Strict Coherence of Conditional Rewriting Modulo Axioms[1]

José Meseguer

University of Illinois at Urbana-Champaign, IL 61801, USA

Abstract

Conditional rewriting modulo axioms with rich types makes specifications and declarative programs very expressive and succinct and is used in all well-known rule-based languages. However, the current foundations of rewriting modulo axioms have focused for the most part on the unconditional and untyped case. The main purpose of this work is to generalize the foundations of rewriting modulo axioms to the conditional order-sorted case. A related goal is to simplify such foundations. In particular, even in the unconditional case, the notion of *strict coherence* proposed here makes rewriting modulo axioms simpler and easier to understand. Good properties of strictly coherent conditional theories, like operational equi-termination of the R/B and R, B relations and general conditions for the conditional Church-Rosser property modulo B are also studied.

Keywords: Conditional rewriting modulo equations, coherence, order-sorted specifications, operational termination, Church-Rosser property.

1. Introduction

Techniques for rewriting modulo axioms B are enormously useful. In practical, declarative programming terms, what they afford —particularly in combination with an expressive type stucture such as order-sorted or membership equational logic [17, 32]— is making available to the programmer a very rich variety of user-definable *data types* such as multisets, sets, lists with associative matching, combinations of all these with the usual tree-like data structures, and so on. Such expressive data types and matching *modulo* their algebraic properties allow the formulation of very expressive and remarkably succinct solutions to many computational problems as declarative programs. Substantiating this claim would require another paper; but I can refer the reader to [7] and, regarding efficient implementation of rewriting modulo commonly used axioms to [14], for what I consider by now overwhelming evidence.

[1]Partially Supported by NSF Grant CNS 13-19109.

In spite of the great usefulness of techiques for rewriting modulo axioms, they are quite specialized, a kind of *esoterica* among rewriting techniques, with many puzzling phenomena. The difficulties in accessing this area were recognized and addressed by Narendran, Subramanian and Guo in their expository note [35], studded with many intriguing examples, where they say:

> *Over the years we (and several others) have found the concepts very hard to internalize. One of the problems is that only the case where $E = AC$ has been investigated in detail. . . . . Experience with other equational theories has been lacking. As a result, many misleading and erroneous statements have crept into even some excellent papers.*

The above words contain a warning, since any study in this area runs the risk of making the entire subject even more impenetrable or, what is worse, of adding more erronous statements to the literature. Yet, some courage is needed, because the foundations of rewriting modulo axioms are still partially undeveloped and there is a real need, comming from practical applications, to obtain more general foundations.

I am referring particularly to the area of *conditional rewriting modulo axioms.* Conditional rewrite rules make declarative programs more expressive and are, for this reason, supported, in combination with rewriting modulo axioms, by many declarative rule-based languages such as OBJ [18], ASF+SDF [40], ELAN [5], CafeOBJ [15] and Maude [7]. However, there are at present two related foundational problems. The first problem is that, except for the limited foundations of conditional rewriting modulo equations provided by papers such as, e.g., [31, 4, 6, 13], the overwhelming majority of studies in this area, e.g., [19, 24, 26, 25, 37, 20, 21, 3, 22, 35, 23, 16] treat only the *unconditional* rewriting case. The second problem is that all the papers treating the unconditional case do so for *unsorted* signatures, which are unusable in practice, since all the declarative languages just mentioned support, for obvious reasons of expressiveness, many-sorted, order-sorted, or membership equational logic type structures.

To address the practical needs just explained, the main goal of this paper is to develop new foundations for *conditional* rewriting modulo axioms for rewrite theories with an *order-sorted* [17, 32] type structure. This of course includes the many-sorted case as a special case which, in turn, contains the unsorted case as the *least general possible.* Fortunately, the technical complexities involved in treating the much more general order-sorted case are minimal. However, since conditional rewriting is unavoidably more complex and subtle than unconditional rewriting, how can one even hope to make the somewhat esoteric subject of rewriting modulo axioms more accessible in a conditional setting? My answer to this real and challenging question is to distinguish two issues:

1. Since conditional rewriting includes unconditional rewriting as a special case, the overall subject of rewriting modulo axioms *will* be simplified and made more accessible if the *specialization* of the new, more general treatment to the unconditional case is indeed simpler and more easily

understandable than earlier unconditional treatments. This is achieved in Section 2, where several equivalent notions characterizing what I call *strict coherence* of rewriting modulo axioms are presented. Strict coherence is considerably simpler and has substantially better properties than the well-known notion of *coherence* [20, 21], which is at present the standard notion in the subject. In Section 4 I revisit this matter and show in detail that, if the axioms B are regular and linear, specifications, including conditional ones, can be completed (at least in the limit) to become strictly coherent, and can be easily checked for this property.[2]

2. Conditional rewriting modulo axioms *is* intrinsically more complex and subtle than unconditional rewriting modulo: this is the price to be paid for intrinsically more expressive specifications and programs. The relevant question, however, is whether conditional rewriting modulo axioms can be made *as simple as possible with the best possible properties*. This I achieve: (i) in Section 4 by showing that if the axioms B are linear and regular the closure under B-extensions of a conditional specification enjoys the remarkably good and simple property of strict coherence; (ii) in Section 5 by showing that if a conditional specification is closed under B-extensions, the R/B- and R,B-rewrite relations are *operationally equi-terminating*, i.e., they have the same conditional termination properties; and (iii) in Section 6, where I give theorems characterizing conditional rewrite theories that enjoy the Church-Rosser property modulo B, and identify general conditions under which provable equality of a conditional equational theory becomes decidable by rewriting modulo B.

The paper is organized as follows. Strict coherence is defined in Section 2. Conditional order-sorted rewriting modulo axioms is defined in Section 3. Strict coherence modulo B of conditional order-sorted rewrite theories for regular and linear axioms B is studied in Section 4. Equi-termination of conditional R/B- and R,B-rewriting for theories closed under B-extensions is proved in Section 5. The conditional Church-Rosser property modulo B is studied in Section 6. A discussion of related work and concluding remarks are given in Section 7.

2. Abstract Characterization of Strict Coherence

In this section strict coherence is characterized by means of four equivalent properties, namely, **Completeness**, **Bisimulation**, **Strict Coherence**, and **Strict Local Coherence**. The last two notions are *stronger versions* of the

[2] Admittedly, the regularity and linearity of B make the application of strict coherence less general than that of coherence, where no such limitations are imposed. However, I argue in Section 2 that such greater generality comes at a considerably high price of losing many useful properties and gaining a number of anomalies; and further argue in Section 7 that *strong coherence* [41, 13] is a promising alternative for achieving a general setting for rewriting modulo equational axioms that can even be conditional.

notions of *coherence* and *local coherence* in [21], and are related to, yet different from, the notions of *strong coherence* and *strong local coherence* in [41, 13]. The qualification "strict" has been chosen to avoid terminological confusion with all these related but different notions of coherence in [21, 41, 13].

The equivalences with **Completeness** and with **Bisimulation** help bringing out some important semantic properties implicit in strict coherence, as already emphasized in [12, 13]. A dicussion of some semantic consequences of these four equivalente properties, why they are important, and why in general they do not hold when the axioms B fail to be regular and linear is also given. The treatment below is in terms of abstract relations in the spirit of, e.g., [19, 21].

Let T be a set, whose elements are denoted $t, t', u, u', v, v', w, w'$ and so on. We will asume several binary relations on T, including the following. First, a symmetric relation on T, denoted $\leftrightarrow_B$. The smallest equivalence relation generated by $\leftrightarrow_B$ is its reflexive-transitivive closure, denoted $=_B$. R is a binary relation on T, denoted $\rightarrow_R$. The relation R/B is the composition[3] $=_B; R; =_B$ and is denoted $\rightarrow_{R/B}$. We also assume another relation R, B between R and R/B, that is, $R \subseteq R, B \subseteq R/B$. The relation R, B is denoted $\rightarrow_{R,B}$.

In practical applications R will be some rewrite relation,[4] and $\leftrightarrow_B$ (resp. $=_B$) the one-step equality relation (resp. the equality relation) generated by equations B. The relation $\rightarrow_{R/B}$ then describes rewriting *modulo* B. That is, it describes the action of R on $=_B$-equivalence classes. Indeed, $\rightarrow_{R/B}$ induces a binary relation —also denoted $\rightarrow_{R/B}$ by abuse of language— on the quotient set $T/{=_B}$ defined by the equivalence:

$$[t]_B \rightarrow_{R/B} [t']_B \quad \Leftrightarrow \quad t \rightarrow_{R/B} t',$$

where $[t]_B$ abbreviates the equivalence class $[t]_{=_B}$.

The intuition about the abstract relation $\rightarrow_{R,B}$ is that it is easier to compute than $\rightarrow_{R/B}$, but should still allow us to perform "essentially the same rewrites" as $\rightarrow_{R/B}$. This is captured by the **Completeness** property below. I follow the usual diagrammatic convention, where dashed lines indicate existential quantification. I spell this out in a first instance (the **Completeness** property), and freely use the convention from then on.

1. **Completeness**. This property relates $\rightarrow_{R/B}$ and $\rightarrow_{R,B}$ by the following property:

$$(\forall u, v \in T)\; u \rightarrow_{R/B} v \Rightarrow ((\exists v' \in T)\; u \rightarrow_{R,B} v' \wedge v =_B v').$$

Diagrammatically, the existential quantification is precisely described by the

[3] A relation composition $G; H$ is written in diagrammatic order, i.e., $G; H = \{(x, z) \mid (\exists y)\; xGy \wedge yHz\}$.

[4] But not necessarily the *standard* one: see, e.g., the discussions right before Proposition 1 and Corollary 4, showing that for conditional rewriting R is *not* the standard rewrite relation.

dashed lines in the diagram below.

$$\begin{tikzcd} u \arrow[r, "R/B"'] \arrow[dr, dotted, "R,B"'] & v \arrow[d, dotted, dash, "B"] \\ & v' \end{tikzcd}$$

where here and in what follows dotted lines indicate existential quantification.

A related intuition about $\to_{R,B}$ is that it should in an appropriate sense *simutate* $\to_{R/B}$. This is captured by the **Bisimulation** property below.

2. **Bisimulation**. This property also relates $\to_{R/B}$ and $\to_{R,B}$ as follows:

$$\begin{tikzcd} u \arrow[r, "R/B"'] \arrow[d, equal, "B"'] & v \arrow[d, dotted, dash, "B"] \\ u' \arrow[r, dotted, "R,B"'] & v' \end{tikzcd}$$

As its name indicates, this property is equivalent to the relation $=_B$ being a *bisimulation* between the transition systems $(T, \to_{R/B})$ and $(T, \to_{R,B})$. Strictly speaking, the property just states that $=_B$ is a *simulation relation* of $(T, \to_{R/B})$ by $(T, \to_{R,B})$. However, $=_B$ is *always* a simulation of $(T, \to_{R,B})$ by $(T, \to_{R/B})$ (and thus a bisimulation), since we have $(=_B; \to_{R,B}) \subseteq (=_B; \to_{R/B}) = \to_{R/B}$. Therefore, $(u \to_{R,B} v \wedge u =_B u')$ implies $u' \to_{R/B} v$.

3. **Strict Coherence**. This property relates $\to_{R,B}$ to itself. It can be briefly summarized by saying that $=_B$ is a *bisimulation* of $(T, \to_{R,B})$. Instead of writing the corresponding formula, I state it diagrammatically:

$$\begin{tikzcd} u \arrow[r, "R,B"'] \arrow[d, equal, "B"'] & v \arrow[d, dotted, dash, "B"] \\ u' \arrow[r, dotted, "R,B"'] & v' \end{tikzcd}$$

4. **Strict Local Coherence**. This property also relates $\to_{R,B}$ to itself, but is easier to check because it uses $\leftrightarrow_B$ instead of $=_B$ in its universal part (the existential part still uses $=_B$).

$$\begin{tikzcd} u \arrow[r, "R,B"'] \arrow[d, leftrightarrow, "B"'] & v \arrow[d, dotted, dash, "B"] \\ u' \arrow[r, dotted, "R,B"'] & v' \end{tikzcd}$$

Theorem 1. *The above four properties are equivalent.*

Proof. Since $R, B \subseteq R/B$, $= \subseteq =_B$, and $\leftrightarrow_B \subseteq =_B$, we obviously have (2) $\Rightarrow$ (1), (2) $\Rightarrow$ (3) and (3) $\Rightarrow$ (4). The implication (1) $\Rightarrow$ (2) follows directly from the relational identity $R/B = (=_B; R/B)$. Since $=_B$ is the reflexive-transitive closure of $\leftrightarrow_B$, the implication (4) $\Rightarrow$ (3) follows easily by induction on the lenght of the chain of $\leftrightarrow_B$ steps. The proof that (3) $\Rightarrow$ (2) is summarized in the diagram below.

$$\begin{tikzcd}
u \arrow[rrr, "R/B"] \arrow[dd, equal, "B"'] \arrow[dr, equal, "B"'] & & & v \arrow[dd, dotted, no head, "B"] \\
& w \arrow[r, "R"'] \arrow[d, phantom, "(2)"] & w' \arrow[ur, equal, "B"] \arrow[dr, dotted, no head, "B"] & \\
u' \arrow[ur, equal, "B"] \arrow[rrr, dotted, "R{,}B"'] & {} & & v'
\end{tikzcd}$$

$\square$

The above theorem has as an immediate consequence the *equi-termination*[5] of $\to_{R/B}$ and $\to_{R,B}$.

Corollary 1. *Under any of* (1)–(4), $\to_{R/B}$ *terminates iff* $\to_{R,B}$ *terminates.*

Proof. Since $R, B \subseteq R/B$, the ($\Rightarrow$) part is obvious. To prove the ($\Leftarrow$) part, assume that $\to_{R,B}$ terminates but $\to_{R/B}$ does not, so that we have an infinite sequence

$$t_0 \to_{R/B} t_1 \to_{R/B} t_2 \dots t_n \to_{R/B} t_{n+1} \dots$$

because of the **Bisimulation** property we then obtain an infinite sequence

$$t_0 \to_{R,B} t'_1 \to_{R,B} t'_2 \dots t'_n \to_{R,B} t'_{n+1} \dots$$

with $t_i =_B t'_i$, contradicting the termination of $\to_{R,B}$. $\square$

Another important consequence of the above theorem is that the relation $\to_{R,B}$ can be *directly* used to rewrite in equivalence classes, since **Completeness** gives us the equivalence:

$$[t]_B \to_{R/B} [t']_B \quad \Leftrightarrow \quad (\exists u)\ t \to_{R,B} u \ \wedge\ u =_B t'.$$

In the standard interpretation of $\to_{R,B}$ (more on this in the discussion below), if R finite and unconditional and there is a finitary B-matching algorithm, the set of $u's$ such that $t \to_{R,B} u$ is finite and can be effectively computed. Therefore, one can effectively describe the finite set of one-step rewrites $[t]_B \to_{R/B} [t']_B$ from $[t]_B$.

[5] For the concrete instances of $\to_{R/B}$ and $\to_{R,B}$ where R is a set of unsorted and unconditional rewrite rules, B is (the substitution closure of) a set of regular linear equations, and $\to_{R,B}$ is given the standard interpretation (more on this below), their equi-termination under the **Completeness** assumption has been proved in [16].

2.1. Discussion

The motivation behind the above four equivalent notions of *strict coherence* is twofold: (i) they are in practice the right notions for rewriting with rules R modulo a set B of *regular and linear* equations; and (ii) if one drops from B either the linearity or the regularity requirements, then various serious anomalies make rewriting modulo B highly problematic.

An equation $u = v$ is *regular* iff $\mathcal{V}ar(u) = \mathcal{V}ar(v)$, that is, both sides have the exact same variables. A term t is *linear* iff each of its variables occurs only once (at a single position) in t. An equation $u = v$ is *linear* iff both u and v are linear. The nilpotency equation $x * x = 0$ is neither regular nor linear.

Suppose that B has a non-regular equation $u = v$ with, say, $x \in \mathcal{V}ar(v) - \mathcal{V}ar(u)$ and with $n \geq 1$ occurrences of x in v. Let $l \to r$ be *any* rewrite rule in R. Then the relation $\to_{R/B}$ is non-terminating, since we have the looping rewrite $u \to^n_{R/B} u$ given by:

$$u =_B v(x \mapsto l) \to^n_R v(x \mapsto r) =_B u.$$

where $(x \mapsto l)$ denotes the obvious substitution of x by l. This makes rewriting modulo non-regular equations B hopeless in practice.

Even assuming regularity, non-linearity has also adverse consequences. The *standard* definition of $t \to_{R,B} t'$ is that there is a position p in t, a rule $l \to r$ in R and a substitution θ such that $t_p =_B l\theta$, and then $t' = t[r\theta]_p$. That is, t' is obtained by replacing t_p by $r\theta$ in t at position p (for more details see Sections 3.1–3.2). The first immediate consequence is that $\to_{R,B}$ can no longer *bisimulate* $\to_{R/B}$, so that we can no longer use $\to_{R,B}$ to efficiently achieve the effect of rewriting in B-equivalence classes. Consider, for example, an equation $u = v$ where x occurs once in u but $n > 1$ times in v. Let $l \to r$ be a rewrite rule in R, and consider the term $v(x \mapsto l)$. We obviously have $v(x \mapsto l) \to_{R/B} v(x \mapsto r)$, since we have

$$v(x \mapsto l) =_B u(x \mapsto l) \to_R u(x \mapsto r) =_B v(x \mapsto r)$$

but with $\to_{R,B}$ in general we may need to take $n > 1$ steps to get $v(x \mapsto l) \to^n_{R,B} v(x \mapsto r)$, so that **Bisimulation** is lost, and with it the ability to use $\to_{R,B}$ to get the effect of rewriting on B-equivalence classes. For example, for $B = \{f(x) \cdot f(x) = f(x)\}$ and $R = \{a \to b\}$, we have $f(a) \cdot f(a) \to_{R/B} f(b) \cdot f(b)$, but we only have $f(a) \cdot f(a) \to^2_{R,B} f(b) \cdot f(b)$.

What is worse, if linearity is dropped, *equi-termination* no longer holds. Consider, for example, B consisting of a single idempotency equation $x \cdot x = x$, and R having the single rule $a \to b$. Since the equation and the rule have no symbols in common, this rule is *coherent* in the sense of [21]. Note that the relation $\to_{R,B}$ is *terminating*, since the number of occurrences of a in a term decreases at least by 1 each time it is used, and $\to_{R,B}$ cannot be applied to a term unless some a occurs in it. However, $\to_{R/B}$ is non-terminating, as witnessed by the sequence:

$$a =_B a \cdot a \to_R b \cdot a =_B b \cdot (a \cdot a) \to_R b \cdot (b \cdot a) =_B b \cdot (b \cdot (a \cdot a)) \to_R \ldots$$

All the above-mentioned anomalies are well-known. In fact, many things can go wrong in the non-regular and/or non-linear cases. For good sources of "counterexamples" that show how unreliable one's intuition can be in such treacherous waters see, e.g., [35, 23].

Rewriting modulo B for general sets of equations B, and the relations $\to_{R/B}$ and $\to_{R,B}$, have been thoroughly studied (see, e.g., [37, 21, 3, 22]), and to deal with general sets of equations B more general notions of coherence and local coherence have been proposed, e.g., in [20, 21]. All the just-mentioned treatmens are unconditional. In Section 3 I generalize rewriting modulo B (with no restrictions on B) to *conditional order-sorted* rewrite theories. However, for all the reasons mentioned above about the difficulties with non-regular and/or non-linear axioms B, in Sections 4, 5, and parts of Section 6, I focus on the simpler and much better behaved case of equations B that are both regular and linear. This seems to be the most practical case. Yet, except for [37] and a few papers afterwards, e.g., [16, 12, 13], it seems comparatively less studied.

3. Conditional Order-Sorted Rewriting Modulo Axioms

In this section, rewriting modulo B is generalized, in *two* orthogonal dimensions, to rewriting modulo B in conditional order-sorted rewrite theories. The first dimension of generality has to do with typing. Most treatments of rewriting deal with the unsorted case. This is a *special case* of many-sorted rewriting, which, in turn, is a *special case* of order-sorted rewriting. The obvious logical asymmetry is that *all* results about order-sorted rewriting apply automatically to many-sorted and unsorted rewriting, but *not conversely.* Since most applications to declarative programming and algebraic specification are typed, this makes unsorted treatments unusable in practice for such applications, so that the extra generality is not at all an extravagant caprice but a necessity. The second dimension of generality consists in allowing rewrite rules R that are *conditional* and of the most general kind possible[6] —namely (the natural generalization of) oriented 4-CTRSs [36]. Except for [31, 4, 6, 13], all treatmens of equational rewriting I am aware of deal only with unsorted and unconditional rewriting. This makes such treatments unusable in practice for conditional theories. In fact, conditional rewriting substantially increases the expressive power of a language and is for this reason supported by all the well-known rewriting-based languages such as OBJ [18], ASF+SDF [40], ELAN [5], CafeOBJ [15] and Maude [7].

[6] I give in Section 6.2 additional results that apply to the —also very general, but with much better executability properties— special case of (the natural generalization of) strongly deterministic 3-CTRSs [36], whose rules can have extra variables in their condition and right-hand side, but they are instantiated incrementally by matching in the process of solving the condition.

3.1. Preliminaries on Order-Sorted Signatures, Terms and Equations

I follow the standard terminology and notation of term rewriting (see, e.g., [36, 2, 9, 39, 8]) and order-sorted algebra [17, 32], Readers familiar with such terminology and notation can skip this section and proceed to Section 3.2. Let me recall the notions of order-sorted signature, term, substitution and equation. An order-sorted signature $(\Sigma, S, \leq)$ consists of a poset of sorts $(S, \leq)$ and an $S^* \times S$-indexed family of sets $\Sigma = \{\Sigma_{s_1 \ldots s_n, s}\}_{(s_1 \ldots s_n, s) \in S^* \times S}$ of function symbols. Throughout, Σ is assumed to be *preregular*, so that each term t has a least sort, denoted $ls(t)$ (see [17]). Σ is also assumed to be *kind-complete*, that is, for each sort $s \in S$ its connected component in the poset $(S, \leq)$ has a top sort, denoted $[s]$, and for each $f \in \Sigma_{s_1 \ldots s_n, s}$ there is also an $f \in \Sigma_{[s_1] \ldots [s_n], [s]}$. An order-sorted signature can always be extended to a kind-complete one. Maude automatically checks preregularity and adds a new "kind" sort $[s]$ at the top of the connected component of each sort $s \in S$ specified by the user, and automatically lifts each operator to the kind level. Finally, Σ is also assumed to be *sensible*, in the sense that for any two typings $f : s_1 \ldots s_s \longrightarrow s$ and $f : s'_1 \ldots s'_s \longrightarrow s'$ of an n-argument function symbol f, if s_i and s'_i are in the same connected component of $(S, \leq)$ for $1 \leq i \leq n$, then s and s' are also in the same connected component; this provides the right notion of *unambiguous* signature at the order-sorted level.

Given an S-sorted set $\mathcal{X} = \{\mathcal{X}_s\}_{s \in S}$ of *mutually disjoint* countably infinite sets of variables, $\mathcal{T}_\Sigma(\mathcal{X})_s$ denotes the set of Σ-terms of sort s with variables in $\mathcal{X}$, and $\mathcal{T}_\Sigma(\mathcal{X})$ denotes, ambiguously, both the S-sorted set of all Σ-terms with variables in $\mathcal{X}$, and the free Σ-algebra on those variables. Similarly, $\mathcal{T}_\Sigma$ denotes both the S-sorted set of all *ground* Σ-terms that have no variables, and the initial Σ-algebra. Σ is said to have *non-empty sorts* iff $\mathcal{T}_{\Sigma,s} \neq \emptyset$ for each sort s. $\mathcal{V}ar(t)$ denotes the set of variables appearing in term t. A *substitution* is an S-sorted mapping $\sigma : \mathcal{X} \longrightarrow \mathcal{T}_\Sigma(\mathcal{X})$. We define its *domain*, denoted $dom(\sigma)$, as the set $dom(\sigma) = \{x \in \mathcal{X} \mid \sigma(x) \neq x\}$. The homomorphic extension $\sigma : \mathcal{T}_\Sigma(\mathcal{X}) \longrightarrow \mathcal{T}_\Sigma(\mathcal{X})$ is also denoted σ, and its application to a term t is denoted $t\sigma$. $\mathcal{P}(t)$ denotes the set of positions of a Σ-term t, and t_p denotes the *subterm of* t *at position* $p \in \mathcal{P}(t)$. Similarly, $\mathcal{P}_\Sigma(t)$ denotes the *non-variable positions* of t, that is, those $p \in \mathcal{P}(t)$ such that $t_p \notin \mathcal{V}ar(t)$. A term t with its subterm t_p replaced by the term t' is denoted by $t[t']_p$.

For a Σ-equation $u = v$ to be well-formed, the sorts of u and v should be in the same connected component of $(S, \leq)$. For B a set of Σ-equations, $=_B$ denotes the provable B-equality relation [17, 32], and $[t]_B$ denotes the equivalence class of t modulo $=_B$. Given a set of Σ-equations B, a substitution σ is a B-*unifier* of an equation $t = t'$ iff $t\sigma =_B t'\sigma$; let $MGU_B(t = t')$ denote a complete set of most general B-unifiers. Likewise, a substitution σ is a B-*match* from t to t' iff $t' =_B t\sigma$. Since the practical interest is in implementable uses of rewriting modulo B, from Section 4 onwards I will assume that B has a finitary B-matching algorithm; that is, an algorithm generating a complete finite set of B-matches from t to t', denoted $Match_B(t, t')$; that is, for any B-match σ there is a $\tau \in Match_B(t, t')$ such that for all $x \in \mathcal{V}ar(t)$ $\sigma(x) =_B \tau(x)$.

An equation $u = v$ is called *sort-preserving* iff for each well-sorted substitution θ we have $ls(u\theta) = ls(v\theta)$. Using substitutions that specialize variables to smaller sorts it can be easily checked whether an equation is sort-preserving.

3.2. Conditional Order-Sorted Rewriting Modulo B

I develop in detail the semantics of conditional order-sorted rewriting modulo axioms B. Since the goal is to define such rewriting in full generality, *no assumptions are made on* B in this section. However, in Section 4 various assumptions on B, including regularity and linearity, will be explicitly stated. The key notion is that of a *conditional order-sorted rewrite theory*, that is, a triple $\mathcal{R} = (\Sigma, B, R)$, with Σ an order-sorted signature, B a set of Σ-equations, and R a set of conditional rewrite rules of the form $l \to r \ \mathit{if} \ \bigwedge_{i=1..n} u_i \to v_i$, with *no restrictions* on the variables of l, r, or those of the u_i and v_i.

The meaning of $\mathcal{R} = (\Sigma, B, R)$ *need not be equational*; that is, the rules R need not be understood as conditional equations that have been oriented as rewrite rules. Of course for some applications R *can* be understood equationally; for example, Maude's *functional modules* [7] are conditional equational theories that are executed as conditional rewrite theories $\mathcal{R} = (\Sigma, B, R)$ by rewriting modulo B. I further discuss the equational meaning of conditional order-sorted rewrite theories in Section 6. However, in many other applications $\mathcal{R} = (\Sigma, B, R)$ specifies a *concurrent system* whose states are B-equivence classes $[t]_B$ with t a ground Σ-term [31]. The rules R then specify the possible concurrent transitions of such a system. Maude's *system modules* [7] give such a concurrent system semantics to a theory $\mathcal{R} = (\Sigma, B, R)$, which may, for example, specify the semantics of a concurrent programming language, a process calculus, a network protocol, or a cyber-physical or cell biology system [33].

Something not entirely obvious is how the rewrite relations $\to_{R/B}$ and $\to_{R,B}$ should be *defined* for a conditional rewrite theory $\mathcal{R} = (\Sigma, B, R)$. As explained below, the naive generalization of the unconditional relations would actually be wrong. The most satisfactory way is by means of *inference systems*. Here is the inference system[7] defining both $\to_{R/B}$ and $\to^\star_{R/B}$ when Σ has non-empty sorts.

- **Reflexivity**. For each $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$ such that $t =_B t'$, $\dfrac{}{t \to^\star_{R/B} t'}$
- **Replacement**. For $l \to r \ \ \mathit{if} \ \ u_1 \to v_1 \wedge \ldots \wedge u_n \to v_n$ a rule in R, $t, u, u \in \mathcal{T}_\Sigma(\mathcal{X})$, $p \in \mathcal{P}(t)$, and θ a substitution, such that $u =_B t[l\theta]_p$ and $v =_B t[r\theta]_p$,

$$\frac{u_1\theta \to^\star_{R/B} v_1\theta \quad \ldots \quad u_n\theta \to^\star_{R/B} v_n\theta}{u \to_{R/B} v}$$

[7]Modulo the fact that the relations $\to_{R/B}$ and $\to^\star_{R/B}$ are combined into a single relation, denoted $\to$, the inference system given here can easily be proved equivalent to the rewriting logic inference system in [31] (which works directly with B-equivalence classes) for the unsorted case, and to the generalized rewriting logic inference system in [6] when order-sorted equational logic is viewed as a sublogic of membership equational logic.

- **Transitivity** For $t_1, t_2, t_3 \in \mathcal{T}_\Sigma(\mathcal{X})$,

$$\frac{t_1 \rightarrow_{R/B} t_2 \qquad t_2 \rightarrow^{\star}_{R/B} t_3}{t_1 \rightarrow^{\star}_{R/B} t_3}$$

In general, the relation $u \rightarrow_{R/B} v$ may be undecidable, since checking whether $u \rightarrow_{R/B} v$ holds involves searching through the possibly infinite equivalence class $[u]_B$ to find a representative that can be rewritten with R and checking, furthermore, that the result u' of such rewriting belongs to the equivalence class $[v]_B$. For this reason, and for greater efficiency, a much simpler relation $\rightarrow_{R,B}$ is defined, which in the unconditional case becomes decidable for R finite if a finitary B-matching algorithm exists. However, in the conditional case, even with such a B-matching algorithm, the relation $\rightarrow_{R,B}$ may still be undecidable due to the general undecidability of reachability by rewriting. As already mentioned, the key idea about $\rightarrow_{R,B}$ is to replace general B-equalities of the form $u =_B t[l\theta]_p$ by a matching B-equality $t_p =_B l\theta$ with the subterm actually being rewritten. This completely eliminates any need for searching for a redex in the possibly infinite equivalence class $[u]_B$. Here is the inference system defining both $\rightarrow_{R,B}$ and $\rightarrow^{\star}_{R,B}$ when Σ has non-empty sorts.

- **Reflexivity**. For each $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$ such that $t =_B t'$, $\quad \dfrac{}{t \rightarrow^{\star}_{R,B} t'}$
- **Replacement**. For $l \rightarrow r \;\; \mathit{if} \;\; u_1 \rightarrow v_1 \wedge \ldots \wedge u_n \rightarrow v_n$ a rule in R, $t \in \mathcal{T}_\Sigma(\mathcal{X})$, $p \in \mathcal{P}(t)$, and θ a substitution, such that $t_p =_B l\theta$,

$$\frac{u_1\theta \rightarrow^{\star}_{R,B} v_1\theta \quad \ldots \quad u_n\theta \rightarrow^{\star}_{R,B} v_n\theta}{t \rightarrow_{R,B} t[r\theta]_p}$$

- **Transitivity** For $t_1, t_2, t_3 \in \mathcal{T}_\Sigma(\mathcal{X})$,

$$\frac{t_1 \rightarrow_{R,B} t_2 \qquad t_2 \rightarrow^{\star}_{R,B} t_3}{t_1 \rightarrow^{\star}_{R,B} t_3}$$

3.3. Discussion

Note that the only assumption on the conditional order-sorted rewrite theory $\mathcal{R} = (\Sigma, B, R)$ is that the conditional rules in R have *oriented conditions* and are therefore of the form $l \rightarrow r \;\mathit{if}\; \bigwedge_{i=1..n} u_i \rightarrow v_i$. When Σ is unsorted and $B = \emptyset$, such theories specialize to the notion of an *oriented 4-CTRS* [36]. A difficulty with such extremely general rewrite theories is their *infinitely-branching non-determinism*, since there can be an infinite number of possible (not B-equivalent) substitutions θ in a single application of the **Replacement** rule. However, as explained in [38], such infinitely-branching non-deterministic rewrite theories can be quite useful, since they can naturally model *open-concurrent systems*, and can become executable using constrain-solving methods. In Section 6.2, a still very general —yet easily executable— notion of rewrite theory, is discussed. It generalizes the notion of *deterministic 3-CTRS* [36].

Although quite simple, the two inference systems above hide some subtleties worth explaining. They have to do with the claim made above that the naive generalization of the unconditional relations $\rightarrow_{R/B}$, $\rightarrow^*_{R/B}$, $\rightarrow_{R,B}$ and $\rightarrow^*_{R,B}$ would actually be wrong. The two key observations are the following:

1. In standart treatments of unconditional rewriting modulo B, e.g., [21, 3], the relations $\rightarrow^*_{R/B}$ and $\rightarrow^*_{R,B}$ are defined in the *standard sense*, that is, as the *reflexive-transitive* closures of the respective relations $\rightarrow_{R/B}$ and $\rightarrow_{R,B}$.

2. However, in the above two inference systems the relations $\rightarrow^\star_{R/B}$ and $\rightarrow^\star_{R,B}$ are *not* the reflexive-transitive closures of the respective relations $\rightarrow_{R/B}$ and $\rightarrow_{R,B}$. The perceptive reader may have noticed that I use Latex's `\star` simbol for $\rightarrow^\star$, as opposed to the `\ast` simbol typically used for the reflexive-transitive closure $\rightarrow^*$, to mark, unobtrusively, the subtle difference. What we actually have (see Fact (2) in Remark 1 below) is $\rightarrow^\star_{R/B} = (\rightarrow^*_{R/B}; =_B)$, and $\rightarrow^\star_{R,B} = (\rightarrow^*_{R,B}; =_B)$. That is, the B-equality relation $=_B$ is further composed in both cases because of the corresponding **Reflexivity** rule. And this is *crucial* for the **Replacement** rules to work correctly.

I call $\rightarrow^\star_{R/B}$ (resp. $\rightarrow^\star_{R,B}$) the *R/B-reachability relation* (resp. the the *R,B-reachability relation*), because that is exactly what these relations are when we view the terms $t \in \mathcal{T}_\Sigma(\mathcal{X})$ as descriptions of *states* of a system satisfying structural axioms B.

Following the standard approach to conditional rewriting (see, e.g., [36]), the *naive* generalization of rewriting modulo B to the conditional case would proceed as follows. One would define $\rightarrow_{R/B}$ as the union $\rightarrow_{R/B} = \bigcup_n \rightarrow_{R/B,n}$, where $\rightarrow_{R/B,0} = \emptyset$, and for each $n \in \mathbb{N}$, we have $\rightarrow_{R/B,n+1} = \rightarrow_{R/B,n} \cup \{(u,v) \mid u =_B l\sigma \ \rightarrow \ r\sigma =_B v \wedge l \rightarrow r \ \mathit{if} \ \bigwedge_i u_i \rightarrow v_i \in R \wedge \forall i, u_i\sigma \rightarrow^*_{R/B,n} v_i\sigma\}$, where $\rightarrow^*_{R/B,n}$ of course denotes the reflexive-transitive closure. The naive definition of $\rightarrow_{R,B}$ would be entirely analogous. That these are the *wrong* definitions can be illustrated with a simple example.

Example 1. *Consider an unsorted signature with constants a, b, c, unary function symbol f and binary operator $\_\cdot\_$ and let B consist of the commutativity axiom $x \cdot y = y \cdot x$. Let R have just the single conditional rule $f(x \cdot f(y)) \rightarrow c$ if $x \cdot y \rightarrow z \cdot a$. Since f is different from $\_\cdot\_$, this rule is coherent and, indeed, as we shall see in Section 4, strictly coherent. If we were to adopt the above, naive definitions of $\rightarrow_{R/B}$ and $\rightarrow_{R,B}$, the term $f(a \cdot f(b))$ would actually be* irreducible *modulo B. This is because the term $a \cdot b$ that has to be tested in the condition is obviously irreducible modulo B. But for any irreducible term t, if $t \rightarrow^*_{R/B} t'$ and $\rightarrow^*_{R/B}$ is the reflexive-transitive closure of $\rightarrow_{R/B}$, then we must have $t = t'$. Thefore, from $a \cdot b$ we can* never *reach with the reflexive-transitive* *closure* $\to^*_{R/B}$ *any instance of the term* $z \cdot a$*, even if we make the "right" choice and instantiate* z *to* b*.*

This clearly shows that the above, naive definition is wrong. In fact, the term $f(a \cdot f(b))$ *is* reducible to c, since its condition is satisfied in 0 steps by $a \cdot b$ matching modulo commutativity the pattern $z \cdot a$ with matching substitution $z \mapsto b$. Here is, for example, a trace of the execution given by Maude, where `comm` declares the commutativity axiom.

```
mod APORIA is
  sort U .
  ops a b c : -> U .
  op f : U -> U .
  op _._ : U U -> U [comm] .
  vars x y z : U .
  crl f(x . f(y)) => c if x . y => z . a .
endm

Maude> set trace on .
Maude> rewrite f(a . f(b)) .
*********** trial #1
crl f(x . f(y)) => c if x . y => a . z .
x --> a
y --> b
z --> (unbound)
*********** solving condition fragment
x . y => a . z
*********** success for condition fragment
x . y => a . z
x --> a
y --> b
z --> b
*********** success #1
*********** rule
crl f(x . f(y)) => c if x . y => a . z .
x --> a
y --> b
z --> b
f(a . f(b))
--->
c
rewrites: 1 in 0ms cpu (0ms real) (2506 rewrites/second)
result U: c
```

In summary, the key point is that the satisfaction of a rule's condition requires *search*, to see whether each $u_i\theta_{i-1}$ can *reach* an instance $v_i\theta_i$ of the pattern v_i. For this, the above **Reflexivity** rules are crucial in two related ways. First, to be able to reach terms in 0 steps, as the above example illustrates. Second, in the case of the $\to^\star_{R,B}$ relation, to reach the terms $v_i\theta_i$ from $u_i\theta_{i-1}$ in n steps, since for $n \geq 1$ the n-step relation $\rightarrow^n_{R,B}$ will typically rewrite $u_i\theta_{i-1}$ to a term w_i such that we only have $w_i =_B v_i\theta_i$, and we need a last use of **Reflexivity** (always required by the **Transitivity** rule) to close the gap $w_i =_B v_i\theta_i$.

Remark 1. *The easy proof of the following facts is left to the reader:*

1. $\rightarrow_{R/B} \subseteq \rightarrow^\star_{R/B}$, *and* $\rightarrow_{R,B} \subseteq \rightarrow^\star_{R,B}$.
2. $u \rightarrow^\star_{R/B} v$ *holds iff there is a chain of* $n \geq 0$ *rewrite steps followed by a* B*-equality step of the form* $u \rightarrow_{R/B} u_1 \rightarrow_{R/B} u_2 \dots u_{n-1} \rightarrow_{R/B} u_n =_B v$. *And* $u \rightarrow^\star_{R,B} v$ *holds iff there is a chain of* $n \geq 0$ *rewrite steps followed by a* B*-equality step of the form* $u \rightarrow_{R,B} u'_1 \rightarrow_{R,B} u'_2 \dots u'_{n-1} \rightarrow_{R,B} u'_n =_B v$.
3. $(\rightarrow^\star_{R/B}; \rightarrow^\star_{R/B}) \subseteq \rightarrow^\star_{R/B}$.

In general the reachability relation $\rightarrow^\star_{R,B}$ is *not* transitive; that is, we do not have $(\rightarrow^\star_{R,B}; \rightarrow^\star_{R,B}) \subseteq \rightarrow^\star_{R,B}$. For a simple counterexample consider an unsorted signature with constants a, b, c and a binary AC symbol $\_ \cdot \_$, and R with just one unconditional rule $a \cdot b \rightarrow c$. Then we have

$$(b \cdot a) \cdot ((c \cdot a) \cdot b) \rightarrow_{R,AC} c \cdot ((c \cdot a) \cdot b) =_{AC} (b \cdot a) \cdot (c \cdot c) \rightarrow_{R,AC} c \cdot (c \cdot c).$$

Therefore, $((b\cdot a)\cdot((c\cdot a)\cdot b), c\cdot(c\cdot c)) \in (\rightarrow^\star_{R,AC}; \rightarrow^\star_{R,AC})$. But since $c\cdot((c\cdot a)\cdot b)$ is irreducible by $\rightarrow_{R,AC}$, Fact (2) above ensures $((b\cdot a).((c\cdot a)\cdot b), c\cdot(c\cdot c)) \notin \rightarrow^\star_{R,AC}$.

4. Strict Coherence of Conditional Order-Sorted Rewrite Theories

Although the semantics of conditional ordered-sorted rewriting modulo B has been defined in Section 3.2 with no restrictions on B, as mentioned in Section 2.1, non-linear and/or non-regular axioms B can cause serious anomalies. For this reason, throughout this section in which strict coherence is studied, the equational axioms B in a rewrite theory $\mathcal{R} = (\Sigma, B, R)$ will always be regular, linear, sort-preserving, with $=_B$ decidable, have a finitary B-matching algorithm, and be *most general possible*, in the sense that for any $u = v \in B$, each $x \in \mathcal{V}ar(u = v)$ has a "kind" sort $[s]$ at the top of one the connected components in $(S, \leq)$. B being sort-preserving is extremely useful for performing *order-sorted* rewriting modulo B: when B-matching a subterm t_p against a rule's lefthand side to obtain a matching substitution σ, we need to check that σ is well-sorted, that is, that if a variable x has sort s, then some element in the B-equivalence class $[x\sigma]_B$ has also sort s. But since B is sort-preserving, this is equivalent to checking $ls(x\sigma) \leq s$. Of course, in the many-sorted and unsorted cases sort-preservation and greatest possible generality of the equations B are always satisfied, and all the assumptions on Σ boil down to Σ being unambiguous.

The main goal of this section is to show that strict coherence of the rules R in a conditional order-sorted rewrite theory $\mathcal{R} = (\Sigma, B, R)$ is the key notion to bisimulate the relation $\rightarrow_{R/B}$ by means of the much simpler and much more efficient relation $\rightarrow_{R,B}$, and to develop methods of *strict coherence completion* that can try to transform $\mathcal{R}$ into a semantically equivalent theory that is strictly coherent. For this, the notion of rule B-extension plays a key role.

4.1. B-Extensions of Conditional Rules

In the usorted and unconditional case, a useful technique to achive coherence modulo B for a set of rewrite rules R is to *extend* the rules R by suitable contexts obtained from the terms in the axioms B. This technique goes back to Peterson and Stickel [37], who introduced the notion of extension, considered the case where B is regular and linear (their Theorem 9.5), and proved that a finite set of extensions suffice when B is any combination of associtivity (A), commutativity (C), and associativity-commutativity (AC) axioms (their Theorem 10.5). The technique has been generalized to arbitrary sets of axioms B, e.g., [21, 3]. One attractive feature is its simplicity. An alternative, more complex approach is to attempt some kind of completion based on suitable "critical pairs" between axioms and rules in the style of, e.g., [16]; but the number of B-unifiers between two terms may be infinite for some B. Instead, the technique of extensions only relies on a B-*unifiability* algorithm.

Since —except for [4], who does not treat B-extensions at all— all the treatments I am aware of deal only with *unconditional* rules, a nontrivial question is how to adequately generalize the notion of rule B-extension to the order-sorted and conditional case. This I do in Definition 1 below.

Let me begin by recalling the very simple notion of B-extension in the unconditional case. Given an unconditional rule $l \to r$ and axioms B, its B-*extensions* are all rules of the form $u[l]_p \to u[r]_p$ such that either $u = v$ or $v = u$ is in B, and where p is a non-variable and non-top (i.e., $p \neq \epsilon$) position of u such that u_p and l are B-*unifiable* (note, however, that no B-unifier is computed to build the extension). The variables of u and l are always renamed if needed to ensure that u and l have no variables in common. The extended rules can themselves be extended; however, for certain axioms B, such as any combination of A, C, and identity (U) axioms, it is easy to show that the extension process reaches a fixpoint in at most two steps, in the sense that any newly generated extensions are all *instances* modulo B of previously generated rules (for combinations of A and C this is the already-mentioned Theorem 9.5 in [37]).

As in the unconditional and unsorted case, the key notions in their conditional order-sorted generalization are those of B-extension and B-subsumption.

Definition 1. *Let $\mathcal{R} = (\Sigma, B, R)$ be a conditional order-sorted rewrite theory, and let $l \to r$ if C be a rule in R, where C abbreviates the rule's condition. Without loss of generality we assume that $\mathcal{V}ar(B) \cap \mathcal{V}ar(l \to r \textit{ if } C) = \emptyset$. If this is not the case,* only the variables of B *will be renamed; the variables of $l \to r$ if C will* never *be renamed. We then define the set of B-*extensions *of $l \to r$ if C as the set*[8]*:*

$$Ext_B(l \to r \textit{ if } C) = \{u[l]_p \to u[r]_p \textit{ if } C \mid u = v \in B \cup B^{-1} \wedge p \in \mathcal{P}_\Sigma(u) - \{\epsilon\} \wedge MGU_B(l, u_p) \neq \emptyset\}$$

[8]Note that, because of the assumptions that Σ is kind-complete and that all $u = v \in B$ are most general possible and have variables whose sorts are tops of connected components in the sort poset $(S, \leq)$, the terms $u[l]_p$ and $u[r]_p$ are always well-formed Σ-terms.

where, by definition, $B^{-1} = \{v = u \mid u = v \in B\}$*.*

Given two rules $l \to r$ *if* C *and* $l' \to r'$ *if* C *with the* same *condition* C *we say that* $l \to r$ *if* C B-subsumes[9] $l' \to r'$ *if* C *iff there is a substitution* σ *such that: (i)* $dom(\sigma) \cap \mathcal{V}ar(C) = \emptyset$*, (ii)* $l' =_B l\sigma$*, and (iii)* $r' =_B r\sigma$*.*

I now describe in detail an algorithm to try to compute the B-*extension closure* $\overline{Ext}_B(l \to r \textit{ if } C)$ of a conditional rule $l \to r \textit{ if } C$. To avoid non-determinism, I assume that: (i) the set U of all terms u such that $u = v \in B \cup B^{-1}$ has been linearly ordered. I also assume that for each $u \in U$ the non-variable and non-top positions of u have been linearly ordered. Call such positions *usable* positions. The algorithm maintains two queues, one of *extended* rules (i.e., rules whose extensions have already been computed), and another of *generated* rules (i.e., rules generated by the extension process). Initially the queue of extended rules is empty and that of generated rules holds the original rule $l \to r \textit{ if } C$. Note that, by construction, all rules in the queues will always have the exact same condition C. The algorithm repeatedly performs the following sequence of steps until the queue of generated rules is empty.

1. If the queue of generated rules is empty **stop**; otherwise, let $l' \to r' \textit{ if } C$ be the first rule in it.
2. Sequentially (according to the linear order of U and of u's positions), for each $u \in U$ and usable position p, if l' and u_p are B-unifiable, do the following:
   - Generate the extension $u[l']_p \to u[r']_p \textit{ if } C$.
   - If $u[l']_p \to u[r']_p \textit{ if } C$ is B-subsumed by any rule in either of the queues, discard it; otherwise, append it at the end of the queue of generated rules.
3. Once all the terms in U and all usable positions in each $u \in U$ have been tried, dequeue the rule $l' \to r' \textit{ if } C$ and append it at the end of the queue of extended rules.

If after repeating the above loop n times the queue of generated rules becomes empty, the set $\overline{Ext}_B(l \to r \textit{ if } C)$ contains all rules in the queue of extended rules. If the queue of generated rules never becomes empty, we can still think of $\overline{Ext}_B(l \to r \textit{ if } C)$ as the infinite set of all rules ever added to the queue of extended rules.

As a further optimization, one can discard from $\overline{Ext}_B(l \to r \textit{ if } C)$ any rule that is B-subsumed by any other rule. For example, if $B = AU$ for the unsorted binary operator $\_\cdot\_$ and constants a, b, c, we have (disregarding parentheses):

$$\overline{Ext}_{AU}(a \cdot b \to c) = \{a \cdot b \to c,\ x \cdot a \cdot b \to x \cdot c,\ a \cdot b \cdot y \to c \cdot y,\ x \cdot a \cdot b \cdot z \to x \cdot c \cdot z\}$$

[9] Note that for unconditional rules, since C is empty, we have $var(C) = \emptyset$, so that requirement (i) trivially holds for σ. Therefore, the conditional notion of subsumption yields the usual unconditional notion as a special case.

but all rules are AU-subsumed by the last rule $x \cdot a \cdot b \cdot z \to x \cdot c \cdot z$.

Given a conditional order-sorted rewrite theory $\mathcal{R} = (\Sigma, B, R)$, let its B-*extension closure* be the theory $\overline{Ext}_B(\mathcal{R}) = (\Sigma, B, \overline{R})$, where

$$\overline{R} = \bigcup_{(l \to r \ \mathit{if}\ C) \in R} \overline{Ext}_B(l \to r \ \mathit{if}\ C).$$

This theory always exists, but can be infinite if the B-extension closure of any rule in R is infinite.

Is there an algorithm to check whether a conditional theory is already closed under B-extensions? Yes, this is just a B-subsumption check. That is, we *define* $\mathcal{R} = (\Sigma, B, R)$ to be *closed under B-extensions* iff any B-extension of any rule in R is B-subsumed by some rule in R. The notion of "closed under B-extensions" could be broadened by adopting a more relaxed notion of B-subsumption that would, for example, allow a rule like $(a \cdot b) \cdot x \to c \cdot x \ \mathit{if}\ x > 0 \to \mathit{true}$ to B-subsume the rule $a \cdot (b \cdot y) \to c \cdot y \ \mathit{if}\ y > 0 \to \mathit{true}$, where $a, b, 0$ and *true* are constants, and $\_ \cdot \_$ is A or AC. To keep technicalities to a minimum, I will not pursue here the details of such a broadening.

4.2. Strictly Coherent Conditional Theories

As one would expect, the point of computing the extension closure $\overline{Ext}_B(\mathcal{R})$ is to obtain a strictly coherent theory. We can indeed prove a stronger result.

Theorem 2. *(Strict Local Coherence of* **Replacement** *Inferences). Let $\mathcal{R} = (\Sigma, B, R)$ be a conditional order-sorted rewrite theory where B satisfies the assumptions stated at the beginning of Section 4 and is closed under B-extensions. Then, for each instance of* **Replacement** *of the form:*

$$\frac{u_1\theta \to^{\star}_{R,B} v_1\theta \quad \ldots \quad u_n\theta \to^{\star}_{R,B} v_n\theta}{u \to_{R,B} v}$$

and each one-step B-equality proof $u \leftrightarrow_B u'$ there is another instance of **Replacement** *of the form*

$$(\dagger) \qquad \frac{u_1\theta' \to^{\star}_{R,B} v_1\theta' \quad \ldots \quad u_n\theta' \to^{\star}_{R,B} v_n\theta'}{u' \to_{R,B} v'}$$

with $v =_B v'$ and $\theta(x) = \theta'(x)$ for each $x \in \mathcal{V}ar(u_1 \to v_1 \ \wedge \ldots \wedge \ u_n \to v_n)$.

Proof. Let the above instance of **Replacement** be obtained by trying to apply[10] to u at position p with substitution θ rule $l' \to r' \ \ \mathit{if}\, C \in R$ with $C = u_1 \to v_1 \wedge \ldots \wedge u_n \to v_n$. Therefore, $u_p =_B l'\theta$ and $v = u[r'\theta]_p$. Similarly,

[10] Since this is just an inference step, in general it is *not necessarily a rule application* (which would require the condition to be provable). To make this clear, let us call applications of **Replacement** "*rule application attempts.*"

let $u \leftrightarrow_B u'$ be obtained by applying equation $w = w' \in B \cup B^{-1}$ at position q with substitution σ, so that $u_q = w\sigma$, and $u' = u[w'\sigma]_q$.

The proof is by case analysis on the positions p and q using the prefix order $p \leq q$ between positions as strings. (1) If neither $q \leq p$ nor $q > p$ the result is trivial, since $u'_p = u_p$ and $v_q = u_q$, so that we have an application of **Replacement** of the form (†) at position p with $\theta = \theta'$, $v' = u'[r'\theta]_p$, and a one-step B-equality proof $v \leftrightarrow_B v'$ at position q with $w = w'$ instantiated with σ. (2) If $q \leq p$ we have $u'_p =_B u_p =_B l'\theta$ and therefore an application of **Replacement** of the form (†) with $\theta = \theta'$ and $v' = v$. For case (3) ($q > p$) two subcases can be distinguished. Let $x_1, \ldots, x_k$ be the variables in $w = w'$, $r_1, \ldots, r_k$ their respective positions in w, and $r'_1, \ldots, r'_k$ their respective positions in w'. Then either: (i) $q.r_i \geq p$ for some $1 \leq i \leq k$, so that $p = q.r_i.s$, or (ii) $p = q.r$ for r a non-variable and non-top position in w. In case (i), $u_p = u'_{q.r'_i.s}$ and therefore we have an application of **Replacement** of the form (†) with $\theta = \theta'$ and $v' = (u[w'\sigma]_q)[r'\theta]_{q.r'_i.s}$. But this means that we have a one-step B-equality proof $v \leftrightarrow_B v'$ with $w = w'$ and substitution σ' identical to σ except for its value for x_i, which is $\sigma'(x_i) = u_{q.r_i}[r'\theta]_s$. This proves case 3.(i). In case 3.(ii), we have the identity $w_r\sigma = u_p$. Since $u_p =_B l'\theta$, w_r and l' are B-unifiable, so that (assuming as always disjoint variables between B and R) the rule $l' \to r'$ *if* C has a B-extension $w[l']_r \to w[r']_r$ *if* C. Since $\mathcal{R}$ is closed under B-extensions, either this extended rule belongs to R or is subsumed by a rule in R. I prove first the easier case where the extended rule belongs to R. Let θ' extend θ over $\mathcal{V}ar(w[l']_r \to w[r']_r \; if \; C)$ by defining for each $x \in \mathcal{V}ar(w) - vars(w_r)$ $\theta'(x) = \sigma(x)$. This gives us the equalities $u'_q =_B u_q =_B w[l']_r\theta'$ and therefore, since θ' extends θ and instantiates the variables of C in the exact same manner, we have an application of **Replacement** of the form (†) at position q, with $v' = u'[w[r']_r\theta']_q$. But, by the definition of θ' and the fact that $u' = u[u'_q]_q$, it is easy to check that we have the actual term identities $u'[w[r']_r\theta']_q = u[w[r']_r\theta']_q = u[r'\theta] = v$, thus proving the requirements for the inference step (†). This leaves us with the remaining case when there is a rule $l'' \to r''$ *if* C in R subsuming $w[l']_r \to w[r']_r$ *if* C. That is, there is a substitution τ with $dom(\tau) \cap \mathcal{V}ar(C) = \emptyset$ such that $l''\tau =_B w[l']_r$ and $r''\tau =_B w[r']_r$. But then we have $u'_q =_B u_q =_B w[l']_r\theta' =_B l''\tau\theta'$, and since $dom(\tau) \cap \mathcal{V}ar(C) = \emptyset$ and θ' extending θ, $\tau\theta'$ instantiates the variables of C in the exact same manner as θ, we have an application of **Replacement** of the form (†) at position q with $v' = u'[r''\tau\theta']_q$, and the chain of equalities $u'[r''\tau\theta']_q =_B u'[w[r']_r\theta']_q = v$, proving again the requirements for the inference step (†), as desired. □

Since a rewrite step $u \to_{R,B} v$ is just an application of **Replacement** for wich the condition can be proved, and when $u \leftrightarrow_B u'$ the similar application of **Replacement** ensured by (†) in Theorem 2 has the *same condition*, we obtain also a rewrite $u' \to_{R,B} v'$ with $v =_B v'$. That is, we obtain the **Strict Local Coherence** property of the relation $\to_{R,B}$.

An easy induction on the number of steps in an equality proof $u =_B u'$ then gives us:

Corollary 2. *(Strict Coherence of* **Replacement** *Inferences). Let $\mathcal{R} = (\Sigma, B, R)$ be a conditional order-sorted rewrite theory where B satisfies the assumptions stated at the beginning of Section 4 and is closed under B-extensions. Then, for each instance of* **Replacement** *of the form:*

$$\frac{u_1\theta \to^{\star}_{R,B} v_1\theta \quad \ldots \quad u_n\theta \to^{\star}_{R,B} v_n\theta}{u \to_{R,B} v}$$

and each B-equality proof $u =_B u'$ there is another instance of **Replacement** *of the form*

$$(\ddagger) \quad \frac{u_1\theta' \to^{\star}_{R,B} v_1\theta' \quad \ldots \quad u_n\theta' \to^{\star}_{R,B} v_n\theta'}{u' \to_{R,B} v'}$$

with $v =_B v'$ and $\theta(x) = \theta'(x)$ for each $x \in \mathcal{V}ar(u_1 \to v_1 \ \wedge \ldots \wedge \ u_n \to v_n)$. $\square$

Since a rewrite step $u \to_{R,B} v$ is just an application of **Replacement** for wich the condition can be proved, and when $u =_B u'$ the similar application of **Replacement** ensured by ($\ddagger$) in Corollary 2 has the *same condition*, we obtain also a rewrite $u' \to_{R,B} v'$ with $v =_B v'$. That is, we obtain the **Strict Coherence** property of the relation $\to_{R,B}$.

Given an order-sorted signature Σ and a set R of conditional Σ rules, we can define the relation $\to_R$, in the *standard* CTRS sense generalized to the order-sorted case, as the relation $\to_R = \to_{R/\emptyset}$ for the order-sorted conditional rewrite theory $(\Sigma, \emptyset, R)$. For $\mathcal{R} = (\Sigma, B, R)$ we then have obvious inclusions $\to_R \subseteq \to_{R,B} \subseteq \to_{R/B}$. Furthemore, if $\mathcal{R} = (\Sigma, B, R)$ is an *unconditional* order-sorted rewite theory (i.e., all rules in R have an empty condition), routine inspection of the corresponding inference systems shows that we have $\to_{R/B} = (=_B; \to_R ; =_B)$. Therefore, if $\mathcal{R}$ is unconditional and closed under B-extensions we are in the abstract setting of Section 2, and the fact that $\to_{R,B}$ satisfies the **Strict Coherence** property immediately gives us:

Corollary 3. *Let $\mathcal{R} = (\Sigma, B, R)$ be an unconditional order-sorted rewrite theory where B satisfies the assumptions stated at the beginning of Section 4 and is closed under B-extensions. Then $\mathcal{R}$ satisfies the* **Completeness***,* **Bisimulation***,* **Strict Coherence** *and* **Strict Local Coherence** *properties.*

The case when $\mathcal{R} = (\Sigma, B, R)$ is closed under B-extensions but is actually *conditional* is more subtle. One might easily think that all the abstract strict coherence results in Section 2 immediately apply to $\mathcal{R}$; but this would be a notation-induced delusion. We have indeed been using the notations $\to_{R/B}$ and $\to_{R,B}$, and we just defined above the notation $\to_R$ with its standard CTRS meaning. But these relations do not necessarily mean what they meant in Section 2. We indeed have inclusions $\to_R \subseteq \to_{R,B} \subseteq \to_{R/B}$. But what in general we do *not* have is the identity $\to_{R/B} = (=_B; \to_R; =_B)$. In fact, when $\mathcal{R}$ is not closed under B-extensions we do not even have the identity $\to_{R/B} = (=_B; \to_{R,B} ; =_B)$. Here is a simple counterexample. Consider the unsorted rewrite theory

$\mathcal{S}$ whose signature Σ has constants a, b, c, d, e and a binary AC symbol $\_ \cdot \_$ and where R has two rules: $c \cdot d \to e$, and $a \cdot b \to c$ *if* $(c \cdot a) \cdot d \to a \cdot e$. The rules R are simple enough to allow a succinct set-theoretic characterization of the relations $\to_R$, $\to_{R,AC}$, and $\to_{R/AC}$, namely:

- $\to_R = \{(u, u[e]_p) \in \mathcal{T}_\Sigma(\mathcal{X})^2 \mid p \in \mathcal{P}(u) \wedge u_p = c \cdot d\}$,
- $\to_{R,AC} = \{(u, u[e]_p) \in \mathcal{T}_\Sigma(\mathcal{X})^2 \mid p \in \mathcal{P}(u) \wedge u_p =_{AC} c \cdot d\}$, and
- $\to_{R/AC} = (=_{AC} \to_R =_{AC}) \cup \{(u', v') \in \mathcal{T}_\Sigma(\mathcal{X})^2 \mid (\exists u \in \mathcal{T}_\Sigma(\mathcal{X}))(\exists p \in \mathcal{P}(u))\ u =_{AC} u' \wedge u_p = a \cdot b \wedge v' =_{AC} u[c]_p\}$.

If follows clearly from the above set-theoretic characterizations that $\to_{R/AC} \neq (=_{AC}; \to_R; =_{AC})$ and $\to_{R/AC} \neq (=_{AC}; \to_{R,AC}; =_{AC})$. Consider now $\overline{Ext}_{AC}(\mathcal{S})$, where $\overline{R}$ is obtained by adding to R the two extension rules: $(c \cdot d) \cdot x \to e \cdot x$, and $(a \cdot b) \cdot y \to c \cdot y$ *if* $(c \cdot a) \cdot d \to a \cdot e$. We have $\to_{\overline{R}} = \to_R$, and $\to_{\overline{R}/AC} = \to_{R/AC}$. Therefore, we still have $\to_{\overline{R}/AC} \neq (=_{AC}; \to_{\overline{R}}; =_{AC})$, so how can we possibly apply the abstract strict coherence results in Section 2? We can because they are *abstract*, so that we can *choose* how to instantiate the meanings of $\leftrightarrow_B$, R, R,B, and R/B. We can choose the instantiations: $\leftrightarrow_B = \leftrightarrow_{AC}$, $R = \to_{\overline{R},AC}$, $R,B = \to_{\overline{R},AC}$, and $R/B = \to_{\overline{R}/AC}$, for which I show below for any $\mathcal{R}$ closed under B-extensions that $R/B = (=_B; R; =_B)$ holds when we instantiate the abstract relation R as $\to_{R,B}$; that is, for this example, that $\to_{\overline{R}/AC} = (=_{AC}; \to_{\overline{R},AC}; =_{AC})$.

Proposition 1. *Let $\mathcal{R} = (\Sigma, B, R)$ be a conditional order-sorted rewrite theory where B satisfies the assumptions stated at the beginning of Section 4 and $\mathcal{R}$ is closed under B-extensions. Then $\mathcal{R}$ satisfies:*

1. $\to^\star_{R/B} = \to^\star_{R,B}$, *and*
2. $\to_{R/B} = (=_B; \to_{R,B}; =_B)$.

Proof. The inclusions $\to^\star_{R/B} \supseteq \to^\star_{R,B}$, and $\to_{R/B} \supseteq (=_B; \to_{R,B}; =_B)$ are obvious; we just need to prove the opposite inclusions. The proof is by induction on the size of the closed proof tree of each rewrite of the form $u \to_{R/B} v$ or of the form $u \to^\star_{R/B} v$, where the tree size is the number of goal occurrences. The base cases are either an application of **Reflexivity**, where we obviously have $u \to^\star_{R,B} v \Leftrightarrow u \to^\star_{R/B} v$, or an application of **Replacement** with an *unconditional* rule $l \to r \in R$, so that $u \to_{R/B} v$ is obtained as $u =_B u' \to_R u'[r\theta]_p =_B v$, where $u_p = l\theta$, which clearly shows $u =_B; \to_{R,B}; =_B v$. The inductive cases are: (i) **Replacement** applied with a *conditional* rule in R, where the induction hypothesis about (1) applied to the $\to^\star_{R/B}$ rewrites in the condition allows us to conclude as for unconditional **Replacement** that $u =_B; \to_{R,B}; =_B v$, and (ii) an instance of **Transitivity** of the form:

$$\frac{u \to_{R/B} w \qquad w \to^\star_{R/B} v}{u \to^\star_{R/B} v}$$

By the induction hypothesis we have $u =_B u' \to_{R,B} w' =_B w$ for some u', w'. Since $\to_{R,B}$ satisfies the **Strict Coherence** property, we have a rewrite $u \to_{R,B} w''$ with $w'' =_B w'$, and therefore with $w'' =_B w$. Recall now Fact (2) in Remark 1 about $w \to^{\star}_{R/B} v$. Using the transitivity of $=_B$ and the fact that $\to_{R/B} = (=_B; \to_{R/B})$, it is then easy to prove by induction on the number $n \geq 0$ of $\to_{R/B}$-steps in $w \to^{\star}_{R/B} v$, that if it has a proof tree T of size k, then $w'' \to^{\star}_{R/B} v$ also has a proof tree T' of size k, so that the induction hypothesis applies and we get $w'' \to^{\star}_{R,B} v$, which together with $u \to_{R,B} w''$ gives us by **Transitivity** the desired result $u \to^{\star}_{R,B} v$. $\square$

Note, by the way, that (1) above and Fact (3) in Remark 1 immediately give us the transitivity property: $\to^{\star}_{R,B}; \to^{\star}_{R,B} \subseteq \to^{\star}_{R,B}$, which of course also applies to the special case of $\mathcal{R}$ closed under B-extensions and *unconditional*.

Now that the way has been cleared for applying the abstract strict coherence results in Section 2 to a *conditional* theory $\mathcal{R} = (\Sigma, B, R)$ closed under B-extensions, we can instantiate the abstract relations as follows: $R = \to_{R,B}$, $R, B = \to_{R,B}$, and $R/B = \to_{R/B}$ to immediately get:

Corollary 4. *Let $\mathcal{R} = (\Sigma, B, R)$ be a conditional order-sorted rewrite theory where B satisfies the assumptions stated at the beginning of Section 4 and $\mathcal{R}$ is closed under B-extensions. Then $\mathcal{R}$ satisfies the* **Completeness**, **Bisimulation**, **Strict Coherence** *and* **Strict Local Coherence** *properties. Furthermore, if $u =_B u'$ and $u \to_{R,B} v$ at position p with a rule $l' \to r'$ if $C \in R$ and with substitution θ, then there exists a term v' such that $u' \to_{R,B} v'$ at some position q with a rule $l'' \to r''$ if $C \in R$ and with a substitution θ' such that: (i) $v =_B v'$, and (ii) for all $x \in \mathcal{V}ar(C)$ $x\theta = x\theta'$.* $\square$

Corollary 5. *Let $\mathcal{R} = (\Sigma, B, R)$ be as in Corollary 4. Given any chain of $n \geq 0$ R, B-rewrite steps followed by a B-equality step of the form, $u \to_{R,B} u_1 \to_{R,B} u_2 \ldots u_{n-1} \to_{R,B} u_n =_B v$, where at each step a rule $l_i \to r_i$ if $C_i \in R$ has been applied with substitution θ_i, and given any term u' such that $u =_B u'$, there is another chain of $n \geq 0$ rewrite steps followed by a B-equality step of the form, $u' \to_{R,B} u'_1 \to_{R,B} u'_2 \ldots u'_{n-1} \to_{R,B} u'_n =_B v'$, such that: (i) $u_i =_B u'_i$, $1 \leq i \leq n$ and $v =_B v'$, where at each step a rule $l'_i \to r'_i$ if $C_i \in R$ has been applied with substitution θ'_i such that for all $x \in \mathcal{V}ar(C_i)$ $x\theta_i = x\theta'_i$, $1 \leq i \leq n$.*
$\square$

Obviously, it also follows from Corollary 4 that $\to_{R,B}$ can be used to rewrite in equivalence classes using the equivalence:

$$[t]_B \to_{R/B} [t']_B \quad \Leftrightarrow \quad (\exists u)\ t \to_{R,B} u \wedge u =_B t'.$$

Note that if $\mathcal{R} = (\Sigma, B, R)$ is closed under B-extensions and therefore strictly B-coherent, we know from Corollary 1 that $\to_{R/B}$ and $\to_{R,B}$ are *equi-terminating*. However, since looping can also happen when evaluating conditions, termination of the rewrite relations $\to_{R/B}$ and $\to_{R,B}$ is a clearly *insufficient* notion of conditional termination. The appropriate notion is that of *operational termination* [10, 27]. Therefore, the relevant question is whether R/B and R, B are *operationally equi-terminating*.

5. Operational Equi-Termination of R/B and R,B Rewriting

5.1. Operational Termination of Declarative Programs

The central idea of declarative programming can be summarized by the identities: (i) *program = logical theory*, and (ii) *computation = deduction*. Different declarative languages correspond to different computational logics $\mathcal{L}$ defined by inference rules parameterized by each *program*, that is, by each *theory* $\mathcal{S}$ in $\mathcal{L}$. The traditional TRS approach to termination assumes a single relation $\rightarrow$ that terminates iff it has no infinite chains, that is, iff it is well-founded. Although this idea fits well the case of unconditional rewriting, it breaks down for conditional rewriting,[11] and of course for many other computational logics, which may not involve any rewriting at all. A natural way to express termination for a declarative program $\mathcal{S}$ —i.e., a theory— in a general computational logic $\mathcal{L}$ is as *absence of infinite inference*. This is the key intuition formalized by the notion of operational termination [10, 27]. To make the paper self-contained, I summarize below the main general notions, illustrating them for the case of conditional rewriting modulo axioms B. I follow closely —with some additional precisions— the presentation in [10].

The axiomatic context in which operational termination is expressed is the theory of general logics [30]; more specifically its inference aspect, captured by the notion of *entailment system*. For our present purposes, all we need to assume is that:

1. Theories $\mathcal{S}$ in a logic $\mathcal{L}$ belong to a set of theories $Th_{\mathcal{L}}$, so that $\mathcal{S} \in Th_{\mathcal{L}}$. For example, an order-sorted conditional rewrite theory $\mathcal{R} = (\Sigma, B, R)$ belongs to the set of theories of *two* logics: (i) $OSRL(R/B)$, based on the relations $\rightarrow_{R/B}$ and $\rightarrow^{\star}_{R/B}$, and (ii) $OSRL(R,B)$, based on the relations $\rightarrow_{R,B}$ and $\rightarrow^{\star}_{R,B}$.

2. For each theory $\mathcal{S} \in Th_{\mathcal{L}}$ there is a set $Form_{\mathcal{L}}(\mathcal{S})$ of *formulas* of $\mathcal{S}$. For example, for $(\Sigma, B, R) \in Th_{OSRL(R/B)}$ (resp. $(\Sigma, B, R) \in Th_{OSRL(R,B)}$) we have:

   $Form_{OSRL(R/B)}(\Sigma, B, R) =$
   $\{t \rightarrow_{R/B} t' \mid t, t' \in \mathcal{T}_{\Sigma}(\mathcal{X})_{[s]}, s \in S\} \cup \{t \rightarrow^{\star}_{R/B} t' \mid t, t' \in \mathcal{T}_{\Sigma}(\mathcal{X})_{[s]}, s \in S\}$

   $Form_{OSRL(R,B)}(\Sigma, B, R) =$
   $\{t \rightarrow_{R,B} t' \mid t, t' \in \mathcal{T}_{\Sigma}(\mathcal{X})_{[s]}, s \in S\} \cup \{t \rightarrow^{\star}_{R,B} t' \mid t, t' \in \mathcal{T}_{\Sigma}(\mathcal{X})_{[s]}, s \in S\}$

   where S is the set of sorts of the signature Σ.

3. Each theory $\mathcal{S} \in Th_{\mathcal{L}}$ has an associated set of *inference rules* $\mathcal{I}_{\mathcal{L}}(\mathcal{S})$, where each inference rule $\iota \in \mathcal{I}_{\mathcal{L}}(\mathcal{S})$ is a scheme specifying a (possibly infinite) set of pairs $(\vec{\phi}, \varphi)$, called its *instances*, and denoted $\frac{\vec{\phi}}{\varphi}$, where $\vec{\phi} \in Form_{\mathcal{L}}(\mathcal{S}).^{*}$ and $\varphi \in Form_{\mathcal{L}}(\mathcal{S})$.

[11] Because of the additional possibility of looping when evaluating a rule's condition.

For example, for $(\Sigma, B, R) \in Th_{OSRL(R/B)}$ (resp. $(\Sigma, B, R) \in Th_{OSRL(R,B)}$) the corresponding inference systems are those specified for $\rightarrow_{R/B}$ and $\rightarrow^{\star}_{R/B}$ (resp. $\rightarrow_{R,B}$ and $\rightarrow^{\star}_{R,B}$) in Section 3.2.

The key proof-theoretic notion in such a logic $\mathcal{L}$ is that of a *proof tree*.

Definition 2. *The set of (finite) proof trees for a theory $\mathcal{S}$ in a logic $\mathcal{L}$ and the head of a proof tree are defined inductively as follows. A* proof tree *is*

- *either an* open goal, *simply denoted as φ, where φ is a formula for $\mathcal{S}$; then, we define head$(\varphi) = \varphi$,*
- *or a* non-atomic *tree with φ as its head, denoted as*

$$\frac{T_1 \quad \cdots \quad T_n}{\varphi} \quad (\iota)$$

where φ is a formula for $\mathcal{S}$, ι is an inference rule in $\mathcal{I}_{\mathcal{L}}(\mathcal{S})$, and $T_1,\ldots,T_n$ are proof trees such that

$$\frac{head(T_1) \quad \cdots \quad head(T_n)}{\varphi}$$

is an instance of ι.

We say that a proof tree is closed *whenever it is finite and contains no open goals. If T is a closed proof tree for $\mathcal{S}$, we then write $\mathcal{S} \vdash head(T)$, and call $head(T)$ a* theorem *of $\mathcal{S}$.*

Notice the difference between φ, an open goal, and $\overline{\varphi}$, a goal closed by a rule ι without premises.

Increasing chains of (finite) proof trees can give rise to infinite proof trees.

Definition 3. *A proof tree T is a* proper prefix *of a proof tree T' if there are one or more open goals $\varphi_1, \ldots, \varphi_n$ in T such that T' is obtained from T by replacing each φ_i by a non-atomic proof tree T_i having φ_i as its head. We denote the proper prefix relation as $T \subset T'$.*

An infinite proof tree *is an infinite increasing chain of finite trees, that is, a sequence $\{T_i\}_{i\in\mathbb{N}}$ such that for all i, $T_i \subset T_{i+1}$.*

We characterize the proof trees with computational meaning (those which are computed by an *interpreter* for $\mathcal{L}$ which solves goals in a proof tree bottom-up and from left to right), by means of the notion of well-formed proof tree.

Definition 4. *We say that a proof tree T is* well-formed *if it is either an open goal, or a closed proof tree, or a proof tree of the form*

$$\frac{T_1 \quad \cdots \quad T_n}{\varphi} \quad (\iota)$$

where for each j T_j is itself well-formed, and there is $i \leq n$ such that T_i is not closed, for any $j < i$ T_j is closed, and each of the T_{i+1} ,...,T_n is an open goal. An infinite proof tree is well-formed *if it is an ascending chain of well-formed finite proof trees. $\mathcal{S}$ is called* operationally terminating *if no infinite well-formed proof tree for $\mathcal{S}$ exists.*

Operational termination intuitively means that, given an initial goal, an interpreter that solves goals bottom-up and from left to right will either succeed in finite time in producing a closed proof tree, or will fail in finite time, not being able to close or extend further any of the possible proof trees, after exhaustively searching all such proof trees.

For the inference systems of the logics $OSRL(R/B)$ and $OSRL(R,B)$, as already mentioned in Section 3.3, the key challenge for an interpreter is how to guess the substitution θ in the **Replacement** rule, which may require using *symbolic constraints*. As further discussed in Section 6.2, a much easier to implement interpreter for $OSRL(R,B)$ treats the —still very general— special case where the rules in the conditional order-sorted rewrite theory $\mathcal{R}$ generalize those of a deterministic 3-CTRS [36], so that the substitution θ can be computed *incrementally*, as each subgoal in the condition gets solved.

5.2. Proof of Operational Equi-Termination of R/B and R,B Rewriting

Given a conditional order-sorted rewrite theory $\mathcal{R} = (\Sigma, B, R)$ an interpreter evaluating goals for $\mathcal{R}$ in the logic $OSRL(R,B)$ is much easier to implement and much more efficient than an intepreter evaluating similar goals in the logic $OSRL(R/B)$. Of course, without the strict coherence of the rules R an intepreter for $\mathcal{R}$ in the logic $OSRL(R,B)$ would be *incomplete*. So we should in any case assume that $\mathcal{R}$ is closed under B-extensions and therefore strictly coherent. But, assuming that, what about operational termination? Is it the same in both logics?

Theorem 3. *Let $\mathcal{R} = (\Sigma, B, R)$ be closed under the B-extensions. Then $\mathcal{R}$ is operationally terminating in $OSRL(R/B)$ iff $\mathcal{R}$ is operationally terminating in $OSRL(R,B)$.*

Proof. The proof of the ($\Rightarrow$) direction is straightforward. Just notice that, by systematically changing each goal $u \rightarrow_{R,B} u'$, or $v \rightarrow^{\star}_{R,B} v'$, in a well-formed proof tree for $\mathcal{R}$ in $OSRL(R,B)$ into a corresponding goal $u \rightarrow_{R/B} u'$, or $v \rightarrow^{\star}_{R/B}$ v', we obtain a well-formed proof tree for $\mathcal{R}$ in $OSRL(R/B)$. This is because, up to such renaming of goals, the corresponding instances of the **Reflexivity** and **Transitivity** rules are the same in both logics; and the **Replacement** rule is *more restrictive* in $OSRL(R,B)$ than in $OSRL(R/B)$. Therefore, if $\mathcal{R}$ is operationally terminating in $OSRL(R/B)$ there are no well-formed infinite proof trees for $\mathcal{R}$ in $OSRL(R/B)$ and, *a fortiori*, no well-formed infinite proof trees for $\mathcal{R}$ in $OSRL(R,B)$.

To prove the ($\Leftarrow$) direction we reason by contradiction and assume that $\mathcal{R}$ is operationally terminating in $OSRL(R,B)$ but there is a well-formed infinite proof tree for $\mathcal{R}$ in $OSRL(R/B)$. We will reach the desired contradiction if we can then show that there is a well-formed infinite proof tree for $\mathcal{R}$ in $OSRL(R, B)$.

Let $\{T_i\}_{i\in\mathbb{N}}$ be the well-formed infinite proof tree for $\mathcal{R}$ in $OSRL(R/B)$. Without loss of generality we may assume that the well-formed finite tree inclusions $T_i \subset T_{i+1}$ are such that T_0 is an open goal, and for each $i \in \mathbb{N}$, T_{i+1} is just the proper prefix of T_i obtained by a one-step expansion of the *current goal* ϕ of T_i, denoted $\phi = \mathit{cgoal}(T_i)$, by an instance of an inference rule having ϕ as its head; where for a non-closed finite proof tree we define: (i) $\mathit{cgoal}(\varphi) = \varphi$ for an open goal, and (ii) $\mathit{cgoal}(\frac{T_1 \quad \cdots \quad T_n}{\varphi}) = \mathit{cgoal}(T_j)$, where T_j is the leftmost non-closed proof tree in the sequence $T_1 \quad \cdots \quad T_n$. We can obtain the desired contradiction by a sequence of lemmas.

The proof of the following lemma is by induction on n and is left to the reader.

Lemma 1. *Let $\{T_i\}_{i\in\mathbb{N}}$ be a well-formed infinite proof tree for $\mathcal{R}$ in $OSRL(R/B)$ satisfying the assumptions above. Then for each $i \in \mathbb{N}$ all open goals in T_i other than $\mathit{cgoal}(T_i)$ are of the form $u \rightarrow^\star_{R/B} v$ for some u, v.* $\square$

Call a well-formed finite tree T for $\mathcal{R}$ in $OSRL(R/B)$ $\rightarrow^\star$*current* iff $\mathit{cgoal}(T)$ is of the form $u \rightarrow^\star_{R/B} v$ for some u, v.

Lemma 2. *Let $\{T_i\}_{i\in\mathbb{N}}$ be a well-formed infinite proof tree for $\mathcal{R}$ in $OSRL(R/B)$ satisfying the assumptions above. Then for each $i \in \mathbb{N}$ there is a smallest $j > i$ such that T_j is $\rightarrow^\star$*current.

Proof. Let $\mathit{cgoal}(T_i) = t \rightarrow_{R/B} t'$. Since the only rule that can be applied to it is **Replacement**, if the rule applied is unconditional, then the result follows from Lemma 1; and if it is conditional, then $\mathit{cgoal}(T_{i+1}) = u_1\theta \rightarrow^\star_{R/B} v_1\theta$ for some θ, where $u_1 \rightarrow v_1$ is the first goal in the rule's condition. Instead, if $\mathit{cgoal}(T_i) = t \rightarrow^\star_{R/B} t'$, and we then apply **Reflexivity**, the result again follows from Lemma 1. Otherwise, we have applied an instance of **Transitivity** of the form $\frac{t\rightarrow_{R/B}t'' \quad t''\rightarrow^\star_{R/B}t'}{t\rightarrow^\star_{R/B}t'}$, and $\mathit{cgoal}(T_{i+1}) = t \rightarrow_{R/B} t''$. But then T_{i+2} must be obtained by an application of **Replacement** to expand $t \rightarrow_{R/B} t''$, and the above reasoning shows that T_{i+2} is $\rightarrow^\star$*current*. $\square$

As a consequece of the above two lemmas we then obtain:

Corollary 6. *Let $\{T_i\}_{i\in\mathbb{N}}$ be a well-formed infinite proof tree for $\mathcal{R}$ in $OSRL(R/B)$ satisfying the assumptions above. The set $\{T_0\} \cup \{T_i \mid i > 0,\ T_i \ \rightarrow^\star \text{ current}\}$ is an infinite chain of well-formed trees, which we can denote $\{T_{\alpha(i)}\}_{i\in\mathbb{N}}$ for a monotonically increasing function α with $\alpha(0) = 0$. Furthermore, for each $i > 0$ all open goals in $T_{\alpha(i)}$ are of the form $u \rightarrow^\star_{R/B} v$ for some u, v.* $\square$

The next useful notion is that of B-*similarity* between a proof tree T for $\mathcal{R}$ in $OSRL(R/B)$ and a poof tree U for $\mathcal{R}$ in $OSRL(R, B)$, denoted $T \approx_B U$ and defined inductively as follows: (i) for open goals we have $(u \rightarrow_{R/B} v) \approx_B$

$(u' \to_{R,B} v')$ (resp. $(u \to^{\star}_{R/B} v) \approx_B (u' \to^{\star}_{R,B} v')$) iff $u =_B u'$ and $v =_B v'$; (ii) for a proof tree T for $\mathcal{R}$ in $OSRL(R/B)$ of the form $\frac{T_1 \quad \cdots \quad T_n}{\varphi}\ (\iota)$, a proof tree U for $\mathcal{R}$ in $OSRL(R,B)$ satisfies $T \approx_B U$ iff U is of the form $\frac{U_1 \quad \cdots \quad U_n}{\phi}\ (\iota)$, with $\varphi \approx_B \phi$ and $T_i \approx_B U_i$, $1 \leq i \leq n$.

The desired contradiction then follows from the following lemma:

Lemma 3. *Let $\{T_{\alpha(i)}\}_{i\in\mathbb{N}}$ be as in Corollary 6. Then there is a well-formed infinite proof tree for $\mathcal{R}$ in $OSRL(R,B)$ of the form $\{U_{\alpha(i)}\}_{i\in\mathbb{N}}$ such that for each $i \in \mathbb{N}$ $T_{\alpha(i)} \approx_B U_{\alpha(i)}$.*

Proof. We distinguish two cases, depending on $T_{\alpha(0)} = T_0$. **Case 1**: T_0 is of the form $u \to_{R/B} v$, then $T_{\alpha(1)} = T_1$ must be obtained by application of **Replacement** with a rule $l \to r \ \ if \ \ u_1 \to v_1 \wedge \ldots \wedge u_n \to v_n$ in R, so that T_1 is of the form:

$$\frac{u_1\theta \to^{\star}_{R/B} v_1\theta \quad \ldots \quad u_n\theta \to^{\star}_{R/B} v_n\theta}{u \to_{R/B} v}$$

with $t, u, u \in \mathcal{T}_{\Sigma}(\mathcal{X})$, $p \in \mathcal{P}(t)$, and θ a substitution, such that $u =_B t[l\theta]_p$ and $v =_B t[r\theta]_p$.

But since $t[l\theta]_p \to_R t[r\theta]_p$ is a special case of $t[l\theta]_p \to_{R,B} t[r\theta]_p$, since $\mathcal{R} = (\Sigma, B, R)$ is closed under B-extensions, we can apply Corollary 2, so that there is a rule $l' \to r' \ \ if \ \ u_1 \to v_1 \wedge \ldots \wedge u_n \to v_n$ in R and a proof tree U_1 for $\mathcal{R}$ in $OSRL(R,B)$ of the form:

$$\frac{u_1\theta' \to^{\star}_{R,B} v_1\theta' \quad \ldots \quad u_n\theta' \to^{\star}_{R,B} v_n\theta'}{u \to_{R,B} v'}$$

with $v =_B v'$ and $\theta(x) = \theta'(x)$ for each $x \in \mathcal{V}ar(u_1 \to v_1 \wedge \ldots \wedge u_n \to v_n)$. Therefore, choosing $U_0 = u \to_{R,B} v'$ we have $T_0 \approx_B U_0$, and $T_1 \approx_B U_1$.

Case 2: T_0 is of the form $u \to^{\star}_{R/B} v$. We then choose $U_0 = u \to^{\star}_{R,B} v$.

To prove the lemma, call an ascending finite chain of well-formed proof trees for $\mathcal{R}$ in $OSRL(R,B)$, $\{V_i\}_{0\leq i\leq n}$, *extensible* iff there is a well-formed proof tree V_{n+1} obtained from V_n by extending $cgoal(V_n)$ by a well-formed proof tree. Then the existence of an infinite chain of well-formed proof trees $\{U_{\alpha(i)}\}_{i\in\mathbb{N}}$ such that for each $i \in \mathbb{N}$ $T_{\alpha(i)} \approx_B U_{\alpha(i)}$ is equivalent to the existence of an "infinite chain of extensible finite chains" $\{U_0\} \subset \{U_{\alpha(i)}\}_{0\leq i\leq 1} \subset \ldots \{U_{\alpha(i)}\}_{0\leq i\leq n} \subset \ldots$ such that for each $i \in \mathbb{N}$ $T_{\alpha(i)} \approx_B U_{\alpha(i)}$. We now reason by contradiction. Suppose such a chain of extensible finite chains with the required B-similarity property does not exist. In particular, it does not exist for our choices of U_0 and $U_{\alpha(1)}$ in **Case 1**, and for our choice of U_0 in **Case 2**. This means that, for such choices, there is a finite chain $\{U_{\alpha(i)}\}_{0\leq i\leq n}$ with $T_{\alpha(i)} \approx_B U_{\alpha(i)}$, $0 \leq i \leq n$, such that either no extension to a $U_{\alpha(n+1)}$ exists, or for any such extension $U_{\alpha(n+1)}$ we have $T_{\alpha(n+1)} \not\approx_B U_{\alpha(n+1)}$. Note that, in both **Case 1** and **Case 2**, $U_{\alpha(n)}$ is $\to^{\star}$*current*. Let $cgoal(U_{\alpha(n)}) = u' \to^{\star}_{R,B} v'$. Then, since $T_{\alpha(n)} \approx_B U_{\alpha(n)}$, we have $cgoal(T_{\alpha(n)}) = u \to^{\star}_{R/B} v$ with $u =_B u'$ and $v =_B v'$, and $T_{\alpha(n+1)}$

is obtained by either an application of **Reflexivity**, which, can then also be applied to $u' \rightarrow^{\star}_{R,B} v'$, yielding the contradiction of an extension $U_{\alpha(n+1)}$ with $T_{\alpha(n+1)} \approx_B U_{\alpha(n+1)}$; or $T_{\alpha(n+1)}$ is obtained by an application of **Transitivity** of the form $\frac{u \rightarrow_{R/B} w \;\; w \rightarrow^{\star}_{R/B} v}{u \rightarrow^{\star}_{R/B} v}$ followed by an application of **Replacement** to expand $u \rightarrow_{R/B} w$ to

$$\frac{u_1\theta \rightarrow^{\star}_{R/B} v_1\theta \quad \ldots \quad u_n\theta \rightarrow^{\star}_{R/B} v_n\theta}{u \rightarrow_{R/B} w}$$

But, applying again Corollary 2, we then get an application of **Replacement**

$$\frac{u_1\theta' \rightarrow^{\star}_{R,B} v_1\theta' \quad \ldots \quad u_n\theta' \rightarrow^{\star}_{R,B} v_n\theta'}{u' \rightarrow_{R,B} w'}$$

with $w =_B w'$ and $\theta(x) = \theta'(x)$ for each $x \in \mathcal{V}ar(u_1 \rightarrow v_1 \;\wedge \ldots \wedge\; u_n \rightarrow v_n)$. But this means that we also have an application of **Transitivity** of the form $\frac{u' \rightarrow_{R,B} w' \;\; w' \rightarrow^{\star}_{R,B} v'}{u' \rightarrow^{\star}_{R,B} v'}$ which, followed by the application of **Replacement** to the goal $u' \rightarrow_{R,B} w'$, yields the contradiction of a well-formed proof tree $U_{\alpha(n+1)}$ with $T_{\alpha(n+1)} \approx_B U_{\alpha(n+1)}$. □

This finishes the proof of the theorem. □

6. The Church-Rosser Property

As mentioned in Section 3.2, the meaning of $\mathcal{R} = (\Sigma, B, R)$ need not be equational. However, it *can* be equational, and many applications to functional programming, theorem proving, and equational logic use such an equational interpretation. Given an unconditional equational theory (Σ, E) we can orient its equations E from left to right as rewrite rules $\vec{E}$ to obtain a TRS $(\Sigma, \vec{E})$. The Church-Rosser property is then the key property giving us a *complete* method of *reducing* equational reasoning to rewriting. $(\Sigma, \vec{E})$ is said to be *Church-Rosser* iff for any Σ-terms t, t' we have the equivalence:

$$t =_E t' \;\Leftrightarrow\; t \downarrow_{\vec{E}} t',$$

where the *joinability relation* $t \downarrow_{\vec{E}} t'$ is defined by the equivalence:

$$(\natural) \;\; t \downarrow_{\vec{E}} t' \quad \Leftrightarrow \quad (\exists u)\, t \rightarrow^{*}_{\vec{E}} u \wedge t' \rightarrow^{*}_{\vec{E}} u.$$

It is well-known and very easy to prove that $(\Sigma, \vec{E})$ is confluent iff it is Church-Rosser (this is called the *Church-Rosser Theorem*).

In the present setting, the obvious generalization of the Church-Rosser property assumes a *conditional* order-sorted equational theory of the form $(\Sigma, E \cup B)$, where the equations B are unconditional. One would then like to call the conditional order-sorted rewrite theory $(\Sigma, B, \vec{E})$ *Church-Rosser modulo B* iff it satisfies the equivalence:

$$t =_{E \cup B} t' \;\Leftrightarrow\; t \downarrow^{\star}_{\vec{E}/B} t',$$

where the $\star$-joinability modulo B relation $t \downarrow^{\star}_{\vec{E}/B} t'$ is defined in the "obvious" way by replacing in ($\natural$) $t \downarrow_{\vec{E}} t'$ by $t \downarrow^{\star}_{\vec{E}/B} t'$, and $\rightarrow^{*}_{\vec{E}}$ by $\rightarrow^{\star}_{\vec{E}/B}$. I say "obvious" in quotes and with some irony, since, as pointed out in Section 3.3, the relation $\rightarrow^{\star}_{\vec{E}/B}$ is *not* the reflexive-transitive closure of $\rightarrow_{\vec{E}/B}$. One then would also like to prove a *Church-Rosser Theorem modulo* B, showing that, under suitable conditions, $(\Sigma, B, \vec{E})$ is Church-Rosser modulo B iff it is confluent modulo B.

In contrast with the trivial proof of the Church-Rosser Theorem in the unconditional case and without axioms, proving a *conditional* Church-Rosser Theorem *modulo* axioms B is nontrivial. To begin with, if the equations E are conditional, it is not entirely obvious what the rules $\vec{E}$ mean, since we have to deal with their conditions; also, even in the unsorted case, the notion of confluence modulo B is somewhat more subtle (see [21], and Definition 5 and Lemma 5 below for the general case). Furthermore, the easy road to prove the Church-Rosser Theorem via abstract reduction relations is now blocked by the simple fact that, whereas in the unconditional case both equational reasoning and rewriting can be reduced to stringing rewrite steps together, in the conditional case —as made clear in Section 3.3– we need to deal with *inference systems*, both for equational reasoning and for rewriting, whose mutual relationships are considerably less obvious. All this makes the trivial proof of the Church-Rosser Theorem in the unconditional case non-trivial for conditional theories. Indeed, even for CTRSs (i.e., Σ unsorted and $B = \emptyset$), it is well-known that the Church-Rosser theorem does not hold for an arbitrary confluent theory $\mathcal{R}$ without imposing additional conditions on $\mathcal{R}$ (see [42] and Example 2 below).

Of course, one of the main motivations for a Church-Rosser Theorem is to make equational theories *decidable*; however, as further discussed in Section 6.2, the issue of decidability of the equality relation by rewriting is also nontrivial and particularly subtle in the conditional case. For all these reasons, in Sections 6.1 and 6.2 I state two increasingly stronger versions of a conditional Church-Rosser Theorem modulo axioms B. Furthermore, in Section 6.2 I briefly discuss checkable conditions for confluence, and therefore for the Church-Rosser property, when $\mathcal{R} = (\Sigma, B, R)$ is what I call a *strongly deterministic* conditional rewrite theory. This fully connects the results in [13] with those in this paper.

6.1. The Church-Rosser Property for Conditional Rewriting Modulo B

Given a sensible order-sorted signature Σ, a Σ-*conditional equation* is an implication formula $u_1 = v_1 \wedge \ldots \wedge u_n = v_n \;\Rightarrow\; t = t'$, hereafter written:

$$t = t' \;\; \textit{if} \;\; u_1 = v_1 \wedge \ldots \wedge u_n = v_n,$$

where $t = t'$ and $u_1 = v_1, \ldots, u_n = v_n$ are Σ-equations. A *conditional equational theory* is then a pair (Σ, E), with Σ a sensible order-sorted signature, and E a set of conditional Σ-equations.

Conditional equations are implicitly assumed to be *universally quantified.* Sound inference systems for order-sorted conditional equational logic (and even for many-sorted logic) must make such quantification explicit [34, 17, 32]. However, the need for explicit quantification can be avoided by assuming that Σ has *non-empty sorts* (recall that this means $\mathcal{T}_{\Sigma,s} \neq \emptyset$ for each $s \in S$) . To simplify the exposition, I will assume throughout that Σ has non-empty sorts (recall from Section 3.1 that we also always assume Σ to be kind-complete, preregular, and sensible; in the unsorted and many-sorted cases all this just boils down to Σ having non-empty sorts and being unambiguous).

Here is a simple inference system for conditional order-sorted logic under the above assumptions on Σ. Given an order-sorted conditional equational theory (Σ, E), its *theorems* are those Σ-equations that can be derived by finite application of the following inference rules:

- **Reflexivity**. For each Σ-term t, $\dfrac{}{t = t}$
- **Replacement**. For either $(t = t' \;\; \textit{if} \;\; u_1 = v_1 \, \wedge \, \ldots \, \wedge \, u_n = v_n) \in E$, or $(t' = t \;\; \textit{if} \;\; u_1 = v_1 \, \wedge \, \ldots \, \wedge \, u_n = v_n) \in E$, substitution θ, and Σ-term u with position p such that $u_p = t\theta$,

$$\frac{u_1\theta = v_1\theta \quad \ldots \quad u_n\theta = v_n\theta}{u = u[t'\theta]_p}$$

- **Transitivity**

$$\frac{t_1 = t_2 \qquad t_2 = t_3}{t_1 = t_3}$$

It is easy to check that, under the above assumptions on Σ, this inference system is equivalent to similar inference systems in [17, 32], which have been proved *sound and complete* with respect to the model-theoretic semantics provided by order-sorted algebras as models of conditional order-sorted equational theories.

The next order of business is to relate equational logic to rewriting. We can begin with a very simple question: can equational deduction in a conditional order-sorted equational theory be *reduced* to conditional rewriting deduction for *any* such theory? The answer is in the affirmative, as follows. Assume that the conditional equational theory is of the form $(\Sigma, E \cup B)$, where the equations B are unconditional (note that we can choose $B = \emptyset$ as a special case). Our desired order-sorted conditional rewrite theory simulating $(\Sigma, E \cup B)$ is of the form $(\Sigma, B, \overleftrightarrow{E})$, where $\overleftrightarrow{E} = \overrightarrow{E} \cup \overleftarrow{E}$, and

- $\overrightarrow{E} = \{t \to t' \;\; \textit{if} \;\; u_1 \to v_1 \wedge \ldots \wedge u_n \to v_n \mid (t = t' \;\; \textit{if} \;\; u_1 = v_1 \wedge \ldots \wedge u_n = v_n) \in E\}$
- $\overleftarrow{E} = \{t' \to t \;\; \textit{if} \;\; u_1 \to v_1 \wedge \ldots \wedge u_n \to v_n \mid (t = t' \;\; \textit{if} \;\; u_1 = v_1 \wedge \ldots \wedge u_n = v_n) \in E\}$.

Note the left-to-right orientation for the conditions in both cases.

The key lemma reducing conditional equational deduction to conditional rewriting is then,

Lemma 4. *We have the equivalence:*

$$(\Sigma, E \cup B) \vdash u = v \quad \Leftrightarrow \quad (\Sigma, B, \overleftrightarrow{E}) \vdash u \rightarrow^{\star}_{\overleftrightarrow{E}/B} v.$$

Proof. Since each rewrite proof can be viewed as an equality proof carried out in a more restricted inference system, the ($\Leftarrow$) implication is easy and left to the reader. To prove the ($\Rightarrow$) implication we reason by structural induction on the equational proof trees. The case of an equality $t = t$ obtained by **Reflexivity** follows trivially from the rewriting **Reflexivity** rule. The case of a proof of $t_1 = t_3$ by **Transitivity** follows by induction using Fact (3) in Remark 1. The case of a proof of $u = u[t'\theta]_p$ by **Replacement** follows by induction from rewriting **Replacement** by applying the corresponding conditional rule in either $\overrightarrow{E}$ or $\overleftarrow{E}$ to u at position p with substitution θ. $\Box$

Since the relations $\rightarrow^{\star}_{R/B}$ and $\rightarrow^{\star}_{R,B}$ are not reflexive-transitive closures, a few words should be said about confluence and joinability. Recall the notation $\rightarrow^{*}_{R/B}$ and $\rightarrow^{*}_{R,B}$ for the respective reflexive-transitive closures of $\rightarrow_{R/B}$ and $\rightarrow_{R,B}$. The relevant notions are summarized in the following definition:

Definition 5. *Given a conditional order-sorted rewrite theory $\mathcal{R} = (\Sigma, B, R)$, two terms $u, v \in \mathcal{T}_{\Sigma}(\mathcal{X})$ are called:*

1. R/B-joinable*, denoted $u \downarrow_{R/B} v$, (resp.* R, B-joinable*, denoted $u \downarrow_{R,B} v$) iff there exist $w, w' \in \mathcal{T}_{\Sigma}(\mathcal{X})$ such that $u \rightarrow^{*}_{R/B} w =_B w' \;{}_{R/B}^{*}\!\!\leftarrow v$ (resp. such that $u \rightarrow^{*}_{R,B} w =_B w' \;{}_{R,B}^{*}\!\!\leftarrow v$).*
2. $\star$-R/B-joinable*, denoted $u \downarrow^{\star}_{R/B} v$, (resp.* $\star$-R, B-joinable*, denoted $u \downarrow^{\star}_{R,B} v$) iff there exists $w \in \mathcal{T}_{\Sigma}(\mathcal{X})$ such that $u \rightarrow^{\star}_{R/B} w \;{}_{R/B}^{\star}\!\!\leftarrow v$ (resp. such that $u \rightarrow^{\star}_{R,B} w \;{}_{R,B}^{\star}\!\!\leftarrow v$).*

The relation $\rightarrow_{R/B}$ (resp. $\rightarrow_{R,B}$) is called:

1. Confluent *iff for each $u, v, t \in \mathcal{T}_{\Sigma}(\mathcal{X})$, $u \;{}_{R/B}^{*}\!\!\leftarrow t \rightarrow^{*}_{R/B} v$ implies $u \downarrow_{R/B} v$ (resp. $u \;{}_{R,B}^{*}\!\!\leftarrow t \rightarrow^{*}_{R,B} v$ implies $u \downarrow_{R,B} v$).*
2. $\star$-Confluent *iff for each $u, v, t \in \mathcal{T}_{\Sigma}(\mathcal{X})$, $u \;{}_{R/B}^{\star}\!\!\leftarrow t \rightarrow^{\star}_{R/B} v$ implies $u \downarrow^{\star}_{R/B} u$ (resp. $u \;{}_{R,B}^{\star}\!\!\leftarrow t \rightarrow^{\star}_{R,B} v$ implies $u \downarrow^{\star}_{R,B} v$).*

Note the extra B-equality $w =_B w'$ needed in the notions of R/B-joinability and R, B-joinability, and therefore on the notions of R/B-confluence and R, B-confluence, which makes such notions non-standard. By contrast, no such extra B-equality $w =_B w'$ is needed for $\star$-R/B-joinability, $\star$-R, B-joinability, $\star$-R/B-confluence, and $\star$-R, B-confluence, which makes such notions more natural. Their key relationships can be summarized in the following easy lemma:

Lemma 5. *Given a conditional order-sorted rewrite theory $\mathcal{R} = (\Sigma, B, R)$,*

1. *For each $u, v \in \mathcal{T}_{\Sigma}(\mathcal{X})$, $u \downarrow_{R/B} v \Leftrightarrow u \downarrow^{\star}_{R/B} v$, and $u \downarrow_{R,B} v \Leftrightarrow u \downarrow^{\star}_{R,B} v$.*

2. $\rightarrow_{R/B}$ *is confluent iff it is* $\star$*-confluent.*

3. $\rightarrow_{R,B}$ $\star$*-confluent implies* $\rightarrow_{R,B}$ *confluent, but the converse does not hold in general.*

Furthermore, if B *satisfies the assuptions in Section 4 and* $\mathcal{R}$ *is closed under* B*-extensions we have:*

1. $\forall u, v \in \mathcal{T}_\Sigma(\mathcal{X})$ $u \downarrow_{R/B} u \Leftrightarrow u \downarrow^\star_{R/B} u \Leftrightarrow u \downarrow^\star_{R,B} u \Leftrightarrow u \downarrow_{R,B} u$, *and*

2. $\rightarrow_{R/B}$ *confluent iff* $\rightarrow_{R/B}$ $\star$*-confluent iff* $\rightarrow_{R,B}$ $\star$*-confluent iff* $\rightarrow_{R,B}$ *confluent.*

For a counterexample showing that in general $\rightarrow_{R,B}$ confluent does not imply $\rightarrow_{R,B}$ $\star$-confluent, consider an unsorted signature with constants a, b, c, d binary AC symbol $\_\cdot\_$ and R with just one rule $a \cdot b \rightarrow c$. It is easy to check that $\rightarrow_{R,AC}$ is confluent. However, we have $(c \cdot a) \cdot b \ {}_{R/AC}\!\overset{\star}{\leftarrow} c \cdot (a \cdot b) \rightarrow^\star_{R/AC} c \cdot c$, where both $(c \cdot a) \cdot b$ and $c \cdot c$ are $\rightarrow_{R/AC}$-irreducible and obviously $(c \cdot a) \cdot b \neq_{AC} c \cdot c$.

As already mentioned, the Church-Rosser Theorem does not hold in general for confluent theories in the conditional case, unless some additional conditions are imposed on $\mathcal{R}$. The problem is illustrated by the following simple example from [42]:

Example 2. *Consider the CTRS* $\mathcal{R} = (\Sigma, R)$ *with signature* Σ *having just three constants* a, b, c *and* R *having the rules* $a \rightarrow c$ *and* $b \rightarrow c$ *if* $c \rightarrow a$*.* $\mathcal{R}$ *is confluent. For the conditional equational theory* (Σ, E) *with* E *having the equations* $a = c$ *and* $b = c$ *if* $c = a$*, we obviously have* $E \vdash a = c$*. However,* b *is* $\mathcal{R}$*-irreducible, and* a *can only be rewritten to* c*, so that* $a \not\downarrow_R b$*. That is,* $\mathcal{R}$ *fails to have the Church-Rosser property.*

The Church-Rosser property for CTRSs (called there *logicality*) has been carefully studied in [42], where several sufficient conditions on $\mathcal{R}$ ensuring the Church-Rosser Theorem are given. Let me briefly summarize a class of CTRSs enjoying the Church-Rosser property proposed (among other classes) in [42]. Given a CTRS (Σ, R), call a Σ-term t *R-irreducible* iff there is no t' such that $t \rightarrow_R t'$. Likewise, let us call a substitution θ *R-irreducible* iff $x\theta$ is R-irreducible for each $x \in dom(\theta)$. Finally, call a Σ-term t *strongly R-irreducible* iff $t\theta$ is R-irreducible for each R-irreducible θ. Furthermore, we call (Σ, R) *weakly terminating* iff for each Σ-term t there is an R-irreducible t' such that $t \rightarrow^* t'$. The class in question is that of all CTRSs $\mathcal{R} = (\Sigma, \vec{E})$ associated to conditional equational theories (Σ, E) such that $\mathcal{R}$ is confluent and weakly terminating, and for each rewrite rule $l \rightarrow r$ *if* $\bigwedge_{i=1..n} u_i \rightarrow v_i$ in $\vec{E}$ all the v_j, $1 \leq j \leq n$ are strongly R-irreducible. They enjoy the Church-Rosser property. That is, we have:

Theorem 4. *[42] If the CTRS* $\mathcal{R}$ *satisfies the above conditions, then for any* Σ*-terms* t, t' *we have the equivalence:*

$$t =_E t' \ \Leftrightarrow \ t \downarrow_{\vec{E}} t'.$$

The above class of CTRSs can be naturally generalized to conditional order-sorted theories. Given a conditional order-sorted rewrite theory $\mathcal{R} = (\Sigma, B, R)$, we call a Σ-term t *R/B-irreducible* iff there is no t' such that $t \to_{R/B} t'$. Likewise, we call a substitution θ *R/B-irreducible* iff $x\theta$ is R/B-irreducible for each $x \in dom(\theta)$. We call a Σ-term t *strongly R/B-irreducible* iff $t\theta$ is R/B-irreducible for each R/B-irreducible θ. And we call $\mathcal{R} = (\Sigma, B, R)$ *weakly terminating* modulo B iff for each Σ-term t there is an R/B-irreducible t' such that $t \to^{\star}_{R/B} t'$.

Since we are in an order-sorted setting, a further property, satisfied automatically by unsorted and many-sorted rewrite theories, is also relevant, namely, sort-decreasingness. $\mathcal{R} = (\Sigma, B, R)$ is called *sort-decreasing* modulo B iff whenever $t \to_{R/B} t'$ we have $ls(t) \geq ls(t')$. A checkable sufficient condition for the sort-decreasingness of $\mathcal{R} = (\Sigma, B, R)$ is that: (i) B is sort-preserving, and (ii) for all rules $l \to r$ *if* $\bigwedge_{i=1..n} u_i \to v_i$ in R and all "sort specializations" ρ (i.e., sort-lowering substitutions ρ such that for all $x : s$ in $dom(\rho)$ we have $\rho : x : s \mapsto x' : s'$ with $s \geq s'$) the property $ls(l\rho) \geq ls(r\rho)$ holds. Here is the main theorem, generalizing Theorem 4 above:

Theorem 5. *(Church-Rosser Theorem modulo B). Let $\mathcal{R} = (\Sigma, B, \vec{E})$, associated to a conditional equational theory $(\Sigma, E \cup B)$, be such that $\to_{\vec{E}/B}$ is sort-decreasing and weakly terminating modulo B, and for each rewrite rule $l \to r$ if $\bigwedge_{i=1..n} u_i \to v_i$ in $\vec{E}$ all the v_j, $1 \leq j \leq n$, are strongly $\vec{E}/B$-irreducible. Then $\to_{\vec{E}/B}$ is confluent modulo B iff for any Σ-terms t, t' we have the equivalence:*

$$(\spadesuit) \quad t =_{E\cup B} t' \;\Leftrightarrow\; t \downarrow_{\vec{E}/B} t'.$$

Proof. Since we have the theory inclusion $(\Sigma, B, \vec{E}) \subseteq (\Sigma, B, \overset{\leftrightarrow}{E})$, Lemma 4 easily gives us the $(\Leftarrow)$ implication in the above equivalence $(\spadesuit)$. Therefore, all we need to prove is that, under the given assumptions, $\mathcal{R}$ is confluent iff the implication $t =_{E\cup B} t' \;\Rightarrow\; t \downarrow_{\vec{E}/B} t'$ holds. Suppose the implication holds. We then need to prove that $u \;{}_{R/B}\!\!\overset{*}{\leftarrow} t \to^{*}_{R/B} v$ implies $u \downarrow_{R/B} v$. But, again by $(\Sigma, B, \vec{E}) \subseteq (\Sigma, B, \overset{\leftrightarrow}{E})$, this follows easily from Lemma 4, which gives us $u =_{E\cup B} v$.

Suppose now that $\mathcal{R}$ is confluent. We need to prove that $t =_{E\cup B} t' \;\Rightarrow\; t \downarrow_{\vec{E}/B} t'$ holds. Call a set G of Σ-equations *deduction closed* iff $G \vdash u = v$ implies $(u = v) \in G$, where $\vdash$ is the provability relation for the inference system of order-sorted conditional equational logic presented above. It is easy to prove that confluence and the other assumptions on $\mathcal{R}$ make the set of equations

$$=_{\downarrow_{\vec{E}/B}} = \; \{u = v \mid u, v \in \mathcal{T}_{\Sigma}(\mathcal{X}) \;\wedge\; u \downarrow_{\vec{E}/B} v\}$$

deduction-closed. We will be done if we prove $=_{E\cup B} \subseteq =_{\downarrow_{\vec{E}/B}}$.

Recall the notion of free order-sorted Σ/G-algebra $\mathcal{T}_{\Sigma/G}(\mathcal{X})$ on $\mathcal{X}$ for G a set of either conditional or unconconditional equations [17, 32]. For each top sort $[s]$

in a connected component of the poset $(S, \leq)$ define $\mathcal{T}_{\Sigma/G}(\mathcal{X})_{[s]} = \mathcal{T}_{\Sigma}(\mathcal{X})_{[s]}/=_G$, and for any other sort s in the same connected component define $\mathcal{T}_{\Sigma/G}(\mathcal{X})_s = \{[t]_G \in \mathcal{T}_{\Sigma/G}(\mathcal{X})_{[s]} \mid \exists u \in [t]_G \; s.t. \; ls(u) = s\}$. The operations Σ for $\mathcal{T}_{\Sigma/G}(\mathcal{X})$ are defined in the usual way by operating on representatives of G-equivalence classes. We have two such free algebras on $\mathcal{X}$, namely, $\mathcal{T}_{\Sigma/E\cup B}(\mathcal{X})$, assocITated to $E \cup B$, and $\mathcal{T}_{\Sigma/=_{\downarrow_{\vec{E}/B}}}(\mathcal{X})$, associated to the deduction-closed equations $=_{\downarrow_{\vec{E}/B}}$.

The desired inclusion $=_{E\cup B} \subseteq =_{\downarrow_{\vec{E}/B}}$ will follow easily from the freeness theorem for order-sorted algebras [17, 32] if we show that $\mathcal{T}_{\Sigma/=_{\downarrow_{\vec{E}/B}}}(\mathcal{X}) \models E \cup B$. The satisfaction $\mathcal{T}_{\Sigma/=_{\downarrow_{\vec{E}/B}}}(\mathcal{X}) \models B$ follows trivially from the **Reflexivity** rule for rewriting modulo B. We just need to show that $\mathcal{T}_{\Sigma/=_{\downarrow_{\vec{E}/B}}}(\mathcal{X}) \models E$. Let $l = r \; if \; \bigwedge_{i=1..n} u_i = v_i$ be a conditional equation in E. We need to show that for each sort-preserving assignment $a : \mathcal{X} \longrightarrow \mathcal{T}_{\Sigma/=_{\downarrow_{\vec{E}/B}}}(\mathcal{X})$ such that $\overline{a}(u_i) = \overline{a}(v_i)$, $1 \leq i \leq n$ we have $\overline{a}(l) = \overline{a}(r)$, where $\overline{a}$ is the homomorphic extension of a. But note that a can always be described as $a(x) = [\theta(x)]_{=_{\downarrow_{\vec{E}/B}}}$ for some (by definition sort-preserving) substitution θ. Therefore, we just need to show that $u_i\theta \downarrow_{\vec{E}/B} v_i\theta$, $1 \leq i \leq n$ implies $l\theta \downarrow_{\vec{E}/B} r\theta$.

Since $\mathcal{R}$ is weakly terminating and sort-decreasing modulo B, we have also an (again sort-preserving thanks to sort-decreasingness) substitution $\theta!_{\vec{E}/B}$ defined for each x by: $\theta!_{\vec{E}/B}(x) = \theta(x)!_{\vec{E}/B}$, where, by definition, $\theta(x)!_{\vec{E}/B}$ is an R/B-irreducible term reachable from $\theta(x)$ thanks to the weak termination modulo B assumption.

Since $u_i\theta \downarrow_{\vec{E}/B} v_i\theta$, $1 \leq i \leq n$ and $\rightarrow_{R/B}$ is confluent, we also have $(u_i\theta!_{\vec{E}/B}) \downarrow_{\vec{E}/B} (v_i\theta!_{\vec{E}/B})$, $1 \leq i \leq n$, which by $\theta!_{\vec{E}/B}$ R/B-irreducible substitution and the v_i strongly R/B-irreducible yields $(u_i\theta!_{\vec{E}/B}) \rightarrow^{\star}_{\vec{E}/B} (v_i\theta!_{\vec{E}/B})$. Therefore, by **Replacement** we get: $(l\theta!_{\vec{E}/B}) \rightarrow_{\vec{E}/B} (r\theta!_{\vec{E}/B})$. But since $(l\theta) \rightarrow^{\star}_{\vec{E}/B} (l\theta!_{\vec{E}/B})$, and $(r\theta) \rightarrow^{\star}_{\vec{E}/B} (r\theta!_{\vec{E}/B})$, we get $l\theta \downarrow_{\vec{E}/B} r\theta$, as desired. $\square$

The class of theories described in Theorem 5 is very general. It includes, in particular, all confluent, sort-decreasing and weakly terminating modulo B rewrite theories that interpret a conditional equation $l = r \; if \; \bigwedge_{i=1..n} u_i = v_i$ as a conditional rewrite rule $l \rightarrow r \; if \; \bigwedge_{i=1..n} u_i \downarrow v_i$. I have not even bothered discussing such theories because, up to a simple transformation, they can be reduced to rewrite theories with oriented conditions. The transformation $\mathcal{R} \mapsto \mathcal{R}^{\equiv}$ in question adds: (i) a new sort *Truth* with a constant *tt* in a new connected component; (ii) for each top sort $[s]$ of each connected component of the poset of sorts of $\mathcal{R}$ an operator $\_ \equiv \_ : [s] \; [s] \longrightarrow \mathit{Truth}$ and a rewrite rule $x \equiv x \rightarrow tt$, with x of sort $[s]$. Then each rule $l \rightarrow r \; if \; \bigwedge_{i=1..n} u_i \downarrow v_i$ in $\mathcal{R}$ is mapped to the rule $l \rightarrow r \; if \; \bigwedge_{i=1..n} u_i \equiv v_i \rightarrow tt$ in $\mathcal{R}^{\equiv}$. Note that tt is $\mathcal{R}^{\equiv}$-irreducible and obviously strongly $\mathcal{R}^{\equiv}$-irreducible.

6.2. Strongly Deterministic Rewrite Theories and Decidability Issues

I am particularly interested in the use of confluent order-sorted rewrite theories as *functional programs* having an initial algebra semantics as equational theories; and on conditions ensuring that such an initial algebra semantics *agrees* with their operational semantics by rewriting. Furthermore, for any practical applications, the effective implementability of such programs and, when possible, their good decidability properties are paramount.

However, all these desirable properties are not available in general for CTRSs in the class proposed in [42] and shown there to satisfy Theorem 4. A fortiori, they are not available in the even broader class of confluent conditional order-sorted theories satisfying Theorem 5. The reasons why such good properties are lacking are the following:

1. Since no restrictions are given on the variables appearing in the condition and the righthand side of a rule $l \to r$ *if* $\bigwedge_{i=1..n} u_i \to v_i$, guessing which substitution θ to use when applying the **Replacement** rule becomes quite difficult, since in general an infinite number of choices for θ may exist. This makes implementations of rewriting difficult, so that symbolic methods may be needed.

2. A second problem, further discussed below, is that the class of CTRSs in Theorem 4 and, a fortiori, the class of confluent conditional order-sorted theories satisfying Theorem 5 contain all kinds of *monsters*; that is, theories where one's computational intuitions break down.

3. This leads to a third problem of *decidability*, with two closely-related manifestations. One is that, although mathematically the results in Theorems 4 and 5 ensure the existence of initial algebras, such initial algebras are in general *undecidable* data types lacking a good computational correspondence between mathematical, initial algebra semantics, and operational semantics by rewriting. A second, broader manifestation is that, in spite of the equivalence $t =_{E\cup B} t' \;\Leftrightarrow\; t \downarrow_{\vec{E}/B} t'$ ensured by Theorem 5, the equality relation $=_{E\cup B}$ is in general *undecidable*. This nullifies one of the key advantages of the unconditional Church-Rosser property in the weakly terminating case under B-coherence and finitary B-matching algorithm assumptions, namely, the *decidability* of the equality relation $t =_{E\cup B} t'$ by comparing for B-equality the $\vec{E}, B$-irreducible terms $t!_{\vec{E},B}$ and $t'!_{\vec{E},B}$.

The main theme of this section is the study of additional requirements on a rewrite theory $\mathcal{R}$ overcoming the just-mentioned problems (1)–(3). A first step towards overcoming Problem (1) while remaining within the class of confluent theories of Theorem 5 is restricting the rewrite theories $\mathcal{R} = (\Sigma, B, \vec{E})$ to be *strongly deterministic* in the following sense:

Definition 6. *Let $\mathcal{R} = (\Sigma, B, R)$ be a conditional order-sorted rewrite theory. A rule $l \to r$ if $\bigwedge_{i=1..n} u_i \to v_i$ in R is called* deterministic *iff: (i) $\forall j \in [1..n], \mathcal{V}ar(u_j) \subseteq \mathcal{V}ar(l) \cup \bigcup_{k<j} \mathcal{V}ar(v_k)$, and (ii) $\mathcal{V}ar(r) \subseteq \mathcal{V}ar(l) \cup \bigcup_{j\leq n} \mathcal{V}ar(v_j)$. $\mathcal{R}$ is* deterministic *iff all its rules are so.*

A determinsitic rewrite theory $\mathcal{R} = (\Sigma, B, R)$ is called strongly deterministic *if, in addition, each rewrite rule $l \to r$ if $\bigwedge_{i=1..n} u_i \to v_i$ in R is such that the v_i, $1 \leq i \leq n$, are strongly R/B-irreducible.*

Note that when Σ is unsorted and $B = \emptyset$, a deterministic (resp. strongly deterministic) conditional rewrite theory specializes to the notion of a *deterministic* (resp. *strongly deterministic*) *3-CTRS* [36].

The key intuition about both deterministic 3-CTRSs and deterministic order-sorted rewrite theories is that the extra variables in the righthand side and the condition of a rule $l \to r$ *if* $\bigwedge_{i=1..n} u_i \to v_i$ are incrementally instantiated by matching. That is, the conditions are solved *from left to right* by rewriting each $u_i\sigma$ to an instance (modulo B in our case) of the pattern v_i, thus incrementally extending the domain of σ, which can then be used to start solving the next condition by rewriting $u_{i+1}\sigma$.

Specifically, if we assume that B is regular and linear, the deterministic rules R are closed under B-extensions, and there is a finitary B-matching algorithm, rewriting with R modulo B can be bisimulated as R,B-rewriting. The way the substitution θ in the **Replacement** rule of the inference system for $\to_{R,B}$ and $\to^*_{R,B}$ is computed in practice is to choose a position $p \in \mathcal{P}(t)$, and a θ_0 in the finite set $Match_B(l, t_p)$ and then extend θ_0 to θ incrementally by trying to satisfy each of the conditions in the rule from left to right. The crucial point is that we can start the search process to satisfy the first condition with the term $u_1\theta_0$. If that first condition can be satisfied, the instantiation of the extra variables in the pattern v_1 gives us an extended substitution θ_1 with which we can start the search for satisfying the second condition from the term $u_2\theta_1$, and so on. Various examples of deterministic and strongly determinisitc theories can be found in both [36] and, for rewrite theories, in [7]. Note that the requirement of strong determinism is essential for the Church-Rosser property, since the CTRS in Example 2 is confluent, terminating and deterministic, but *not* strongly deterministic.

Strong determinism, however, does not solve Problem (2), that is, the presence of "monsters" theories, where the usual computational intutions break down. Such monsters lurk also within the class of strongly deterministic theories. Here is an extremely simple monster, namely, the CTRS $\mathcal{R}$ with constants a, b, c and the single rule $a \to b$ *if* $a \to c$. Since its rewrite relation is empty, it is trivially confluent and terminating and, furthermore, since c is strongly irreducible, it is strongly deterministic. In particular, this theory belongs to the class described in Theorem 4 above and, a fortiori, to the class of confluent theories described in Theorem 5. What is wrong with this CTRS is that all terms are R-irreducible, yet, an interpreter trying to evaluate a will *loop forever*! Salvador Lucas and I argue in [28] that calling a a *normal form* of this CTRS is a bad joke, because the intuitive idea of a normal form is that it is the *result* of the normalization process; that is, of rewriting a term until no more reductions are possible; but this is precisely what we cannot do with a.

This is just the tip of the iceberg. The broader problem is that there are "monster" CTRSs $\mathcal{R}$ for which the set $Irr(\mathcal{R})$ of $\mathcal{R}$-irreducible terms is *not* recursively enumerable [39, 28]. So there is no hope, given an irreducible term t, to *know* that it is irreducible; and therefore no hope in general to know when a computation *terminates*. All this means that, in their full generality, the notions of irreducible term and of weakly terminating CTRS are highly problematic, since they violate all the usual intuitions and expectations about both irreducibility and termination. Furthermore, since irreducibility in general is undecidable, all hopes to *decide* equality of two terms by evaluating both to irreducible terms and comparing them for B-equality evaporate.

As argued in [28], the root of these problems is that in the entire literature on CTRSs *two* different notions —which are identical for TRSs but completely different for CTRSs— have been conflated: (i) that of an *R-irreducible* term; and (ii) that of a term in *R-normal form*. Conflating these two notions causes all kinds of *aporias*. In reality, given a CTRS $\mathcal{R}$ we can distinguish *two* sets, one contained in the other: $\mathsf{NF}(\mathcal{R}) \subseteq \mathit{Irr}(\mathcal{R})$, where $\mathsf{NF}(\mathcal{R})$ is the set of *normal forms* of $\mathcal{R}$. That is, every normal form is an irreducible term, but some irreducible terms such as, for example, the constant a in the last example are *not* normal forms. So, what is a normal form?

Definition 7 (Normal form, normal theory, weak normalization). *[28] Given an order-sorted conditional rewrite theory $\mathcal{R} = (\Sigma, B, R)$, a term t is called a* normal form *iff: (i) it is $\mathcal{R}$-irreducible (that is, there is no term u such that $t \rightarrow_{R/B} u$); and (ii) there are no infinite well-formed proof trees whose root has the form $t \rightarrow_{R/B} u$ for any u. That is, all proof attempts to perform a one-step rewrite on t modulo B fail in finite time.*

Let $\mathsf{NF}(\mathcal{R})$ denote the set of normal forms of $\mathcal{R}$, and $\mathit{Irr}(\mathcal{R})$ the set of irreducible terms of $\mathcal{R}$. $\mathcal{R}$ is called normal[12] *iff the inclusion $\mathsf{NF}(\mathcal{R}) \subseteq \mathit{Irr}(\mathcal{R})$ is an equality, i.e., iff every irreducible term is a normal form. If $\mathcal{R}$ is not normal, we call it* abnormal*.*

If every term s has a normal form, i.e., $s \rightarrow^{\star}_{R/B} t$ for some normal form t, then $\mathcal{R}$ is called weakly operationally terminating *(or* weakly normalizing*).*

All this leads to the notion of a *convergent* (resp. *weakly convergent*) conditional rewrite theory $\mathcal{R}$, which extends to the order-sorted, conditional and modulo cases the good properties of convergent theories in the unsorted and unconditional case.

Definition 8. *A normal, strongly deterministic conditional rewrite theory $\mathcal{R} = (\Sigma, B, R)$ satisfying the assumptions at the beginning of Section 4 is called* convergent *(resp.* weakly convergent*) iff R is: (i) sort-decreasing modulo B; (ii) closed under B-extensions; (iii) confluent modulo B; and (iv) operationally terminating (resp. weakly normalizing) modulo B.*

Problems (1)–(3) can be overcome by weakly convergent theories in the following way:

[12] Note that this meaning of "normal" is in open conflict with the definition of a *normal CTRS* (see, e.g., [36]) as a CTRS whose rewrite rules R are all of the form $l \rightarrow r$ *if* $\bigwedge_{i=1..n} u_i \rightarrow v_i$ with each v_j ground and, not only R-irreducible, but, furthermore, R_u-irreducible, where R_u is the set of unconditional rules obtained from R by dropping all conditions. Since these two meanings of "normal" are so different, no confusion should arise.

Theorem 6. *(Church Rosser Theorem modulo B with Decidable Equality). Let $\mathcal{R} = (\Sigma, B, \vec{E})$, associated to a conditional equational theory $(\Sigma, E \cup B)$, be normal, strongly deterministic, sort-decreasing modulo B, closed under B-extensions, and weakly normalizing modulo B. Then $\mathcal{R}$ is confluent modulo B iff for any Σ-terms t, t' we have the equivalence:*

$$t =_{E \cup B} t' \;\Leftrightarrow\; t \downarrow_{\vec{E}/B} t'.$$

Furthermore, for any weakly convergent and therefore Church-Rosser modulo B $\mathcal{R} = (\Sigma, B, \vec{E})$, if E is finite the equality relation $=_{E \cup B}$ is decidable.

Proof. $\mathcal{R} = (\Sigma, B, \vec{E})$ belongs to the class of theories in Theorem 5, so that its confluence modulo B holds iff the above equivalence holds.

Suppose now that $\mathcal{R} = (\Sigma, B, \vec{E})$ is weakly convergent and therefore by the above argument is Church-Rosser modulo B. By the finiteness of E and of B-matches, plus strong determinism (which allows incremental computation of substitutions used in **Replacement** steps), given a term t, its R, B-normal form $t!_{\vec{E},B}$ can be effectively computed up to B-equality by enumerating all rewrite proofs of goals of the form $t \rightarrow^{\star}_{R,B} u$ for any u in increasing order of proof size until encountering a proof of $t \rightarrow^{\star}_{R,B} u$ with u a term for which no further R, B-rewrites are possible, which exists and can be effectively identified by the weak normalization assumption. This, plus the decidability of $=_B$, makes $t!_{\vec{E},B} =_B t'!_{\vec{E},B}$ decidable. But since confluence modulo B gives us the equivalence $t \downarrow_{\vec{E}/B} t' \;\Leftrightarrow\; t!_{\vec{E},B} =_B t'!_{\vec{E},B}$, this makes $t =_{E \cup B} t'$ decidable, as desired. $\square$

Corollary 7. *(Agreement of Mathematical and Operational Semantics). Let $\mathcal{R} = (\Sigma, B, \vec{E})$, associated to a conditional equational theory $(\Sigma, E \cup B)$, be weakly convergent. Define the* canonical term algebra *$\mathcal{C}_{\vec{E},B}$ with $\mathcal{C}_{\vec{E}/B,s} = \{[t!_{\vec{E},B}]_B \mid t \in \mathcal{T}_\Sigma \;\wedge\; ls(t!_{\vec{E},B}) \leq s\}$ for each $s \in S$, and with operations $f : s_1 \ldots, s_n \longrightarrow s$ mapping each $([t_1!_{\vec{E},B}]_B, \ldots, [t_n!_{\vec{E},B}]_B)$ to the B-equivalence class $[f(t_1!_{\vec{E},B}, \ldots, t_n!_{\vec{E},B})!_{\vec{E},B}]_B$. Then $\mathcal{C}_{\vec{E},B}$ is a computable algebra*[13] *and we have an isomorphism of algebras:*

$$\mathcal{T}_{\Sigma/E \cup B} \;\cong\; \mathcal{C}_{\vec{E},B}.$$

This corollary manifests the full agreement between the initial algebra semantics furnished by $\mathcal{T}_{\Sigma/E \cup B}$ and the operational semantics by reduction to canonical form furnished by $\mathcal{C}_{\vec{E},B}$. Note that if we give a term t for evaluation to an interpreter, the result returned by the interpreter[14] is precisely $t!_{\vec{E},B}$.

[13] That is, an algebra where both the operations and the equality predicate are computable functions.

[14] For a convergent rewrite theory this is exactly the case. For a weakly convergent rewrite theory various evaluation strategies —including the inefficient one sketched out in the proof of Theorem 6— are possible, depending on $\mathcal{R}$. As explained in [28], several such strategies are supported by Maude under various assumptions on $\mathcal{R}$.

Therefore, the canonical term algebra $\mathcal{C}_{\vec{E},B}$ is precisely (up to B-equality) the algebra of *values* obtained by normalization modulo B and therefore a perfect algebraic summary of the operational semantics of the functional program $\mathcal{R} = (\Sigma, B, \vec{E})$.

Weakly convergent rewrite theories are a very general class of functional programs with good computational and decidability properties, including the above agreement between their mathematical and operational semantics. But how can we *check* that a conditional rewrite theory is convergent or weakly convergent? Closure under B-extensions is easy to check by the methods presented in this paper. As already mentioned, easily checkable sufficient conditions for sort-decreasingness modulo B (and tools [13]) also exist. Proof methods and tools to show operational termination of order-sorted rewrite theories have been developed in, e.g., [10, 12, 11, 28]; and sufficient conditions for a theory being normal have been studied in [28]. Checking of confluence modulo regular and linear axioms B with a finitary unification algorithm under the operational termination and closure under B-extensions assumptions, and a tool supporting such checking for various combinations of associativity, commutativity and identity axioms have been documented in [13]. Indeed, such checking amounts to checking the confluence of *conditional critical pairs* modulo the axioms B, and generalizes to the order-sorted and modulo cases a similar method for checking confluence of operationally terminating strongly deterministic CTRSs in [1].

7. Related Work and Conclusions

The most obviously related work are the various studies on unconditional equational rewriting, e.g., [19, 24, 26, 25, 37, 20, 21, 3, 22, 35, 23, 16]. For conditional rewriting modulo axioms, earlier work includes, e.g., [31, 4, 6, 13]. In particular, [4] considered conditional rewriting modulo B with the R,B-relation, but without studying B-extensions, and only under the assumptions of no extra variables in a rule's condition and of the simplifying termination [36] of R modulo B. In this work, conditional rewriting modulo axioms B has been considered in its fullest generality, namely, for order-sorted conditional rewrite theories with no restrictions whatsoever on either B or the rule's variables. However, due to the problematic nature of non-regular or non-linear axioms B, closure under B-extensions has been studied only for regular and linear axioms B. This could certainly be generalized; but, for the reasons already given in the paper and the additional reasons given below in the discussion of strong coherence, I see no compelling practical reasons to embark in such a generalization.

As already mentioned, in the unsorted and unconditional case, equi-termination of R/B and R,B, under what here is called the **Completeness** property, was shown in [16]. This result has been here broadly generalized to the operational equi-termination of R/B and R,B in the order-sorted and conditional case, assuming closure under B-extensions. This of course ensures **Completeness** and all other equivalent strict coherence properties. The study of such equivalent notions of strict coherence was initiated in [12, 13].

An interesting question is what to do to rewrite modulo axioms B when the equational axioms B fall beyond the pale of regular and linear equations and could even be conditional. As already mentioned, a generalization of the R, B relation in the style of, e.g., [20, 21, 3] is possible, but brings with it considerable technical difficulties and limitations: for example, bisimulation and equitermination are no longer possible. However, a different alternative exists, namely, *allowing two rewrite relations*. Within an equational logic setting, an early step in this direction was taken by Marché [29]. In the broader, not necessarily equational setting of rewriting logic, the strong coherence ideas initiated in [41] and substantially generalized in [13] have matured to a point where there is now ample evidence through many examples, language implementations, and tools such as the Maude Coherence Checker described in [13], supporting the claim that allowing two rewrite relations provides a much more flexible method of achieving, in an effectively computable way, the effect of rewriting modulo a very broad class of equational axioms, including conditional ones. The general idea is to decompose a rewrite theory $\mathcal{R}$ as $\mathcal{R} = (\Sigma, E \cup B, R)$, where: (i) B are regular and linear equations; (ii) $(\Sigma, B, \vec{E})$ is a convergent conditional rewrite theory exactly in the sense of Definition 8; and (iii) R are not necessarily equational and possibly conditional rewrite rules closed under B-extensions whose conditions are given an equational meaning and are solved by rewriting with $\vec{E}$ modulo B. There are, therefore, two rewrite relations, namely, a convergent equational one, $\rightarrow_{\vec{E},B}$, and a not necessarily equational one $\rightarrow_{R,B}$, which uses $\rightarrow_{\vec{E},B}$ as an auxiliary relation to evaluate its conditions. The right property ensuring the effect of rewriting with R modulo $E \cup B$ is the *strong coherence* of the rules R with the equational rules $\vec{E}$ modulo B [41, 13]. Furthermore, the conditions under which strong coherence can be achieved can be substantially relaxed for initial models where the equations E are sufficiently complete with respect to a subsignature $\Omega \subseteq \Sigma$ of constructor symbols [13]. The work presented here is actually directly relevant for strong coherence in the conditional case, since this requires both $\vec{E}$ and R to be closed under B-extensions.

In conclusion, this work has developed the foundations of conditional rewriting modulo axioms under very general assumptions about the type structure and the kinds of conditions allowed. This generality is not a caprice: it is needed and used in actual applications to rule-based languages and in formal specification and reasoning tools. But such generality should not obscure the obvious fact that, even in the unconditional case, new concepts and results are provided: the notion of stict coherence, and the specialization of all the subsequent results in the paper to the unconditional case afford a considerably simpler conceptual setting for rewriting modulo axioms in the (for all purposes most practical) case of regular and linear axioms B, than that provided by more general but considerably more complex approaches such as [20, 21, 3]. Issues such as operational equi-termination, the Church-Rosser Theorem, and executability and decidability have also been studied in detail.

Acknowledgements. Francisco Durán and Salvador Lucas were involved in the joint early development of the strict coherence ideas in [12, 13]. I thank Santiago Escobar and Salvador Lucas for their comments and suggestions to improve the paper.

[1] J. Avenhaus and C. Loría-Sáenz. On conditional rewrite systems with extra variables and deterministic logic programs. In F. Pfenning, editor, *Logic Programming and Automated Reasoning, 5th International Conference, LPAR 1994, Proceedings*, volume 822 of *Springer LNCS*, pages 215–229, 1994.

[2] F. Baader and T. Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.

[3] L. Bachmair and N. Dershowitz. Completion for rewriting modulo a congruence. *Theor. Comput. Sci.*, 67(2&3):173–201, 1989.

[4] A. Bockmayr. Conditional narrowing modulo of set of equations. *Appl. Algebra Eng. Commun. Comput.*, 4:147–168, 1993.

[5] P. Borovanský, C. Kirchner, H. Kirchner, and P.-E. Moreau. ELAN from a rewriting logic point of view. *Theoretical Computer Science*, 285:155–185, 2002.

[6] R. Bruni and J. Meseguer. Semantic foundations for generalized rewrite theories. *Theor. Comput. Sci.*, 360(1-3):386–414, 2006.

[7] M. Clavel, F. Durán, S. Eker, J. Meseguer, P. Lincoln, N. Martí-Oliet, and C. Talcott. *All About Maude – A High-Performance Logical Framework.* Springer LNCS Vol. 4350, 2007.

[8] N. Dershowitz and J.-P. Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume Formal Models and Sematics (B), pages 244–320. Elsevier, 1990.

[9] N. Dershowitz and D. Plaisted. Rewriting. In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, volume I, chapter 9, pages 535–610. Elsevier, 2001.

[10] F. Durán, S. Lucas, C. Marché, J. Meseguer, and X. Urbain. Proving operational termination of membership equational programs. *Higher-Order and Symbolic Computation*, 21(1-2):59–88, 2008.

[11] F. Durán, S. Lucas, and J. Meseguer. Methods for proving termination of rewriting-based programming languages by transformation. *Electr. Notes Theor. Comput. Sci.*, 248:93–113, 2009.

[12] F. Durán, S. Lucas, and J. Meseguer. Termination modulo combinations of equational theories. In *Frontiers of Combining Systems, 7th International Symposium, FroCoS 2009, Trento, Italy, September 16-18, 2009. Proceedings*, volume 5749 of *Lecture Notes in Computer Science*, pages 246–262. Springer, 2009.

[13] F. Durán and J. Meseguer. On the Church-Rosser and coherence properties of conditional order-sorted rewrite theories. *J. Algebraic and Logic Programming*, 81:816–850, 2012.

[14] S. Eker. Associative-commutative rewriting on large terms. In R. Nieuwenhuis, editor, *RTA*, volume 2706 of *Lecture Notes in Computer Science*, pages 14–29. Springer, 2003.

[15] K. Futatsugi and R. Diaconescu. *CafeOBJ Report*. World Scientific, AMAST Series, 1998.

[16] J. Giesl and D. Kapur. Dependency pairs for equational rewriting. In *RTA 2001*, volume 2051 of *Lecture Notes in Computer Science*, pages 93–108. Springer, 2001.

[17] J. Goguen and J. Meseguer. Order-sorted algebra I: Equational deduction for multiple inheritance, overloading, exceptions and partial operations. *Theoretical Computer Science*, 105:217–273, 1992.

[18] J. Goguen, T. Winkler, J. Meseguer, K. Futatsugi, and J.-P. Jouannaud. Introducing OBJ. In *Software Engineering with OBJ: Algebraic Specification in Action*, pages 3–167. Kluwer, 2000.

[19] G. Huet. Confluent reductions: Abstract properties and applications to term rewriting systems. *Journal of the Association for Computing Machinery*, 27:797–821, 1980. Preliminary version in *18th Symposium on Mathematical Foundations of Computer Science*, 1977.

[20] J.-P. Jouannaud. Confluent and coherent equational term rewriting systems: Application to proofs in abstract data types. In G. Ausiello and M. Protasi, editors, *CAAP*, volume 159 of *Lecture Notes in Computer Science*, pages 269–283. Springer, 1983.

[21] J.-P. Jouannaud and HélèneKirchner. Completion of a set of rules modulo a set of equations. *SIAM Journal of Computing*, 15:1155–1194, November 1986.

[22] J.-P. Jouannaud and J. Li. Church-Rosser properties of normal rewriting. In P. Cégielski and A. Durand, editors, *CSL*, volume 16 of *LIPIcs*, pages 350–365. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2012.

[23] C. Kirchner and H. Kirchner. Rewriting, Solving, Proving. Unpublished book draft available online, 2006.

[24] D. Lankford and A. Ballantyne. Decision procedures for simple equational theories with a commutative axiom: complete sets of commutative reductions. Technical Report ATP-35, Department of Mathematics and Computer Science, Univ. of Texas, Austin, 1977.

[25] D. Lankford and A. Ballantyne. Decision procedures for simple equational theories with commutative-associative axioms: complete sets of commutative-associative reductions. Technical Report ATP-39, Department of Mathematics and Computer Science, Univ. of Texas, Austin, 1977.

[26] D. Lankford and A. Ballantyne. Decision procedures for simple equational theories with permutative axioms: complete sets of permutative reductions. Technical Report ATP-37, Department of Mathematics and Computer Science, Univ. of Texas, Austin, 1977.

[27] S. Lucas, C. Marché, and J. Meseguer. Operational termination of conditional term rewriting systems. *Information Processing Letters*, 95(4):446–453, 2005.

[28] S. Lucas and J. Meseguer. Strong and weak operational termination of order-sorted rewrite theories. In *Proc. WRLA 2014*. Springer LNCS, to appear, 2014.

[29] C. Marché. Normalised rewriting and normalised completion. In *Proc. LICS'94*, pages 394–403. IEEE, 1994.

[30] J. Meseguer. General logics. In H.-D. E. et al., editor, *Logic Colloquium'87*, pages 275–329. North-Holland, 1989.

[31] J. Meseguer. Conditional rewriting logic as a unified model of concurrency. *Theoretical Computer Science*, 96(1):73–155, 1992.

[32] J. Meseguer. Membership algebra as a logical framework for equational specification. In F. Parisi-Presicce, editor, *Proc. WADT'97*, pages 18–61. Springer LNCS 1376, 1998.

[33] J. Meseguer. Twenty years of rewriting logic. *J. Algebraic and Logic Programming*, 81:721–781, 2012.

[34] J. Meseguer and J. Goguen. Initiality, induction and computability. In M. Nivat and J. Reynolds, editors, *Algebraic Methods in Semantics*, pages 459–541. Cambridge University Press, 1985.

[35] P. Narendran, M. Subramanian, and Q. Guo. Observations on equational rewriting. Unpublished manuscript, ca. 1994.

[36] E. Ohlebusch. *Advanced Topics in Term Rewriting*. Springer Verlag, 2002.

[37] G. E. Peterson and M. E. Stickel. Complete sets of reductions for some equational theories. *Journal of the Association Computing Machinery*, 28(2):233–264, 1981.

[38] C. Rocha, J. Meseguer, and C. Muñoz. Rewriting Modulo SMT and Open System Analysis. In *Proc. WRLA 2014*. Springer LNCS, to appear, 2014.

[39] Terese. *Term Rewriting Systems*. Cambridge University Press, 2003.

[40] A. van Deursen, J. Heering, and P. Klint. *Language Prototyping: An Algebraic Specification Approach.* World Scientific, 1996.

[41] P. Viry. Equational rules for rewriting logic. *Theoretical Computer Science*, 285:487–517, 2002.

[42] T. Yamada, J. Avenhaus, C. Loría-Sáenz, and A. Middeldorp. Logicality of conditional rewrite systems. *Theor. Comput. Sci.*, 236(1-2):209–232, 2000.