_2}) = z^2_{s_3}$,

(e) $< (w^1_{s_4} \simeq z^1_{s_3} \sqcap w^2_{s_4} \simeq z^2_{s_3}) \sqcup (z^1_{s_3} \simeq w^2_{s_4} \sqcap w^2_{s_4} \simeq z^1_{s_3}), (w^1_{s_4} \simeq z^2_{s_3} \sqcap w^2_{s_4} \simeq z^1_{s_3}) \sqcup (w^1_{s_4} \simeq z^1_{s_3} \sqcap w^2_{s_4} \simeq z^2_{s_3}) >$ from the $B^{\simeq}$-unifier σ which must satisfy $\sigma(x^1_{s_1}) = \sigma(x^1_{s_2}) = w^1_{s_4}$, $\sigma(x^2_{s_1}) = \sigma(x^2_{s_2}) = w^2_{s_4}$, $\sigma(y^1_{s_1}) = \sigma(y^2_{s_2}) = z^1_{s_3}$, and $\sigma(y^2_{s_1}) = \sigma(y^1_{s_2} = z^2_{s_3}$,

(f) $< (w^1_{s_4} \simeq z^1_{s_3} \sqcap w^2_{s_4} \simeq z^2_{s_3}) \sqcup (z^1_{s_3} \simeq w^2_{s_4} \sqcap w^2_{s_4} \simeq z^1_{s_3}), (w^1_{s_4} \simeq z^1_{s_3} \sqcap w^2_{s_4} \simeq z^2_{s_3}) \sqcup (w^1_{s_4} \simeq z^2_{s_3} \sqcap w^2_{s_4} \simeq z^1_{s_3}) >$ from the $B^{\simeq}$-unifier σ which must satisfy $\sigma(x^1_{s_1}) = \sigma(x^1_{s_2}) = w^1_{s_4}$, $\sigma(x^2_{s_1}) = \sigma(x^2_{s_2}) = w^2_{s_4}$, $\sigma(y^1_{s_1}) = \sigma(y^1_{s_2}) = z^1_{s_3}$, and $\sigma(y^2_{s_1}) = \sigma(y^2_{s_2}) = z^2_{s_3}$,

(g) $< (w^2_{s_4} \simeq z^1_{s_3} \sqcap w^2_{s_4} \simeq z^2_{s_3}) \sqcup (z^1_{s_3} \simeq w^2_{s_4} \sqcap w^2_{s_4} \simeq z^1_{s_3}), (w^2_{s_4} \simeq z^2_{s_3} \sqcap w^1_{s_4} \simeq z^1_{s_3}) \sqcup (w^2_{s_4} \simeq z^1_{s_3} \sqcap w^1_{s_4} \simeq z^2_{s_3}) >$ from the $B^{\simeq}$-unifier σ which must satisfy $\sigma(x^1_{s_1}) = \sigma(x^2_{s_2}) = w^1_{s_4}$, $\sigma(x^2_{s_1}) = \sigma(x^1_{s_2}) = w^2_{s_4}$, $\sigma(y^1_{s_1}) = \sigma(y^2_{s_2}) = z^1_{s_3}$, and $\sigma(y^2_{s_1}) = \sigma(y^1_{s_2}) = z^2_{s_3}$,

(h) $< (w^1_{s_4} \simeq z^1_{s_3} \sqcap w^2_{s_4} \simeq z^2_{s_3}) \sqcup (z^1_{s_3} \simeq w^2_{s_4} \sqcap w^2_{s_4} \simeq z^1_{s_3}), (w^2_{s_4} \simeq z^1_{s_3} \sqcap w^1_{s_4} \simeq z^2_{s_3}) \sqcup (w^2_{s_4} \simeq z^2_{s_3} \sqcap w^1_{s_4} \simeq z^1_{s_3}) >$ from the $B^{\simeq}$-unifier σ which must satisfy $\sigma(x^1_{s_1}) = \sigma(x^2_{s_2}) = w^1_{s_4}$, $\sigma(x^2_{s_1}) = \sigma(x^1_{s_2}) = w^2_{s_4}$, $\sigma(y^1_{s_1}) = \sigma(y^1_{s_2}) = z^1_{s_3}$, and $\sigma(y^2_{s_1}) = \sigma(y^2_{s_2}) = z^2_{s_3}$.

- For the oriented equations defining $\_ \simeq \_$, if $f \in \Omega$ is a A-symbol. $B^{\simeq}$-unification is infinitary in general, but by the form of the rules we can reason as follows (for the sake of readability, we use the infix operator $\_ \cdot \_$ to represent the A-symbol f):
  1. for $x_{k_1} \simeq x_{k_1} \to \top$ and $x^1_{s_2} \cdot x^2_{s_2} \simeq g(y^1_{s_{1_2}}, \ldots, y^n_{s_{n_2}}) \to \bot$ do not yield critical pairs;
  2. for $x_{k_1} \simeq x_{k_1} \to \top$ and $x^1_{s_2} \cdot x^2_{s_2} \simeq x^i_{s_2} \to \bot$ do not yield critical pairs;
  3. for $x^1_{s_1} \cdot x^2_{s_1} \simeq x^i_{s_1} \to \bot$, with $i \in \{1, 2\}$ and $x^1_{s_2} \cdot x^2_{s_2} \simeq g(y^1_{s_{1_2}}, \ldots, y^n_{s_{n_2}}) \to \bot$, for any $B^{\simeq}$-unifier σ we obtain the trivial critical pair $< \bot, \bot >$;
  4. for $x^1_{s_1} \cdot x^2_{s_1} \simeq x^i_s \to \bot$ and $x^1_{s_2} \cdot x^2_{s_2} \simeq x^{j'}_s \to \bot$, for any $B^{\simeq}$-unifier σ we obtain the trivial critical pair $< \bot, \bot >$;
  5. for $x^1_{s_1} \cdot x^2_{s_1} \simeq x^1_{s_1} \cdot y^2_{s_1} \to x^2_{s_1} \simeq y_{s_1}$ and $x_{k_2} \simeq x_{k_2} \to \top$, any $B^{\simeq}$-unifier σ is of the form: $x^i_{s_1} \mapsto u^i$, $y_{s_1} \mapsto v$, $x_{k_2} \mapsto w$ and must satisfy that $u^1 \cdot u^2 =_{B^{\simeq}} w =_{B^{\simeq}} u^1 \cdot v$. Therefore, by the left cancelation property of free semigroups we must have $u^2 =_{B^{\simeq}} v$. Therefore, the critical pair $< \top, u^2 \simeq v >$ is joinable by using $x_{k_3} \simeq x_{k_3} = \top$;
  6. the case $x^1_{s_1} \cdot x^2_{s_1} \simeq y_{s_1} \cdot x^2_{s_1} \to x^1_{s_1} \simeq y_{s_1}$ and $x_{k_2} \simeq x_{k_2} \to \top$ is symmetric to case (5);
  7. for $x^1_{s_1} \cdot x^2_{s_1} \simeq x^1_{s_1} \cdot y_{s_1} \to x^2_{s_1} \simeq y_{s_1}$ and $x^1_{s_2} \cdot x^2_{s_2} \simeq y_{s_2} \cdot x^2_{s_2} \to x^1_{s_2} \simeq y_{s_2}$ any $B^{\simeq}$-unifier σ that yields a critical pair must satisfy:

(a) $\sigma(x^1_{s_1}) \cdot \sigma(x^2_{s_1}) =_B \simeq\ u \cdot v =_B \simeq\ v' \cdot u' =_B \simeq\ \sigma(x^1_{s_2}) \cdot \sigma(x^2_{s_2})$, and $\sigma(x^1_{s_1}) \cdot \sigma(y^2_{s_1}) =_B \simeq\ u \cdot w =_B \simeq\ w' \cdot u' =_B \simeq\ \sigma(y^1_{s_2}) \cdot \sigma(x^2_{s_2})$ or is of the form

(b) $\sigma(x^1_{s_1}) \cdot \sigma(x^2_{s_1}) =_B \simeq\ u \cdot v =_B \simeq\ v' \cdot u' =_B \simeq\ \sigma(y^1_{s_2}) \cdot \sigma(x^2_{s_2})$, and $\sigma(x^1_{s_1}) \cdot \sigma(y^2_{s_1}) =_B \simeq\ u \cdot w =_B \simeq\ w' \cdot u' =_B \simeq\ \sigma(x^1_{s_2}) \cdot \sigma(x^2_{s_2})$.

Pictorically, both cases (7a) and (7b) can be represented as follows:

u	v	$\simeq$	u	w
$=_B \simeq$			$=_B \simeq$	
v'	u'	$\simeq$	w'	u'

We discuss in detail case (7a) since case (7b) is entirely analogous. We reason by subcases depending on the relative composition betweee $|u| + |u'|$, $|u \cdot v|$, and $|u \cdot w|$, where $|u|$ denotes the length of u as a word modulo A.

(a) If $|u| + |u'| = |u \cdot v|$ and $|u| + |u'| = |u \cdot w|$ (there is no overlap between u and u' on both terms) then $u \cdot v =_B \simeq\ u \cdot u' =_B \simeq\ v' \cdot u'$ and $u \cdot w =_B \simeq\ u \cdot u' =_B \simeq\ w' \cdot u'$. We get $< u' \simeq u', u \simeq u >$, which is trivially joinable;

(b) if $|u| + |u'| < |u \cdot v|$ and $|u| + |u'| < |u \cdot w|$ (there is no overlap between u and u' on both terms) then $u \cdot v =_B \simeq\ u \cdot q \cdot u' =_B \simeq\ v' \cdot u'$ and $u \cdot w =_B \simeq\ u \cdot p \cdot u' =_B \simeq\ w' \cdot u'$. We get $< q \cdot u' \simeq p \cdot u', u \cdot q \simeq u \cdot p >$. By cancelation property of free semigroups we must have $< q \simeq p, q \simeq p >$, which is trivially joinable;

(c) if $|u| + |u'| < |u \cdot v|$ and $|u| + |u'| = |u \cdot w|$ (there is no overlap between u and u' on both terms) then $u \cdot v =_B \simeq\ u \cdot q \cdot u' =_B \simeq\ v' \cdot u'$ and $u \cdot w =_B \simeq\ u \cdot u' =_B \simeq\ w' \cdot u'$. We get $< q \cdot u' \simeq u', u \cdot q \simeq u >$. Applying $x^1_{s_3} \cdot x^2_{s_3} \simeq x^1_{s_3} = \bot$ and $x^1_{s_4} \cdot x^2_{s_4} \simeq x^2_{s_4} = \bot$, the critical pair is joinable: $< \bot, \bot >$;

(d) the case $|u| + |u'| = |u \cdot v|$ and $|u| + |u'| < |u \cdot w|$ is entirely similar to case (7c);

(e) if $|u| + |u'| < |u \cdot v|$ and $|u| + |u'| > |u \cdot w|$ (there is overlap between u and u' on the second term) then $u \cdot v =_B \simeq\ u \cdot q \cdot u' =_B \simeq\ v' \cdot u'$ and $u \cdot w =_B \simeq\ w' \cdot p \cdot w =_B \simeq\ w' \cdot u'$. We get $< q \cdot u' \simeq w, u \cdot q \simeq w' >$. Since $u' =_B \simeq\ p \cdot w$ and $u =_B \simeq\ w' \cdot p$, we have $< q \cdot p \cdot w \simeq w, w' \cdot p \cdot q \simeq w' > =< \bot, \bot >$, applying $x^1_{s_3} \cdot x^2_{s_3} \simeq x^1_{s_3} = \bot$ and $x^1_{s_4} \cdot x^2_{s_4} \simeq x^2_{s_4} = \bot$;

(f) if $|u| + |u'| = |u \cdot v|$ and $|u| + |u'| > |u \cdot w|$ (there is overlap between u and u' on the second term) then $u \cdot v =_B \simeq\ u \cdot u' =_B \simeq\ v' \cdot u'$ and $u \cdot w =_B \simeq\ w' \cdot p \cdot w =_B \simeq\ w' \cdot u'$. We get $< u' \simeq w, u \simeq w' >$. Since $u' =_B \simeq\ p \cdot w$ and $u =_B \simeq\ w' \cdot p$, we have $< p \cdot w \simeq w, w' \cdot p \simeq w' > =< \bot, \bot >$, applying $x^1_{s_3} \cdot x^2_{s_3} \simeq x^1_{s_3} = \bot$ and $x^1_{s_4} \cdot x^2_{s_4} \simeq x^2_{s_4} = \bot$;

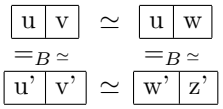
(g) the case $|u| + |u'| > |u \cdot v|$ and $|u| + |u'| < |u \cdot w|$ is entirely similar to case (7e);

(h) the case $|u| + |u'| > |u \cdot v|$ and $|u| + |u'| = |u \cdot w|$ is entirely similar to case (7f);

(i) if $|u| + |u'| > |u \cdot v|$ and $|u| + |u'| > |u \cdot w|$ (there is overlap between u and u' on both terms) then $u \cdot v =_{B\simeq} v' \cdot q \cdot v =_{B\simeq} v' \cdot u'$ and $u \cdot w =_{B\simeq} w' \cdot p \cdot w =_{B\simeq} w' \cdot u'$. We get $< v \simeq w, v' \simeq w' >$. Since $u' =_{B\simeq} q \cdot v =_{B\simeq} p \cdot w$ and $u =_{B\simeq} v' \cdot q =_{B\simeq} w' \cdot p$, we have three cases:
   i. If $|p| = |q|$ then we have that $p =_{B\simeq} q$, $v =_{B\simeq} w'$, $v' =_{B\simeq} w'$, and hence $< \top, \top >$.
   ii. If $|p| > |q|$ the unique possibility that fits with the restrictions is that $p =_{B\simeq} q \cdot q' \cdot q$, and hence $u' =_{B\simeq} q \cdot v =_{B\simeq} q \cdot q' \cdot q \cdot w$, $u =_{B\simeq} v' \cdot q =_{B\simeq} w' \cdot q \cdot q' \cdot q$. By left and right cancellation we get $v =_{B\simeq} q' \cdot q \cdot w$, $v' =_{B\simeq} w' \cdot q \cdot q'$, and $< q' \cdot q \cdot w \simeq w, w' \cdot q \cdot q' \simeq w' > = < \bot, \bot >$, applying $x^1_{s_3} \cdot x^2_{s_3} \simeq x^1_{s_3} = \bot$ and $x^1_{s_4} \cdot x^2_{s_4} \simeq x^2_{s_4} = \bot$.
   iii. the case $|p| < |q|$ is symmetric to case (7(i)ii);

8. for $x^1_{s_1} \cdot x^2_{s_1} \simeq y^1_{s_1} \cdot y^2_{s_1} \to \bot$ if $\lrcorner(x^1_{s_1} \simeq y^1_{s_1}) \sqcap \lrcorner(\mathrm{root}^k_f(x^1_{s_1})) \sqcap \lrcorner(\mathrm{root}^k_f(y^1_{s_1})) = \top$ and $x_{k_2} \simeq x_{k_2} \to \top$, any $B^{\simeq}$-unifier σ which yields a critical pair is of the form: $x^i_{s_1} \mapsto u^i$, $y^i_{s_1} \mapsto v^i$, $x_{k_2} \mapsto w$ and must satisfy that $u^1 \cdot u^2 =_{B\simeq} w =_{B\simeq} v^1 \cdot v^2$. Therefore, $\lrcorner(\mathrm{root}^k_f(u^1)) \sqcap \lrcorner(\mathrm{root}^k_f(v^1)) \sqcap \lrcorner(u^1 \simeq v^1) \Rightarrow < \bot, \top >$. Since $\lrcorner(\mathrm{root}^k_f(u^1)) \sqcap \lrcorner(\mathrm{root}^k_f(v^1))$, this means that $|u^2| = |v^2|$, and hence $u^2 =_{B\simeq} v^2$ and $u^1 =_{B\simeq} v^1$ and $\lrcorner(u^1 \simeq v^1) = \bot$, by applying $x_{k_3} \simeq x_{k_3} = \top$. Therefore, the critical pair is unfeasible [5];
9. for $x^1_{s_1} \cdot x^2_{s_1} \simeq y^1_{s_1} \cdot y^2_{s_1} \to \bot$ if $\lrcorner(x^1_{s_1} \simeq y^1_{s_1}) \sqcap \lrcorner(\mathrm{root}^k_f(x^1_{s_1})) \sqcap \lrcorner(\mathrm{root}^k_f(y^1_{s_1})) = \top$ and $x^1_{s_2} \cdot x^2_{s_2} \simeq x^1_{s_2} \cdot y_{s_2} \to x^2_{s_2} \simeq y_{s_2}$, any $B^{\simeq}$-unifier σ that yields a critical pair must satisfy:
   (a) $\sigma(x^1_{s_1}) \cdot \sigma(x^2_{s_1}) =_{B\simeq} u \cdot v =_{B\simeq} u' \cdot v' =_{B\simeq} \sigma(x^1_{s_2}) \cdot \sigma(x^2_{s_2})$, and $\sigma(y^1_{s_1}) \cdot \sigma(y^2_{s_1}) =_{B\simeq} u \cdot w =_{B\simeq} w' \cdot z' =_{B\simeq} \sigma(x^1_{s_2}) \cdot \sigma(y_{s_2})$ or is of the form
   (b) $\sigma(x^1_{s_1}) \cdot \sigma(x^2_{s_1}) =_{B\simeq} u \cdot v =_{B\simeq} u' \cdot v' =_{B\simeq} \sigma(x^1_{s_2}) \cdot \sigma(y_{s_2})$, and $\sigma(y^1_{s_1}) \cdot \sigma(y^2_{s_1}) =_{B\simeq} u \cdot w =_{B\simeq} w' \cdot z' =_{B\simeq} \sigma(x^1_{s_2}) \cdot \sigma(x^2_{s_2})$.

   Pictorically, both cases (9a) and (9b) can be represented as follows:



   This means that $u = u' \cdot q \cdot v = w' \cdot p \cdot w$. Since $|u'| = |w'| = 1$ then $u' =_{B\simeq} w'$, and $\lrcorner(u' \simeq w') = \bot$, by applying $x_{k_3} \simeq x_{k_3} = \top$. Therefore, the critical pair is unfeasible;
10. for $x^1_{s_1} \cdot x^2_{s_1} \simeq y^1_{s_1} \cdot y^2_{s_1} \to \bot$ if $\lrcorner(x^1_{s_1} \simeq y^1_{s_1}) \sqcap \lrcorner(\mathrm{root}^k_f(x^1_{s_1})) \sqcap \lrcorner(\mathrm{root}^k_f(y^1_{s_1})) = \top$ and $x^1_{s_2} \cdot x^2_{s_2} \simeq y_{s_2} \cdot x^2_{s_2} \to x^1_{s_2} \simeq y_{s_2}$, any $B^{\simeq}$-unifier σ that yields a critical pair must satisfy:
   (a) $\sigma(x^1_{s_1}) \cdot \sigma(x^2_{s_1}) =_{B\simeq} u \cdot v =_{B\simeq} u' \cdot v' =_{B\simeq} \sigma(x^1_{s_2}) \cdot \sigma(x^2_{s_2})$, and $\sigma(y^1_{s_1}) \cdot \sigma(y^2_{s_1}) =_{B\simeq} u \cdot w =_{B\simeq} w' \cdot z' =_{B\simeq} \sigma(y^1_{s_2}) \cdot \sigma(x^2_{s_2})$ or is of the form
   (b) $\sigma(x^1_{s_1}) \cdot \sigma(x^2_{s_1}) =_{B\simeq} u \cdot v =_{B\simeq} u' \cdot v' =_{B\simeq} \sigma(y^1_{s_2}) \cdot \sigma(x^2_{s_2})$, and $\sigma(y^1_{s_1}) \cdot \sigma(y^2_{s_1}) =_{B\simeq} u \cdot w =_{B\simeq} w' \cdot z' =_{B\simeq} \sigma(x^1_{s_2}) \cdot \sigma(x^2_{s_2})$.

Pictorically, both cases (10a) and (10b) can be represented as follows:

$$\begin{array}{ccc} \boxed{\text{u}\,|\,\text{v}} & \simeq & \boxed{\text{w}\,|\,\text{v}} \\ =_{B\simeq} & & =_{B\simeq} \\ \boxed{\text{u'}\,|\,\text{v'}} & \simeq & \boxed{\text{w'}\,|\,\text{z'}} \end{array}$$

This means that $u =_{B\simeq} u' \cdot q$ and $w =_{B\simeq} w' \cdot p$. Applying $x^1_{s_3} \cdot x^2_{s_3} \simeq y^1_{s_3} \cdot y^2_{s_3} \to \bot$ if $\lrcorner(x^1_{s_3} \simeq y^1_{s_3}) \sqcap \lrcorner(\text{root}^k_f(x^1_{s_3})) \sqcap \lrcorner(\text{root}^k_f(y^1_{s_3})) = \top$ to the resulting terms, we get $< \bot, \bot >$. Therefore, the critical pair is joinable;

11. for $x^1_{s_1} \cdot x^2_{s_1} \simeq x^1_{s_1} \to \bot$ and $x^1_{s_2} \cdot x^2_{s_2} \simeq x^1_{s_2} \cdot y_{s_2} \to x^2_{s_2} \simeq y_{s_2}$, any $B^{\simeq}$-unifier σ that yields a critical pair must satisfy:
    (a) $\sigma(x^1_{s_1}) \cdot \sigma(x^2_{s_1}) =_{B\simeq} u \cdot v \cdot w =_{B\simeq} u' \cdot v' =_{B\simeq} \sigma(x^1_{s_2}) \cdot \sigma(x^2_{s_2})$, and $\sigma(x^1_{s_1}) =_{B\simeq} u \cdot v =_{B\simeq} u' \cdot z' =_{B\simeq} \sigma(x^1_{s_2}) \cdot \sigma(y_{s_2})$ or is of the form
    (b) $\sigma(x^1_{s_1}) \cdot \sigma(x^2_{s_1}) =_{B\simeq} u \cdot v \cdot w =_{B\simeq} u' \cdot v' =_{B\simeq} \sigma(x^1_{s_2}) \cdot \sigma(y_{s_2})$, and $\sigma(x^1_{s_1}) =_{B\simeq} u \cdot v =_{B\simeq} u' \cdot z' =_{B\simeq} \sigma(x^1_{s_2}) \cdot \sigma(x^2_{s_2})$.
    Pictorically, both cases (11a) and (11b) can be represented as follows:

$$\begin{array}{ccc} \boxed{\text{u}\,|\,\text{v}\,|\,\text{w}} & \simeq & \boxed{\text{u}\,|\,\text{v}} \\ =_{B\simeq} & & =_{B\simeq} \\ \boxed{\text{u'}\,|\,\text{v'}} & \simeq & \boxed{\text{u'}\,|\,\text{z'}} \end{array}$$

    Then, $|u'| \not\geq |u \cdot v|$. Therefore, $u \cdot v =_{B\simeq} u' \cdot z'$ and we get the critical pair $< \bot, z' \cdot w \simeq z' >$. Again, applying the rule $x^1_{s_3} \cdot x^2_{s_3} \simeq x^1_{s_3} \to \bot$ the critical pair is joinable;
12. for $x^1_{s_1} \cdot x^2_{s_1} \simeq x^1_{s_1} \to \bot$ and $x^1_{s_2} \cdot x^2_{s_2} \simeq y_{s_2} \cdot x^2_{s_2} \to x^1_{s_2} \simeq y_{s_2}$ is symmetric to case (11);
13. for $x^1_{s_1} \cdot x^2_{s_1} \simeq y^1_{s_1} \cdot y^2_{s_1} \to \bot$ if $\lrcorner(x^1_{s_1} \simeq y^1_{s_1}) \sqcap \lrcorner(\text{root}^k_f(x^1_{s_1})) \sqcap \lrcorner(\text{root}^k_f(y^1_{s_1})) = \top$ and $x^1_{s_2} \cdot x^2_{s_2} \simeq x^1_{s_2} \to \bot$, for any $B^{\simeq}$-unifier σ we obtain the trivial critical pair $< \bot, \bot >$;
14. for $x^1_{s_1} \cdot x^2_{s_1} \simeq y^1_{s_1} \cdot y^2_{s_1} \to \bot$ if $\lrcorner(x^1_{s_1} \simeq y^1_{s_1}) \sqcap \lrcorner(\text{root}^k_f(x^1_{s_1})) \sqcap \lrcorner(\text{root}^k_f(y^1_{s_1})) = \top$ and $x^1_{s_2} \cdot x^2_{s_2} \simeq y^1_{s_2} \cdot y^2_{s_2} \to \bot$ if $\lrcorner(x^1_{s_2} \simeq y^1_{s_2}) \sqcap \lrcorner(\text{root}^k_f(x^1_{s_2})) \sqcap \lrcorner(\text{root}^k_f(y^1_{s_2})) = \top$, for any $B^{\simeq}$-unifier σ we obtain the trivial critical pair $< \bot, \bot >$.

– For the oriented equations defining $\_ \simeq \_$, if $f \in \Omega$ is a AC-symbol (for the sake of readability, we use the infix operator $\_ + \_$ to represent the AC-symbol f):

1. for $x_{k_1} \simeq x_{k_1} \to \top$ and $x^1_{s_2} + x^2_{s_2} \simeq g(y^1_{s_2}, \ldots, y^n_{s_n}) \to \bot$ do not yield critical pairs;
2. for $x_{k_1} \simeq x_{k_1} \to \top$ and $x^1_{s_2} + x^2_{s_2} \simeq x^1_{s_2} \to \bot$ do not yield critical pairs;
3. for $x^1_{s_1} + x^2_{s_1} \simeq x^1_{s_1} \to \bot$ and $x^1_{s_2} + x^2_{s_2} \simeq g(y^1_{s_{1_2}}, \ldots, y^n_{s_{n_2}}) \to \bot$, for any $B^{\simeq}$-unifier σ we obtain the trivial critical pair $< \bot, \bot >$;
4. for $x^1_{s_1} + x^2_{s_1} \simeq x^1_{s_1} + y_{s_1} \to x^2_{s_1} \simeq y_{s_1}$ and $x_{k_2} \simeq x_{k_2} \to \top$, any $B^{\simeq}$-unifier σ that yields a critical pair is of the form: $x^i_{s_1} \mapsto u^i$, $y_{s_1} \mapsto v$, $x_{k_2} \mapsto w$ and must satisfy that $u^1 + u^2 =_{B\simeq} w =_{B\simeq} u^1 + v$. Therefore, by the cancelation property of free commutative semigroups we must have $u^2 =_{B\simeq} v$. Therefore, the critical pair $< \top, u^2 \simeq v >$ is joinable;

5. for $x^1_{s_1} + x^2_{s_1} \simeq y^1_{s_1} + y^2_{s_1} \to \bot$ if $\backsim(\mathrm{in}^k_f(x^1_{s_1}, y^1_{s_1} + y^2_{s_1})) \sqcap \backsim(\mathrm{root}^k_f(x^1_{s_1})) = \top$ and $x_{k_2} \simeq x_{k_2} \to \top$, any $B^{\simeq}$-unifier σ that yields a critical pair is of the form: $x^i_{s_1} \mapsto u^i$, $y^i_{s_1} \mapsto v^i$, $x_{k_2} \mapsto w$ and must satisfy that $u^1 + u^2 =_{B\simeq} w =_{B\simeq} v^1 + v^2$. Therefore, $\backsim(\mathrm{root}^k_f(u^1)) \sqcap \backsim(\mathrm{in}^k_f(u^1, v^1 + v^2)) \Rightarrow < \bot, \top >$ where $u^1 + u^2 =_{B\simeq} w =_{B\simeq} v^1 + v^2$. We now reason by cases. If $u^1 = g(t_1, \ldots, t_m)$ then we have $\backsim(\mathrm{in}^k_f(g(t_1, \ldots, t_m), v^1 + v^2)) =_{B\simeq} \backsim(\mathrm{in}^k_f(g(t_1, \ldots, t_m), g(t_1, \ldots, t_m) + v^2)) \to^+_{E\simeq/B\simeq} \backsim(\top) \to_{E\simeq/B\simeq} \bot$, and the critical pair is unfeasible; otherwise, $u^1 = w_1 + w_2$, but then $\backsim(\mathrm{root}^k_f(w_1 + w_2)) \to^+_{E\simeq/B\simeq} \backsim(\top) \to_{E\simeq/B\simeq} \bot$ and the critical pair is again unfeasible;
6. for $x^1_{s_1} + x^2_{s_1} \simeq y^1_{s_1} + y^2_{s_1} \to \bot$ if $\backsim(\mathrm{in}^k_f(x^1_{s_1}, y^1_{s_1} + y^2_{s_1}) \sqcap \backsim(\mathrm{root}^k_f(x^1_{s_1})) = \top$ and $x^1_{s_2} + x^2_{s_2} \simeq x^1_{s_2} + y_{s_2} \to x^2_{s_2} \simeq y_{s_2}$, any $B^{\simeq}$-unifier σ that yields a critical pair must satisfy:
   (a) $\sigma(x^1_{s_1}) + \sigma(x^2_{s_1}) =_{B\simeq} u + v =_{B\simeq} u' + v' =_{B\simeq} \sigma(x^1_{s_2}) + \sigma(x^2_{s_2})$, and $\sigma(y^1_{s_1}) + \sigma(y^2_{s_1}) =_{B\simeq} w + z =_{B\simeq} u' + z' =_{B\simeq} \sigma(x^1_{s_2}) + \sigma(y_{s_2})$ or is of the form
   (b) $\sigma(x^1_{s_1}) + \sigma(x^2_{s_1}) =_{B\simeq} u + v =_{B\simeq} u' + v' =_{B\simeq} \sigma(x^1_{s_2}) + \sigma(y_{s_2})$, and $\sigma(y^1_{s_1}) + \sigma(y^2_{s_1}) =_{B\simeq} w + z =_{B\simeq} u' + z' =_{B\simeq} \sigma(x^1_{s_2}) + \sigma(x^2_{s_2})$.

   Pictorically, both cases (6*a*) and (6*b*) can be represented as follows:

u	v	$\simeq$	w	z
$=_{B\simeq}$			$=_{B\simeq}$	
u'	v'	$\simeq$	u'	w'

   Therefore, we have $\backsim(\mathrm{in}^k_f(u, w + z)) \sqcap \backsim(\mathrm{root}^k_f(u)) \Rightarrow < \bot, v' \simeq w' >$. If $\backsim(\mathrm{in}^k_f(u, w + z))$ then $\backsim(\mathrm{in}^k_f(u, w'))$ and $v' =_{B\simeq} u$ or $v' =_{B\simeq} u + p$.
   (a) If $\mathsf{root}(v') \neq \mathsf{root}(w')$ then the critical pair is joinable: $< \bot, \bot >$.
   (b) If $\mathsf{root}(v') = \mathsf{root}(w')$ and $\backsim(\mathrm{root}^k_f(v'))$ then $v' =_{B\simeq} u$, $u \simeq w' \to^*_{E\simeq/B\simeq} \bot$, and the critical pair is joinable: $< \bot, \bot >$.
   (c) If $\mathsf{root}(v') = \mathsf{root}(w')$ and $\mathrm{root}^k_f(v')$ then $v' =_{B\simeq} u + p$, and we can apply $x^1_{s_3} + x^2_{s_3} \simeq y^1_{s_3} + y^2_{s_3} \to \bot$ if $\backsim(\mathrm{in}^k_f(x^1_{s_3}, y^1_{s_3} + y^2_{s_3}) \sqcap \backsim(\mathrm{root}^k_f(x^1_{s_3})) = \top$, obtaining a joinable critical pair: $< \bot, \bot >$;
7. for $x^1_{s_1} + x^2_{s_1} \simeq x^1_{s_1} \to \bot$ and $x^1_{s_2} + x^2_{s_2} \simeq x^1_{s_2} + y^2_{s_2} \to x^2_{s_2} \simeq y^2_{s_2}$, yield the critical pairs:
   (a) $< \bot, w^2_{s_3} \simeq w^2_{s_3} + w^3_{s_3} >$ with the $B^{\simeq}$-unifier σ, $x^1_{s_1} \mapsto w^1_{s_3} + w^2_{s_3}$, $x^2_{s_1} \mapsto w^3_{s_3}$, $x^{i'}_s \mapsto w^i_{s_3}$, $y^2_{s_2} \mapsto w^2_{s_3} + w^3_{s_3}$. We can apply the rule $x^1_{s_4} + x^2_{s_4} \simeq x^1_{s_4} \to \bot$ to get a joinable critical pair,
   (b) $< \bot, w^2_{s_3} + w^3_{s_3} \simeq w^2_{s_3} >$ with the $B^{\simeq}$-unifier σ, $x^1_{s_1} \mapsto w^1_{s_3} + w^2_{s_3}$, $x^2_{s_1} \mapsto w^3_{s_3}$, $x^1_{s_2} \mapsto w^1_{s_3}$, $x^2_{s_2} \mapsto w^2_{s_3} + w^3_{s_3}$, and $y^2_{s_2} \mapsto w^2_{s_3}$. We can apply the rule $x^1_{s_4} + x^2_{s_4} \simeq x^1_{s_4} \to \bot$ to get a joinable critical pair;
8. for $x^1_{s_1} + x^2_{s_1} \simeq y^1_{s_1} + y^2_{s_1} \to \bot$ if $\backsim(\mathrm{in}^k_f(x^1_{s_1}, y^1_{s_1} + y^2_{s_1})) \sqcap \backsim(\mathrm{root}^k_f(x^1_{s_1})) = \top$ and $x^1_{s_2} + x^2_{s_2} \simeq y^1_{s_2} + y^2_{s_2} \to \bot$ if $\backsim(x^1_{s_2} \simeq y^1_{s_2}) \sqcap \backsim(\mathrm{root}^k_f(x^1_{s_2})) \sqcap \backsim(\mathrm{root}^k_f(y^1_{s_2})) = \top$, for any $B^{\simeq}$-unifier σ we obtain the trivial critical pair $< \bot, \bot >$;

9. for $x^1_{s_1}+x^2_{s_1} \simeq x^1_{s_1}+y^2_{s_1} \to x^2_{s_1} \simeq y^2_{s_1}$ and $x^1_{s_2}+x^2_{s_2} \simeq x^1_{s_2}+y^2_{s_2} \to x^2_{s_2} \simeq y^2_{s_2}$, any $B^{\simeq}$-unifier σ that yields a critical pair must satisfy:
   (a) $\sigma(x^1_{s_1}) + \sigma(x^2_{s_1}) =_{B^{\simeq}} u + v =_{B^{\simeq}} u' + v' =_{B^{\simeq}} \sigma(x^1_{s_2}) + \sigma(x^2_{s_2})$, and $\sigma(x^1_{s_1}) + \sigma(y^2_{s_1}) =_{B^{\simeq}} u + w =_{B^{\simeq}} u' + w' =_{B^{\simeq}} \sigma(x^1_{s_2}) + \sigma(y_{s_2})$ or is of the form
   (b) $\sigma(x^1_{s_1}) + \sigma(x^2_{s_1}) =_{B^{\simeq}} u + v =_{B^{\simeq}} u' + v' =_{B^{\simeq}} \sigma(x^1_{s_2}) + \sigma(y^2_{s_2})$, and $\sigma(x^1_{s_1}) + \sigma(y^2_{s_1}) =_{B^{\simeq}} u + w =_{B^{\simeq}} u' + w' =_{B^{\simeq}} \sigma(x^1_{s_2}) + \sigma(x^2_{s_2})$.

   Both cases (9a) and (9b) can be represented as follows: $u + v =_{B^{\simeq}} u_1 + \cdots + u_n + v_1 + \cdots + v_m + w_1 + \cdots + w_o + z$ and $u' + v' =_{B^{\simeq}} u_1 + \cdots + u_n + v_1 + \cdots + v_m + w_1 + \cdots + w_o + z'$ where $u_1 + \cdots + u_n$ are the elements shared by u and u', $v_1 + \cdots + v_m$ are the elements from u not shared with u' and $w_1 + \cdots + w_o$ are the elements from u' not shared with u (can be empty sets). We can consider the following cases:
   (a) if $u_1 + \cdots + u_n$ is empty, we have two possible cases:
      i. $v_1 + \cdots + v_m$ is not empty, $w_1 + \cdots + w_o$ is not empty, z is empty, and z' is empty then the critical pairs is of the form $< w_1 + \cdots + w_o \simeq w_1 + \cdots + w_o, v_1 + \cdots + v_m \simeq v_1 + \cdots + v_m >$. Using the rule $x^2_{k_3} \simeq x_{k_3} \to \top$ on both sides we get the joinable critical pair $< \top, \top >$,
      ii. $v_1 + \cdots + v_m$ is not empty, $w_1 + \cdots + w_o$ is not empty, z is empty, and z' is not empty then the critical pairs is of the form $< w_1 + \cdots + w_o \simeq w_1 + \cdots + w_o + z', v_1 + \cdots + v_m \simeq v_1 + \cdots + v_m + z' >$. Using the rule $x^1_{s_3} + x^2_{s_3} \simeq x^1_{s_3} \to \bot$ on both sides we get the joinable critical pair $< \bot, \bot >$,
      iii. $v_1 + \cdots + v_m$ is not empty, $w_1 + \cdots + w_o$ is not empty, z is not empty, and z' is empty the case is symmetric to (9$(a)ii$),
      iv. $v_1 + \cdots + v_m$ is not empty, $w_1 + \cdots + w_o$ is not empty, z is not empty, and z' is not empty then the critical pairs is of the form $< w_1 + \cdots + w_o + z \simeq w_1 + \cdots + w_o + z', v_1 + \cdots + v_m + z \simeq v_1 + \cdots + v_m + z' >$. Using the rule $x^1_{s_3} + x^2_{s_3} \simeq x^1_{s_3} + y^2_{s_3} \to x^2_{s_3} \simeq y^2_{s_3}$ on both sides we get the joinable critical pair $< z \simeq z', z \simeq z' >$,
   (b) if $u_1 + \cdots + u_n$ is not empty, we have eight possible cases:
      i. $v_1 + \cdots + v_m$ is empty, $w_1 + \cdots + w_o$ is empty, z is not empty and z' is not empty then the critical pairs is of the form $< z \simeq z', z \simeq z' >$ and is joinable,
      ii. $v_1 + \cdots + v_m$ is not empty, $w_1 + \cdots + w_o$ is empty, z is not empty and z' is not empty then the critical pairs is of the form $< z \simeq z', v_1 + \cdots + v_m + z \simeq v_1 + \cdots + v_m + z' >$. Using the rule $x^1_{s_3} + x^2_{s_3} \simeq x^1_{s_3} + y^2_{s_3} \to x^2_{s_3} \simeq y^2_{s_3}$ on the right-hand side we get the joinable critical pair $< z \simeq z', z \simeq z' >$,
      iii. $v_1 + \cdots + v_m$ is empty, $w_1 + \cdots + w_o$ is not empty, z is not empty and z' is not empty then the critical pairs is of the form $< w_1 + \cdots + w_o + z \simeq w_1 + \cdots + w_o + z', z \simeq z' >$. Using the rule $x^1_{s_3} + x^2_{s_3} \simeq x^1_{s_3} + y^2_{s_3} \to x^2_{s_3} \simeq y^2_{s_3}$ on the left-hand side we get the joinable critical pair $< z \simeq z', z \simeq z' >$,

iv. $v_1 + \cdots + v_m$ is not empty, $w_1 + \cdots + w_o$ is not empty, the cases are symmetric to (9a).

10. for $x^1_{s_1} + x^2_{s_1} \simeq x^1_{s_1} \to \bot$ and $x^1_{s_2} + x^2_{s_2} \simeq y^1_{s_2} + y^2_{s_2} \to \bot$ if $\backsim(x^1_{s_2} \simeq y^1_{s_2}) \sqcap \backsim(\mathrm{root}^k_f(x^1_{s_2})) \sqcap \backsim(\mathrm{root}^k_f(y^1_{s_2})) = \top$, for any $B^{\simeq}$-unifier σ we obtain the trivial critical pair $< \bot, \bot >$.

– For root^k_f rules when f is an A or AC symbol, we have $\mathrm{root}^k_f(f(x^1_{s_1}, x^n_s)) = \top$ and $\mathrm{root}^k_f(g(x^1_{s'_1}, \ldots, x^m_{s'_m})) = \bot$ do not yield critical pairs.

– For in^k_f rules when f is an AC-symbol:

1. for $\mathrm{in}^k_f(x_{s_1}, y_{k_1}) \to \bot$ if $\mathrm{root}^k_f(x_{s_1}) = \top$ and $\mathrm{in}^k_f(x_{s_2}, x_{s_2} + y_{s_2}) \to \top$ if $\backsim(\mathrm{root}^k_f(x_{s_2})) = \top$, we get the unfeasible critical pair $\mathrm{root}^k_f(w_{s_3}) \wedge \backsim(\mathrm{root}^k_f(w_{s_3})) \Rightarrow < \bot, \top >$ for the $B^{\simeq}$-unifier σ: $x_{s_1} \mapsto w_{s_3}$, $y_{k_1} \mapsto w_{s_3} + z_{s_3}$, $x_{s_2} \mapsto w_{s_3}$ and $y_{s_2} \mapsto z_{s_3}$;
2. for $\mathrm{in}^k_f(x_{s_1}, y_{k_1}) \to \bot$ if $\mathrm{root}^k_f(x_{s_1}) = \top$ and $\mathrm{in}^k_f(x_{s_2}, y^1_{s_{1_2}} + y^2_{s_{1_2}}) \to (x_{s_2} \simeq y^1_{s_{1_2}}) \sqcup \mathrm{in}^k_f(x_{s_2}, y^2_{s_{1_2}})$ if $\backsim(\mathrm{root}^k_f(x_{s_2})) \sqcap \backsim(\mathrm{root}^k_f(y^1_{s_{1_2}})) = \top$ the case is symmetric to (1);
3. for $\mathrm{in}^k_f(x_{s_1}, y_{k_1}) \to \bot$ if $\mathrm{root}^k_f(x_{s_1}) = \top$ and $\mathrm{in}^k_f(x_{s_2}, y_{s_2}) \to x_{s_2} \simeq y_{s_2}$ if $\backsim(\mathrm{root}^k_f(x_{s_2})) \sqcap \backsim(\mathrm{root}^k_f(y_{s_2})) = \top$ is symmetric to (1);
4. for $\mathrm{in}^k_f(x_{s_1}, x_{s_1} + y_{s_1}) \to \top$ if $\backsim(\mathrm{root}^k_f(x_{s_1})) = \top$ and $\mathrm{in}^k_f(x_{k_2}, y^1_{s_{1_2}} + y^2_{s_{1_2}}) \to x_{k_2} \simeq y^1_{s_{1_2}} \sqcup \mathrm{in}^k_f(x_{k_2}, y^2_{s_{1_2}})$ if $\backsim(\mathrm{root}^k_f(x_{k_2})) \sqcap \backsim(\mathrm{root}^k_f(y^1_{s_{1_2}})) = \top$, we get the following $B^{\simeq}$-unifiers σ
   (a) $x_{s_1} \mapsto w^1_{s_3} + w^2_{s_3}$, $y_{s_1} \mapsto w^3_{s_3} + w^4_{s_3}$, $x_{k_2} \mapsto w^1_{s_3} + w^2_{s_3}$, $y^1_{s_1} \mapsto w^1_{s_3} + w^3_{s_3}$ and $y^2_{s_1} \mapsto w^2_{s_3} + w^4_{s_3}$ yielding a unfeasible critical pair of the form $\backsim(\mathrm{root}^k_f(w^1_{s_3} + w^2_{s_3})) \wedge (\backsim(\mathrm{root}^k_f(w^1_{s_3} + w^2_{s_3})) \sqcap \backsim(\mathrm{root}^k_f(w^1_{s_3} + w^3_{s_3})) < \top, w^1_{s_3} + w^2_{s_3} \simeq w^1_{s_3} + w^3_{s_3} \sqcup \mathrm{in}^k_f(w^1_{s_3} + w^2_{s_3}, w^2_{s_3} + w^4_{s_3} >$,
   (b) $x_{s_1} \mapsto w^1_{s_3} + w^2_{s_3}$, $y_{s_1} \mapsto w^3_{s_3}$, $x_{k_2} \mapsto w^1_{s_3} + w^2_{s_3}$, $y^1_{s_1} \mapsto w^1_{s_3} + w^3_{s_3}$ and $y^2_{s_1} \mapsto w^2_{s_3}$ yielding a unfeasible critical pair of the form $\backsim(\mathrm{root}^k_f(w^1_{s_3}+w^2_{s_3})) \wedge (\backsim(\mathrm{root}^k_f(w^1_{s_3}+w^2_{s_3})) \sqcap \backsim(\mathrm{root}^k_f(w^1_{s_3}+w^3_{s_3})) < \top, w^1_{s_3} + w^2_{s_3} \simeq w^1_{s_3} + w^3_{s_3} \sqcup \mathrm{in}^k_f(w^1_{s_3} + w^2_{s_3}, w^2_{s_3}) >$,
   (c) $x_{s_1} \mapsto w^1_{s_3}$, $y_{s_1} \mapsto w^2_{s_3} + w^3_{s_3}$, $x_{k_2} \mapsto w^1_{s_3}$, $y^1_{s_1} \mapsto w^1_{s_3} + w^2_{s_3}$ and $y^2_{s_1} \mapsto w^3_{s_3}$ yielding a unfeasible critical pair of the form $\backsim(\mathrm{root}^k_f(w^1_{s_3})) \wedge (\backsim(\mathrm{root}^k_f(w^1_{s_3})) \sqcap \backsim(\mathrm{root}^k_f(w^1_{s_3} + w^2_{s_3})) < \top, w^1_{s_3} \simeq w^1_{s_3} + w^2_{s_3} \sqcup \mathrm{in}^k_f(w^1_{s_3}, w^3_{s_3}) >$,
   (d) $x_{s_1} \mapsto w^1_{s_3} + w^2_{s_3}$, $y_{s_1} \mapsto w^3_{s_3}$, $x_{k_2} \mapsto w^1_{s_3} + w^2_{s_3}$, $y^1_{s_1} \mapsto w^1_{s_3}$ and $y^2_{s_1} \mapsto w^2_{s_3} + w^3_{s_3}$ yielding a unfeasible critical pair of the form $\backsim(\mathrm{root}^k_f(w^1_{s_3} + w^2_{s_3})) \wedge (\backsim(\mathrm{root}^k_f(w^1_{s_3} + w^2_{s_3})) \sqcap \backsim(\mathrm{root}^k_f(w^1_{s_3})) < \top, w^1_{s_3} + w^2_{s_3} \simeq w^1_{s_3} \sqcup \mathrm{in}^k_f(w^1_{s_3} + w^2_{s_3}, w^2_{s_3} + w^3_{s_3}) >$,
   (e) $x_{s_1} \mapsto w^1_{s_3}$, $y_{s_1} \mapsto w^2_{s_3}$, $x_{k_2} \mapsto w^1_{s_3}$, $y^1_{s_1} \mapsto w^1_{s_3}$ and $y^2_{s_1} \mapsto w^2_{s_3}$ yielding a joinable critical pair of the form $\backsim(\mathrm{root}^k_f(w^1_{s_3})) \wedge (\backsim(\mathrm{root}^k_f(w^1_{s_3})) \sqcap \backsim(\mathrm{root}^k_f(w^1_{s_3})) < \top, w^1_{s_3} \simeq w^1_{s_3} \sqcup \mathrm{in}^k_f(w^1_{s_3}, w^2_{s_3}) >$,
   (f) $x_{s_1} \mapsto w^1_{s_3}$, $y_{s_1} \mapsto w^2_{s_3} + w^3_{s_3}$, $x_{k_2} \mapsto w^1_{s_3}$, $y^1_{s_1} \mapsto w^2_{s_3}$ and $y^2_{s_1} \mapsto w^1_{s_3} + w^3_{s_3}$ yielding a joinable critical pair of the form $\backsim(\mathrm{root}^k_f(w^1_{s_3})) \wedge (\backsim(\mathrm{root}^k_f(w^1_{s_3})) \sqcap \backsim(\mathrm{root}^k_f(w^2_{s_3})) < \top, w^1_{s_3} \simeq w^2_{s_3} \sqcup \mathrm{in}^k_f(w^1_{s_3}, w^1_{s_3} + w^3_{s_3}) >$,

(g) $x_{s_1} \mapsto w^1_{s_3}, y_{s_1} \mapsto w^2_{s_3}, x_{k_2} \mapsto w^1_{s_3}, y^1_{s_1} \mapsto w^2_{s_3}$ and $y^2_{s_1} \mapsto w^1_{s_3}$ yielding a joinable critical pair of the form $\sim(\mathrm{root}^k_f(w^1_{s_3})) \wedge (\sim(\mathrm{root}^k_f(w^1_{s_3})) \sqcap \sim(\mathrm{root}^k_f(w^2_{s_3})) < \top, w^1_{s_3} \simeq w^2_{s_3} \sqcup \mathrm{in}^k_f(w^1_{s_3}, w^1_{s_3}) >$;

5. for $\mathrm{in}^k_f(x_{s_1}, x_{s_1} + y_{s_1}) \to \top$ if $\sim(\mathrm{root}^k_f(x_{s_1})) = \top$ and $\mathrm{in}^k_f(x_{k_2}, y_{k_2}) \to x_{k_2} \simeq y_{k_2}$ if $\sim(\mathrm{root}^k_f(x_{k_2})) \sqcap \sim(\mathrm{root}^k_f(y_{k_2})) = \top$, the unfeasible critical pair $\sim(\mathrm{root}^k_f(w^1_{s_3})) \wedge (\sim(\mathrm{root}^k_f(w^1_{s_3})) \sqcap \sim(\mathrm{root}^k_f(w^1_{s_3} + w^2_{s_3}))) \Rightarrow < \top, w^1_{s_3} \simeq w^1_{s_3} + w^2_{s_3} >$ is obtained with the $B^{\simeq}$-unifier σ such that $x_{s_1} \mapsto w^1_{s_3}, y_{s_1} \mapsto w^2_{s_3}, x_{k_2} \mapsto w^1_{s_3}$ and $y_{k_2} \mapsto w^1_{s_3} + w^2_{s_3}$;
6. For the rules $\mathrm{in}^k_f(x_{k_1}, y^1_{s_1} + y^2_{s_1}) \to x_{k_1} \simeq y^1_{s_1} \sqcup \mathrm{in}^k_f(x_{k_1}, y^2_{s_1})$ if $\sim(\mathrm{root}^k_f(x_{k_1})) \sqcap \sim(\mathrm{root}^k_f(y^1_{s_1})) = \top$ and $\mathrm{in}^k_f(x_{k_2}, y_{k_2}) \to x_{k_2} \simeq y_{k_2}$ if $\sim(\mathrm{root}^k_f(x_{k_2})) \sqcap \sim(\mathrm{root}^k_f(y_{k_2})) = \top$, yields the unfeasible critical pair $(\sim(\mathrm{root}^k_f(w^1_{s_3})) \sqcap \sim(\mathrm{root}^k_f(w^2_{s_3}))) \wedge (\sim(\mathrm{root}^k_f(w^1_{s_3})) \sqcap \sim(\mathrm{root}^k_f(w^2_{s_3} + w^3_{s_3}))) \Rightarrow < w^1_{s_3} \simeq w^2_{s_3} \sqcup \mathrm{in}^k_f(w^1_{s_3}, w^3_{s_3}), w^1_{s_3} \simeq w^2_{s_3} + w^3_{s_3} >$ with the $B^{\simeq}$ unifier θ such that $x_{k_1} \mapsto w^1_{s_3}, y^1_{s_1} \mapsto w^2_{s_3}, y^2_{s_1} \mapsto w^3_{s_3}, x_{k_2} \mapsto w^1_{s_3}$ and $y_{k_2} \mapsto w^2_{s_3} + w^3_{s_3}$.

□

5.4 Preservation of Free Constructors Modulo

In this section we check that $\Omega^{\simeq} = \Omega \uplus \{\top, \bot\} \subseteq \Sigma^{\simeq}$ is a signature of free constructors (for $\mathcal{E}^{\simeq}$) modulo $B^{\simeq}$. The former one establishes that $\Omega^{\simeq}$ is indeed a subsignature of free constructors modulo $B^{\simeq}$ and the latter one that the function symbols in $\Omega^{\simeq}$ are free modulo $B^{\simeq}$. We use the following auxiliary lemma.

Lemma 8. *Let the transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$, where $\mathcal{E}$ is ground sort-decreasing, ground confluent, operationally terminating modulo B theory and Ω is the signature of free constructors modulo B of $\mathcal{E}$. If $t, t' \in T_\Omega$, then $t \simeq t' \to^+_{E^{\simeq}/B^{\simeq}} \top$ iff $t =_B t'$.*

Proof. Consider ($\Leftarrow$) direction. If $t =_B t'$, then $x_k \simeq x_k \to \top$ applies modulo B and we have $t \simeq t' \to \top$.

Consider ($\Rightarrow$) direction. Suppose $t \neq_B t'$. Since B is a combination of C, A and AC axioms, we may reason by structural induction. Note that, by ground confluence, if $t \simeq t' \to^+ \top$ then $t \simeq t' \not\to^+ \bot$.

1. If $\mathsf{root}(t) \neq \mathsf{root}(t')$ then $t = f(t_1, \ldots, t_n)$, $t' = g(u_1, \ldots, u_n)$, $t \neq_B t'$ and $f(t_1, \ldots, t_n) \simeq g(u_1, \ldots, u_n) \to \bot$, as desired.
2. If $\mathsf{root}(t) = \mathsf{root}(t') = f$ and f is an absolutely free constructor symbol then $t = f(t_1, \ldots, t_n)$, $t' = f(t'_1, \ldots, t'_n)$, $f(t_1, \ldots, t_n) \simeq f(t'_1, \ldots, t'_n) \to \prod_{1 \leq i \leq n} t_i \simeq t'_i$. By induction hypothesis, $t_i \simeq t'_i$ iff $t_i =_B t'_i$, hence if there is a t_i, t'_i such that $t_i \neq_B t'_i$, $t \simeq t' \to \bot$, as desired. If for all i, $t_i =_B t'_i$ then $t \simeq t' \to \top$, leading to a contradiction with $t =_B t'$.

3. If $\mathsf{root}(t) = \mathsf{root}(t') = f$ and f is a commutative constructor symbol then $t = f(t_1, t_2)$, $t' = f(t'_1, t'_2)$, $f(t_1, t_2) \simeq f(t'_1, t'_2) \to (t_1 \simeq t'_1 \sqcap t_2 \simeq t'_2) \sqcup (t_1 \simeq t'_2 \sqcap t_2 \simeq t'_1)$. By induction hypothesis, $t_i \simeq t'_j$ iff $t_i =_B t'_j$, and hence $f(t_1, t_2) \simeq f(t'_1, t'_2)$ iff $(t_1 =_B t'_1 \wedge t_2 =_B t'_2) \vee (t_1 =_B t'_2 \wedge t_2 =_B t'_1) = t =_B t'$, as desired.
4. If $\mathsf{root}(t) = \mathsf{root}(t') = f$ and f is an associative constructor symbol then $t = f(t_1, t_2)$, $t' = f(t'_1, t'_2)$, $\mathsf{root}(t_1) \neq f$ and $\mathsf{root}(t'_1) \neq f$. By the induction hypothesis, $t_1 \simeq t'_1 \to^+ \top$ iff $t_1 =_B t'_1$ and $t_2 \simeq t'_2 \to^+ \top$ iff $t_2 =_B t'_2$. If $t_1 =_B t'_1$ then, applying $f(x^1_s, x^2_s) \simeq f(x^1_s, y^2_s) = x^2_s \simeq y^2_s$ we get $t \simeq t' = t_2 \simeq t'_2$ and $t_2 \simeq t'_2 = \top$ iff $t_2 =_B t'_2$, as desired. If $t_1 \neq_B t'_1$ then appying $f(x^1_s, x^2_s) \simeq f(y^1_s, y^2_s) = \bot$ if $\lrcorner(\mathrm{root}^k_f(x^1_s)) \sqcap \lrcorner(\mathrm{root}^k_f(y^1_s)) \sqcap \lrcorner(x^1_s \simeq y^1_s) = \top$ we get $t \simeq t' = \bot$, as desired.
5. If $\mathsf{root}(t) = \mathsf{root}(t') = f$ and f is an associative-commutative constructor symbol, we flatten the terms $t = f(t_1, \ldots, t_n)$, $t' = f(t'_1, \ldots, t'_m)$ where $\mathsf{root}(t_i), \mathsf{root}(t'_j) \neq f$. By the induction hypothesis, $t_i \simeq t'_j \to^+ \top$ iff $t_i =_B t'_j$. If $t_1 =_B t'_1$ then, applying $f(x^1_s, x^2_s) \simeq f(x^1_s, y^2_s) = x^2_s \simeq y^2_s$ we get $t \simeq t' = f(t_2, \ldots, t_n) \simeq f(t'_2, \ldots, t'_m)$ and $f(t_2, \ldots, t_n) \simeq f(t'_2, \ldots, t'_m) = \top$ iff $f(t_2, \ldots, t_n) =_B f(t'_2, \ldots, t'_m)$, as desired. If $t_1 \neq_B t'_1$ and $\mathrm{in}^k_f(t_1, f(t'_2, \ldots, t'_m)) \to^+ \bot$ (note that in^k_f can be unfolded as $\mathrm{in}^k_f(t, f(t_1, \ldots, t_n)) = \bigsqcup_{1 \leq i \leq n} t \simeq t_i$ and by induction hypothesis it is equivalent to $\bigcup_{1 \leq i \leq n} t =_B t_i$), then appying $\mathsf{f}(x^1_s, x^2_s) \simeq \mathsf{f}(y^1_s, y^2_s) = \bot$ if $\lrcorner(\mathrm{root}^k_f(x^1_s))) \sqcap \lrcorner(\mathrm{in}^k_f(x^1_s, f(y^1_s, y^2_s)))$ we get $t \simeq t' \to^+ \bot$, as desired. If $t_1 =_B t'_j$ then $\mathrm{in}^k_f(t_1, f(t'_2, \ldots, t'_m)) \to^+ \top$ and $t' = f(t'_1, \ldots, t_1, \ldots, t'_m) =_B f(t_1, t'_1, \ldots, t'_m)$. Applying $f(x^1_s, x^2_s) \simeq f(x^1_s, y^2_s) = x^2_s \simeq y^2_s$ we get $t \simeq t' = f(t_2, \ldots, t_n) \simeq f(t'_1, \ldots, t'_m)$ and $f(t_2, \ldots, t_n) \simeq f(t'_1, \ldots, t'_m) = \top$ iff $f(t_2, \ldots, t_n) =_B f(t'_1, \ldots, t'_m)$, as desired.

Theorem 4. *If $\mathcal{E}$ is ground sort-decreasing, ground confluent, and operationally terminating modulo B, then $\mathcal{E}^{\simeq}$ has $\Omega^{\simeq} \subseteq \Sigma^{\simeq}$ as a signature of free constructors modulo $B^{\simeq}$.*

Proof. First, we know that all constructor on $T_{\Omega^{\simeq}}$ are irreducible by $E^{\simeq}$ modulo $B^{\simeq}$, so if we can show that for each $t \in T_{\Sigma^{\simeq}/E^{\simeq} \cup B^{\simeq}}$ it $(E^{\simeq}/B^{\simeq})$-canonical form is a $\Omega^{\simeq}$-term, then we are done.

Suppose not, and let t be a term of minimum size such that $can_{E^{\simeq}/B^{\simeq}}(t) \notin T_{\Omega^{\simeq}}$. Obviously t must be of sort Bool, and it top symbol *cannot* be a Boolean connective (if so, by minimality all its arguments are $\bot$ or $\top$ and $\Omega^{\mathrm{Bool}} = \{\top, \bot\}$ is the subsignature of free constructors modulo B^{Bool} of $\mathcal{E}^{\mathrm{Bool}}$), so either is of the form

1. $\mathrm{root}^k_f(t)$, with $t \in T_\Omega$ and f A or AC
   (a) If $t = f(t_1, t_2) \in T_\Omega$, we have $\mathrm{root}^k_f(t) \to \top$, against the hypothesis.
   (b) If $t = g(t_1, \ldots, t_n) \in T_\Omega$ and $g \neq f$, we have $\mathrm{root}^k_f(t) \to \bot$, against the hypothesis.
2. $\mathrm{in}^k_f(t, t')$, with $t, t' \in T_\Omega$ and f AC

(a) If $\mathsf{root}(t) = f$, we have $\mathrm{in}_f^k(t, t') \to \bot$, against the hypothesis.
(b) If $\mathsf{root}(t) \neq f$,
  i. $\mathsf{root}(t') \neq f$, then $\mathrm{in}_f^k(t, t') \to t \simeq t'$, against the hypothesis.
  ii. $\mathsf{root}(t') = f$, then $t' = f(u_1, u_2)$ with $\mathsf{root}(u_1) \neq f$ and $\mathrm{in}_f^k(t, f(u_1, u_2)) \to u_1 \simeq t \sqcup \mathrm{in}_f^k(t, u_2)$, against the hypothesis.

3. $t \simeq t'$, with $t, t' \in T_\Omega$.
(a) If $\mathsf{root}(t) \neq \mathsf{root}(t')$ then $t \simeq t' \to \bot$, against the hypothesis.
(b) If $\mathsf{root}(t) = \mathsf{root}(t') = f$ and f is an absolutely free constructor then $f(t_1, \ldots, t_n) \simeq f(t'_1, \ldots, t'_n) \to \bigsqcap_{1 \leq i \leq n} t_i \simeq t'_i$, against the hypothesis.
(c) If $\mathsf{root}(t) = \mathsf{root}(t') = f$ and f is a commutative constructor then $f(t_1, t_2) \simeq f(t'_1, t'_2) \to (t_1 \simeq t'_1 \sqcap t_2 \simeq t'_2) \sqcup (t_1 \simeq t'_2 \sqcap t_2 \simeq t'_1)$.
(d) If $\mathsf{root}(t) = \mathsf{root}(t') = f$ and f is an associative constructor symbol. Let $t = f(t_1, t_2)$, $t' = f(t'_1, t'_2)$, $\mathsf{root}(t_1) \neq f$ and $\mathsf{root}(t'_1) \neq f$. By minimality $t_1 \simeq t'_1$ reduces to $\top$ or $\bot$. If $t_1 \simeq t'_1$ reduces to $\top$ then $t_1 = t'_1$ by Lemma 8 and $f(t_1, t_2) \simeq f(t_1, t'_2) \to t_2 \simeq t'_2$, against the hypothesis. If $t_1 \simeq t'_1$ reduces to $\bot$ then $f(t_1, t_2) \simeq f(t'_1, t'_2) \to \bot$, against the hypothesis.
(e) If $\mathsf{root}(t) = \mathsf{root}(t') = f$ and f is an associative-commutative constructor symbol. Let $t = f(t_1, t_2)$, $t' = f(t'_1, t'_2)$, $\mathsf{root}(t_1) \neq f$ and $\mathsf{root}(t'_1) \neq f$. By minimality $t_1 \simeq t'_1$ reduces to $\top$ or $\bot$. If $t_1 \simeq t'_1$ reduces to $\top$ then $t_1 = t'_1$ by Lemma 8 and $f(t_1, t_2) \simeq f(t_1, t'_2) \to t_2 \simeq t'_2$, against the hypothesis. If $t_1 \simeq t'_1$ reduces to $\bot$, by minimality $\mathrm{in}_f^k(t_1, t'_2)$ reduces to $\top$ or $\bot$. If $\mathrm{in}_f^k(t_1, t'_2)$ reduces to $\bot$ then $f(t_1, t_2) \simeq f(t'_1, t'_2) \to \bot$, against the hypothesis. If $\mathrm{in}_f^k(t_1, t'_2)$ reduces to $\top$ then there is some subterm t_i in t' such that $t_1 = t'$ by Lemma 8, then $t' = f(t'_1, t'_2) =_B f(t_1, t''_2)$ and $f(t_1, t_2) \simeq f(t_1, t''_2) \to t_2 \simeq t''_2$, against the hypothesis.

□

6 $\mathcal{E}^{\simeq}$ is an Equality Enrichment

In Section 5 the equational theory $\mathcal{E}^{\simeq}$ obtained using the transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ was proved to inherit the good executability properties from $\mathcal{E}$. In this section it is proved that $\mathcal{E}^{\simeq}$ is indeed an equality enrichment, that is, that the equality function $\simeq$ in $\mathcal{E}^{\simeq}$ is a sound and complete equality predicate for $\mathcal{T}_{\mathcal{E}}$.

Theorem 5. *Let $\mathcal{E} = (\Sigma, E \uplus B)$ be an order sorted equational theory with signature $\Omega \subseteq \Sigma$ of free constructors modulo B and let $\mathcal{E}^{\simeq} = (\Sigma^{\simeq}, E^{\simeq} \uplus B^{\simeq})$ be the equational theory obtained by using $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$. If $\mathcal{E}$ is ground sort-decreasing, operationally terminating, and ground confluent modulo B, then $\mathcal{E}^{\simeq}$ is a Boolean equality enrichment of $\mathcal{E}$.*

Proof. From the assumptions and by theorems 1, 2, and 3 if follows that $\mathcal{E}^{\simeq}$ is ground sort-decreasing, operationally terminating, and ground confluent modulo $B^{\simeq}$. Moreover, since Ω is a signature of free constructors modulo B, $\mathcal{E}^{\simeq}$ has

$\Omega^{\simeq} = \Omega \uplus \{\top, \bot\}$ as a signature of free constructors modulo $B^{\simeq}$ by Theorem 4. We check $\mathcal{E}^{\simeq}$ against Definition 1. Let s be a sort in Σ and let k be the topmost sort in the connected component of s in $\Sigma^{\simeq}$. The function symbols in $\Sigma^{\simeq} \setminus \Sigma$ have target sort Bool and because Bool is not a sort in Σ it follows that $\Sigma^{\simeq}$ adds no junk to the sort s. Also note that the equations in $E^{\simeq} \setminus E$ have as left-hand side terms with sort Bool, and then $E^{\simeq}$ adds no confusion to the sort s. Hence, $\mathcal{E}^{\simeq}$ is a protecting extension of $\mathcal{E}$. On the other hand, note that $\Sigma^{\simeq}$ extends the poset of sorts of Σ with the new sort Bool from $\mathcal{E}^{\mathrm{Bool}}$ and Bool belongs to a new connected component in $\Sigma^{\simeq}$. It is also true that $\top$ and $\bot$ are the Bool constructor terms in $\Sigma^{\simeq}$. By ground confluence of $\mathcal{E}^{\simeq}$ and freeness of $\Omega^{\simeq}$ modulo $B^{\simeq}$, it follows that $\top \neq_{\mathcal{E}^{\simeq}} \bot$. Because s is in Σ it follows that $k \neq \mathrm{Bool}$ and thus $\Sigma^{\simeq}$ has an operator $\mathrm{C}\ \_ \simeq \_ : k\ k \longrightarrow \mathrm{Bool}$. It reamins to prove sentences 1 and 2, or equivalently, for any $t, u \in T_{\Sigma,s}$:

$$\mathcal{E} \vdash t = u \iff \mathcal{E}^{\simeq} \vdash (t \simeq u) = \top \iff \mathcal{E}^{\simeq} \nvdash (t \simeq u) = \bot.$$

Let $t, u \in T_{\Sigma,s}$. First note that the second equivalence follows by the ground confluence of $\mathcal{E}^{\simeq}$ and the freeness of $\Omega^{\simeq}$. Also note that $\mathcal{E} \vdash t = u$ trivially implies $\mathcal{E}^{\simeq} \vdash (t \simeq u) = \top$ because of the equation $x_k \simeq x_k = \top$ in $E^{\simeq}$. Then, it is enough to prove that $\mathcal{E} \vdash t = u$ is a logical consequence of $\mathcal{E}^{\simeq} \vdash (t \simeq u) = \top$. Without loss of generality assume $t, u \in T_{\Omega,s}$. If $\mathcal{E}^{\simeq} \vdash (t \simeq u) = \top$ because of the equation $x_k \simeq x_k = \top$ in $E^{\simeq}$, then $t =_{B^{\simeq}} u$ which implies $t =_B u$ and hence $\mathcal{E} \vdash t = u$. Otherwise, let $t = f(t_1, \ldots, t_n)$ and $u = g(u_1, \ldots, u_m)$ and let us proceed by structural induction on the complexity of t and u, and by cases on the axioms B of f:

- f is an absolutely free symbol: by Definition 3 it must be the case that $f = g$, $n = m$, and $(t_i \simeq u_i) = \top$ for $1 \leq i \leq n$, and thus $t = u$ by the induction hypothesis;
- f is a C-symbol: by Definition 4 it must be the case that $f = g$, $n = 2 = m$, and either $(t_1 \simeq u_1) = \top = (t_2 \simeq u_2)$ or $(t_1 \simeq u_2) = \top = (t_2 \simeq u_1)$, and thus $t = u$ by the induction hypothesis;
- f is an A-symbol: by Definition 5 it must be the case that $f = g$, $n = 2 = m$, and either $t_1 = u_1$ and $(t_2 \simeq u_2) = \top$ or $t_2 = u_2$ and $(t_1 \simeq u_1) = \top$, and thus $t = u$ by the induction hypothesis;
- f is an AC-symbol: by Definition 6 it must be the case that $f = g$, $n = 2 = m$, and $t_1 = u_1$ and $(t_2 \simeq u_2) = \top$, and thus $t = u$ by the induction hypothesis.

Finally, $\mathcal{E}^{\simeq}$ is Boolean because $\mathcal{E}^{\mathrm{Bool}} \subseteq \mathcal{E}^{\simeq}$. □

7 Automation of the $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ Transformation, Applications, and a Case Study

The transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ is obviously *constructive*. This means that, using reflection, it can be automated as an equationally-defined function at the metalevel, which takes the meta-representation of $\mathcal{E}$ as input and returns the

meta-representation of $\mathcal{E}^{\simeq}$ as its output. We have achieved this automation in Maude by using the `META-LEVEL` module, thus making it available within the Maude language. The transformation code, as well as a collection of examples, is available at `http://camilorocha.info`.

The transformation itself has already been incorporated into several Maude formal tools, including the Maude CRC-ChC, and the Maude Invariant Analyzer. In the near future it should be added to other tools such as the Maude Termination Tool (MTT) and the Maude Sufficient Completeness Checker (SCC). One obvious advantage of these additions is the possibility of systematically transforming specifications making use of built-in equalities and inequalities, which cannot be handled by formal tools, into specifications where such built-in equalities and inequalities are systematically replaced by equationally-defined equalities, so that formal tools can be applied. But this is not the only possible application by any means. For example, the extended version [8] shows how the addition of equationally-defined equality predicates also makes the specification and verification of safety properties in the Invariant Analyzer tool considerably easier.

It is also clear that adding an equationally-defined equality to Maude's Inductive Theorem Prover (ITP) would make this tool more effective in many ways, and would also greatly reduce the complexities of dealing with arbitrary universal formulas as goals, since all such formulas would be reduced to unconditional equality goals. It would also be very useful to explore the use of the $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ transformation in *inductionless induction* theorem proving. Yet another very useful field of application would be *early failure detection* in narrowing-based unification. The idea is that $E \cup B$-unification goals can be viewed as equality goals, which can be detected to have already *failed* if they can be rewritten to *false* with $E^{\simeq}$ modulo $B^{\simeq}$.

We present now a case study involving the use of the $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$ transformation in the Maude Invariant Analyzer (InvA) tool [15], which is a tool to prove deductively safety properties of a rewrite theory $\mathcal{R}$.

InvA is based on an inference system that transforms all formal temporal reasoning about safety properties of concurrent transitions to purely equational inductive reasoning. InvA provides a substantial degree of mechanization and can automatically discharge many proof obligations without user intervention. We illustrate how equality enrichments can be used to support the deductive verification task in the InvA tool.

A typical mutual exclusion protocol for processes, called `QLOCK`, uses a global queue as follows:

- each process that participates in the protocol does the following:
  - if the process wants to use the critical resource and its name is not in the global queue, it places its name in the queue;
  - if the process wants to use the critical resource and its name is in the global queue, if its name is at the top of the queue then the process gains access to the critical resource; otherwise it waits; and
  - if the process finishes the critical resource, it removes its name from the top of the global queue.

- the protocol should start from the state where the queue is empty; and
- it is assumed that each process can use the critical resource any number of times.

Consider the following equational theory $\mathcal{E}^{\texttt{QLOCK-SYNTAX}}$ that represents the states of `QLOCK` with terms of sort `State`. It protects the equational theory $\mathcal{E}^{\texttt{MSET}}$ presented in Section 4. Processes and names of processes are modeled with natural numbers of sort `Nat` in Peano notation. A term `Pi | Pw | Pc | Q` of sort `State` describes the state in which `Pi` is the collection of processes whose name is not in the global queue (or *idle* processes), `Pw` is the collection of processes whose names that are waiting to gain access to the critical resource (or *waiting* processes), `Pc` is the collection of processes that are using the critical resource (or *critical* processes), and `Q` is the global queue of the system. Sorts `MSet` and `Queue` are used to represent collections of processes and queues of processes' names, respectively.

```
fmod QLOCK-SYNTAX is
  protecting MSET .

  sort Queue .
  op nil : -> Queue [ctor] .
  op _@_ : Nat Queue -> Queue [ctor] .
  op _;_ : Queue Queue -> Queue .
  eq nil ; Q:Queue = Q:Queue .
  eq (N:Nat @ Q1:Queue) ; Q2:Queue = N:Nat @ (Q1:Queue ; Q2:Queue) .

  sort State .
  op _|_|_|_ : MSet MSet MSet Queue -> State [ctor] .
endfm
```

The behavior of a transition system in rewriting logic is specified by rewrite rules that define how the individual transitions change the state of the system. The specification of all transitions of `QLOCK` is described by six rewrite rules in the rewrite theory $\mathcal{R}^{\texttt{QLOCK}}$ as follows.

```
mod QLOCK is
  protecting QLOCK-SYNTAX .

  vars Pi Pw Pc : MSet .   var Q : Queue .   vars N N' N'' : Nat .

  rl [to-wait-1] : N | Pw | Pc | Q  =>  empty | Pw N | Pc
                 | Q ; (N @ nil ) .
  rl [to-wait-2] : N Pi | Pw | Pc | Q  =>  Pi | Pw N | Pc
                 | Q ; (N @ nil ) .
  rl [to-crit-1] : Pi | N | Pc | N @ Q  =>  Pi | empty | Pc N | N @ Q .
  rl [to-crit-2] : Pi | Pw N | Pc | N @ Q  =>  Pi | Pw | Pc N | N @ Q .
  rl [to-idle-1] : Pi | Pw | N | N' @ Q  =>  Pi N | Pw | empty | Q .
  rl [to-idle-2] : Pi | Pw | Pc N | N' @ Q  =>  Pi N | Pw | Pc | Q .
endm
```

Rewrite rules `to-idle-1` and `to-idle-2` specify the behavior of a process that finishes using the critical resource: it goes to state idle and the name on top of the global queue is removed. Similarly, rewrite rules `to-wait-1` and `to-wait-2`, and `to-crit-1` and `to-crit-2`, specify the behavior of a process that wants to use the critical resource and of a process that is granted access to the critical resource, respectively.

We want to verify that the `QLOCK` satisfies the following safety properties. It is key that (i) it satisfies the mutual exclusion property, namely, that at any point of execution there is at most one process using the critical resource. We also want to verify that (ii) the name on top of the global queue coincides with the name of the process using the critical resource, if any. Finally, we want to verify that (iii) the global queue only contains the names of all waiting and critical processes. State predicates `mutex`, `priority`, and `cqueue`, respectively, specify properties (i), (ii), and (iii) in the following equational theory $\mathcal{E}^{\texttt{QLOCK-PREDS}}$. State predicate `init` specifies the set of inital states of `QLOCK`, with auxiliary function `set?` that distinguishes multisets having no repeated elements. State predicate `unique` is an strengthening for `mutex` and `priority`. Auxiliary function `to-soup` on input `Q` of sort `Queue` computes the multiset made from the natural numbers in `Q`.

```
fmod QLOCK-PREDS is
  protecting QLOCK-SYNTAX .
  protecting EQ-MSET .

  vars N N'      : Nat .   var Q   : Queue .
  vars Pi Pw Pc  : MSet .  var NeS  : NeMSet .

  ops init mutex unique priority cqueue : State -> [Bool] .

  eq init( Pi | empty | empty | nil ) = set?(Pi) .
  eq mutex( Pi | Pw | empty | Q ) = true .
  eq mutex( Pi | Pw | N | Q ) = true .
  eq mutex( Pi | Pw | N NeS | Q ) = false .
  eq unique( Pi | Pw | empty | Q ) = set?(Pi Pw) .
  eq unique( Pi | Pw | N | N @ Q ) = set?(Pi Pw N) .
  eq unique( Pi | Pw | N NeS | Q ) = false .
  eq priority( Pi | Pw | empty | Q ) = true .
  eq priority( Pi | Pw | N | N' @ Q ) = N === N' .
  eq priority( Pi | Pw | N Pc | N' @ Q ) = (N === N') and
                                           (Pc === empty) .
  eq cqueue( Pi | Pw | Pc | Q ) = Pw Pc === to-soup(Q) .
....
endfm
```

Observe that $\mathcal{E}^{\texttt{QLOCK-PREDS}}$ protects the equality enrichment $\mathcal{E}^{\texttt{EQ-NAT-SOUP}}$, found in Section 4, for the connected component of sort `MSet` that defines the equality enrichment for sorts `Nat`, `MSet`, and `NeMSet`. The equality enrichments for these sorts are key in the specification of the state predicates. For instance,

predicates `priority` and `cqueue` are directly defined in terms of the equality predicate for sorts `Nat` and `MSet`, and also use the Boolean connective for conjunction `and` that comes with the Boolean equality enrichment. Auxiliary function `set?` also makes use of the equality enrichment for sort `Nat`. Note that, in general, defining from scratch the equality enrichment for an AC-symbol such as the multiset union in $\mathcal{E}^{\texttt{MSet}}$, can be a daunting task. Instead, in $\mathcal{E}^{\texttt{QLOCK-PREDS}}$, the definition of the state predicate `cqueue` was straightforward with the help of the equality enrichment for multisets of natural numbers.

By using the InvA tool we are able to automatically prove that predicates `mutex` and `priority` are invariants of $\mathcal{R}^{\texttt{QLOCK}}$ for any initial state that satisfies predicate `init`. For predicate `cqueue` some proof obligations cannot be automatically discharged. In general terms, 22 out of 26 proof obligations were automatically discharged. However, this is an encouraging result, because the current version of the InvA tool does not have dedicated inference support for Boolean equality enrichments which could greatly improve the degree of deductive automation.

8 Related Work and Conclusions

In [7], the author generalizes and simplifies the technique given in [12] for proving induction hypothesis without induction (so-called *inductionless induction*) using enriched theories with the equality. The notion of *s-taut* related with a sort s can be seen as a initial approximation of what we called in this paper an equality enrichment. The technique described in the paper is based in the result stated in Corollary 2.

In [11], the authors define the notion of *equality enrichment* (without axioms) as an explicit subrepresentation of an *equational equality presentation*. Our work extends this notion of equality enrichment with axioms and also presents an automatic way to generate this equality enrichment modulo axioms. As the authors of [11] also remark, an equality enrichment can be used for using inductionless induction theorem proving technique.

In [13], the authors propose an equality predicate for algebraic specifications. Unlike our work, the authors do not consider axioms and sufficient completeness in their theories, hence they have to manage terms with define symbols. In the positive cases, their equality predicate is equivalent to ours, but in the negative cases, a *false* answer in [13] does not mean that both terms are distinct for any possible instantiation (as we state in our work), because the negative rules are based on a check of convergence between terms. The goal of this behavior is to avoid false positives instead of capturing negative cases.

In conclusion, this paper solves an important open problem: how to make the addition of equationally defined equality predicates effective and automatic for a very wide class of equational specifications with initial algebra semantics. That such a transformation should exists is suggested by the Bergstra-Tucker meta-theorem [2], but such a meta-result is not constructive and gives no insight as to how the transformation could be defined. We have shown that it can be

defined for a very wide class of algebraic specifications with highly expressive features such as ordered-sorted types, conditional equations, and rewriting modulo commonly occurring axioms. We have also shown that all the expected good properties of the input theory $\mathcal{E}$ are preserved by the transformation $\mathcal{E} \mapsto \mathcal{E}^{\simeq}$. Using reflection, this transformation has been implemented in Maude and has already been integrated into several formal tools. As mentioned above, this opens up many useful application to improve the state of the art in formal verification of algebraic specifications in general, and the Maude formal environment in particular.

References

1. Bachmair, L., Plaisted, D.A.: Termination Orderings for Associative-Commutative Rewriting Systems. Journal of Symbolic Computation 1(4), 329–349 (1985)
2. Bergstra, J., Tucker, J.: Characterization of Computable Data Types by Means of a Finite Equational Specification Method. In: de Bakker, J.W., van Leeuwen, J. (eds.) Proc. of the 7th International Colloquium on Automata, Languages and Programming, ICALP'80. LNCS, vol. 81, pp. 76–90. Springer-Verlag (1980)
3. Clavel, M., Durán, F., Eker, S., Lincoln, P., Martí-Oliet, N., Meseguer, J., Talcott, C.: All About Maude – A High-Performance Logical Framework, LNCS, vol. 4350. Springer-Verlag (2007)
4. Durán, F., Lucas, S., Meseguer, J.: Termination Modulo Combinations of Equational Theories. In: Ghilardi, S., Sebastiani, R. (eds.) Proc. of the 7th International Conference on Frontiers of Combining Systems, FroCoS'09. LNCS, vol. 5749, pp. 246–262. Springer-Verlag (2009)
5. Durán, F., Meseguer, J.: A Church-Rosser Checker Tool for Conditional Order-Sorted Equational Maude Specifications. Journal of Logic and Algebraic Programming to appear (2011)
6. Goguen, J., Meseguer, J.: Order-Sorted Algebra I: Equational Deduction for Multiple Inheritance, Overloading, Exceptions and Partial Operations. Theoretical Computer Science 105, 217–273 (1992)
7. Goguen, J.A.: How to Prove Algebraic Inductive Hypotheses Without Induction. In: Bibel, W., Kowalski, R. (eds.) Proc. of the 5th Conference on Automated Deduction, CADE'80. LNCS, vol. 87, pp. 356–373. Springer-Verlag (1980)
8. Gutiérrez, R., Meseguer, J., Rocha, C.: Order-Sorted Equality Enrichments Modulo Axioms (Extended Version). Tech. rep., University of Illinois at Urbana-Champaing (December 2011), available at `http://camilorocha.info`
9. Lucas, S., Marché, C., Meseguer, J.: Operational Termination of Conditional Term Rewriting Systems. Information Processing Letters 95(4), 446–453 (2005)
10. Meseguer, J.: Membership Algebra as a Logical Framework for Equational Specification. In: Parisi-Presicce, F. (ed.) Recent Trends in Algebraic Development Techniques, Proc. of the 12th International Workshop on Workshop on Algebraic Development Techniques, WADT'97. LNCS, vol. 1376, pp. 18–61. Springer-Verlag (1997)
11. Meseguer, J., Goguen, J.A.: Initially, Induction and Computability. Algebraic Methods in Semantics (1986)
12. Musser, D.R.: On Proving Inductive Properties of Abstract Data Types. In: Proc. of the 7th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL'80. pp. 154–162. ACM Press (1980)

13. Nakamura, M., Futatsugi, K.: On Equality Predicates in Algebraic Specification Languages. In: Jones, C.B., Liu, Z., Woodcock, J. (eds.) Proc. of the 4th International Conference on Theoretical Aspects of Computing, ICTAC'07. LNCS, vol. 4711, pp. 381–395. Springer-Verlag (2007)
14. Ohlebusch, E.: Advanced Topics in Term Rewriting. Springer-Verlag (2002)
15. Rocha, C., Meseguer, J.: Proving safety properties of rewrite theories. In: Corradini, A., Klin, B., Cîrstea, C. (eds.) Proc. of 4th International Conference on Algebra and Coalgebra in Computer Science, CALCO'11. LNCS, vol. 6859, pp. 314–328. Springer-Verlag (2011)
16. Rubio, A.: A Fully Syntactic AC-RPO. Information and Computation 178(2), 515–533 (2002)