Up-to Techniques for Weak Bisimulation

Damien Pous

Up-to Techniques for Weak Bisimulation*

Damien Pous

ENS Lyon

Abstract. Up-to techniques have been introduced to enhance the bisimulation proof method for establishing bisimilarity results. While up-to techniques for strong bisimilarity are well understood, in the weak case they come as a collection of unrelated results, and lack a unified presentation. We propose a uniform and modular theory of up-to techniques for weak bisimulation that captures existing proof technology and introduces new techniques. Some proofs rely on non trivial – and new – commutation results based on termination guarantees.

Introduction

Bisimilarity is a widely used behavioural equivalence in concurrency theory. It can be seen as the finest extensional equivalence that enjoys a natural formulation and nice mathematical properties. Bisimilarity can be defined as the greatest *bisimulation*. Given a *labelled transition system* (LTS), allowing one to write transitions between states of the form $P \stackrel{\alpha}{\to} P'$ (meaning that a state P can perform an action α and evolve to P'), we say that a relation $\mathcal{R}$ between states is a bisimulation whenever the leftmost diagram below holds: if P and Q are related by $\mathcal{R}$ and $P \stackrel{\alpha}{\to} P'$, there is Q' such that $Q \stackrel{\alpha}{\to} Q'$ and $\mathcal{R}$ relates P' and Q', and symmetrically for the transitions of Q.

$$\begin{array}{ccc} P & \mathcal{R} & Q \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha} \\ P' & \mathcal{R} & Q' \end{array} \qquad \begin{array}{ccc} P & \mathcal{R} & Q \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha} \\ P' & \mathcal{F}(\mathcal{R}) & Q' \end{array} \qquad \begin{array}{ccc} P & \mathcal{R} & Q \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha} \\ P' & \mathcal{S} & Q' \end{array} \qquad \begin{array}{ccc} P & \mathcal{R} & Q \\ {\scriptstyle\alpha}\downarrow & & \Downarrow{\scriptstyle\alpha} \\ P' & \mathcal{R} & Q' \end{array}$$

Bisimulation is the most popular technique to establish bisimilarity results: to prove that P and Q are bisimilar (written $P \sim Q$), exhibit a bisimulation $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$. *Up-to techniques for bisimulation* have been introduced to alleviate the task of bisimulation proofs, by working with smaller relations. The proof scheme is shown on the second diagram above: a correct up-to technique is given by a function $\mathcal{F}$ from relations to relations such that if we prove that $\mathcal{R}$ 'evolves to' $\mathcal{F}(\mathcal{R})$, then we know that $\mathcal{R} \subseteq \sim$. The advantage is that $\mathcal{R}$ need not be a bisimulation (and can be 'much smaller' than a bisimulation). The notion of evolution of relations (depicted on the third diagram, where $\mathcal{R}$ evolves to $\mathcal{S}$ — its informal meaning is made precise below) serves as the basis of [8], where a

* Author's version of the paper published by Springer in Proc. ICALP'05, available at `http://dx.doi.org/10.1007/11523468_59`.

general theory of up-to techniques for bisimulation is presented. The corresponding framework gives a unified and modular view of known up-to techniques, that can be combined together to yield powerful proof techniques for bisimilarity.

Up to now, we have implicitly been referring to *strong* bisimulation. When analysing nontrivial systems, however, one is often interested in the *weak* version, where a special action, called τ, is isolated, and the game of bisimulation is redefined by abstracting over τ transitions (τ is treated as a *silent* action, while other actions are *visible*). In the weak version of the bisimulation game, as shown on the rightmost diagram above, Q responds to $P \stackrel{\alpha}{\rightarrow} P'$ by performing an $\stackrel{\alpha}{\Rightarrow}$ transition: this means that Q can do zero or several silent steps before and after the transition along α, or even not move at all in the case where $\alpha = \tau$ (and symmetrically when Q offers a challenge). One might then want to follow the same path as above: redefine the evolution of relations, and look for some functions $\mathcal{F}$ that yield correct up-to proof techniques for weak bisimilarity (written $\approx$). An important motivation for doing so is that in general, weak bisimulation proofs tend to be much larger than strong bisimulation proofs, so that having up-to techniques for the weak case is at least as important as in the strong case.

Unfortunately, in the weak case, irregularities appear, the paradigmatic example being given by the unsoundness of the 'weak bisimulation up to weak bisimilarity' proof technique. We recall the counterexample, from [9]. We suppose that the reader is familiar with CCS, and define $\mathcal{R} \triangleq \{(\tau.a, 0)\}$. Let us show that $\mathcal{R}$ is a weak bisimulation up to $\approx$, i.e., that $\mathcal{R}$ evolves to $\approx\mathcal{R}\approx$ (we use juxtaposition to denote relation composition). The right process, 0, cannot move. The only move the left process can do is a τ transition to a, to which the right process answers by no move, and we get the pair $(a, 0)$. Now since we are reasoning up to $\approx$, and since $a \approx \tau.a$, we are allowed to replace this pair with $(\tau.a, 0)$, and we are back in $\mathcal{R}$. Nevertheless, we obviously cannot conclude that $\tau.a$ and 0 are bisimilar processes.

Novel and useful proof techniques have been introduced to circumvent this difficulty [9, 3], notably based on the expansion preorder [1], that allows one to avoid situations where one can 'undo a τ transition' as in the example above. However, as we have experienced in a recent study [4], in some cases reasoning up to expansion is not possible. The intuitive reason can be formulated as follows: when a process P expands a process Q, P has to be more efficient (in terms of internal computations, represented by silent transitions) than Q *at every step*. Typically, expansion is a well suited relation to get rid of intermediate computation steps that do not affect the behaviour of the system. However, it is common (in particular, it is the case in [4]) that along such transitions, an increased efficiency is achieved at the cost of some initial computation. Because of its 'very controlled' nature, expansion fails in handling this kind of pre-calculation techniques.

In the present work, we develop a theory of up-to techniques for weak bisimulation that enjoys nice properties in terms of generality and modularity, and we introduce new useful proof techniques for weak bisimilarity that can be used in that framework.

We start by adapting the work of [7] to the weak case, yielding the notion of *monotonic function* over relations. We explore the class of monotonic functions, and argue that it is too restrictive. We are thus led to relax the notion of monotonicity, and introduce *weakly monotonic* functions, for which up-to techniques can be applied only to reason about visible actions (those that cannot be undone by $\approx$). We then show under which conditions monotonic and weakly monotonic functions can be combined together to obtain sound proof techniques. The resulting framework gives a unified and modular account of existing technology for weak bisimulation proofs. Beyond that, we validate some proof principles, such as 'up to bisimilarity and transitivity on visible actions', that to our knowledge had not been proposed before.

We then attack the question of finding alternatives to the expansion relation to handle τ transitions in weak bisimulation proofs. We propose an *up to controlled bisimulation* technique. The notion of controlled bisimulation intuitively captures the idea of avoiding 'going back in time' in bisimulation proofs. We introduce *relaxed expansion*, a co-inductively defined relation that is a controlled bisimulation and is coarser than expansion. We also propose two new proof principles for which the control on τ steps exploits a different kind of argument, based on termination guarantees. The corresponding correctness proofs are best formulated as rewriting results, that are technically difficult and may be of interest *per se*; we therefore describe them in that setting in a dedicated section. All our results have been formally checked using the Coq proof assistant [7]. For the lack of space, most are omitted in this extended abstract. They can be found in [5].

Outline of the paper. In Sect. 1, we introduce some necessary background and show where the approach of [8] breaks when adapted to the weak case. We develop our theory of up-to techniques for weak bisimulation in Sect. 2, introducing monotonic and weakly monotonic functions. In Sect. 3 we introduce controlled simulations and present new up-to techniques based on this notion. The correctness of some of these techniques is supported by the proofs given in Sect. 4, which are formulated in the setting of commutation results. We give final remarks in Sect. 5.

1 The Problem of "Weak Bisimulation Up to"

1.1 Labelled Transition Systems, Relations, Evolution

We consider a labelled transition system (LTS) $(\mathcal{P}, \mathcal{L}, \rightarrow)$, with domain $\mathcal{P}$, *labels* or *actions* in $\mathcal{L}$ and transition relation $\rightarrow \subseteq \mathcal{P} \times \mathcal{L} \times \mathcal{P}$. The elements of $\mathcal{P}$ are called *processes* and are denoted by P, Q. We distinguish a *silent action*, $\tau \in \mathcal{L}$. We let α, β (resp. a, b) range over actions, in $\mathcal{L}$ (resp. *visible actions*, in $\mathcal{L}\backslash\{\tau\}$). We write $P \xrightarrow{\alpha} Q$ when $(P, \alpha, Q) \in \rightarrow$ (so that $P \xRightarrow{a} Q$ stands for a transition of P along a visible action a).

We let $\mathcal{R}, \mathcal{S}, \mathcal{B}, \mathcal{E}$ range over binary relations (simply called *relations* in the sequel) on processes, and denote respectively by $\mathcal{R}^+, \mathcal{R}^=, \mathcal{R}^\star$ the transitive, reflexive, transitive and reflexive closure of the relation $\mathcal{R}$. $P\ \mathcal{R}\ Q$ stands for $(P,Q) \in \mathcal{R}$. The composition of two relations $\mathcal{R}$ and $\mathcal{S}$, written $\mathcal{RS}$, is defined by $\mathcal{RS} \triangleq \{(P,Q)$ s.t. $P\ \mathcal{R}\ T$ and $T\ \mathcal{S}\ Q$ for some process $T\}$. We will also need the inverse of a relation: $\mathcal{R}^{-1} \triangleq \{(P,Q)$ s.t. $Q\ \mathcal{R}\ P\}$. $\mathcal{I}$ will denote the identity relation. We say that $\mathcal{R}$ *contains* $\mathcal{S}$ (alternatively, that $\mathcal{S}$ is contained in $\mathcal{R}$), written $\mathcal{S} \subseteq \mathcal{R}$, if $P\ \mathcal{S}\ Q$ implies $P\ \mathcal{R}\ Q$. A relation $\mathcal{R}$ *terminates* if there is no infinite sequence $P_1, P_2 \ldots$ such that $\forall i, P_i\ \mathcal{R}\ P_{i+1}$.

Definition 1.1 (weak transitions). *The* weak transition relation*, written* $\stackrel{\alpha}{\Rightarrow}$*, is defined as the reflexive transitive closure of* $\stackrel{\tau}{\rightarrow}$ *when* $\alpha = \tau$*, and the composition* $\stackrel{\tau}{\Rightarrow}\stackrel{\alpha}{\rightarrow}\stackrel{\tau}{\Rightarrow}$ *for* $\alpha = a \in \mathcal{L}\backslash\{\tau\}$*.*

Definition 1.2 (evolution). *Let* α *be an action and* $\mathcal{R}, \mathcal{S}$ *two relations. We say that* $\mathcal{R}$ α-evolves *to* $\mathcal{S}$*, if whenever* $P\ \mathcal{R}\ Q$*,* $P \stackrel{\alpha}{\rightarrow} P'$ *implies* $Q \stackrel{\alpha}{\Rightarrow} Q'$ *and* $P'\ \mathcal{S}\ Q'$ *for some* Q'*. Given two relations* $\mathcal{R}$ *and* $\mathcal{S}$*, we say that:*

- $\mathcal{R}$ evolves to $\mathcal{S}$*, denoted by* $\mathcal{R} \rightarrowtail \mathcal{S}$*, if* $\mathcal{R}$ α*-evolves to* $\mathcal{S}$ *for all* $\alpha \in \mathcal{L}$*,*
- $\mathcal{R}$ evolves silently *to* $\mathcal{S}$*, denoted by* $\mathcal{R} \stackrel{\tau}{\rightarrowtail} \mathcal{S}$*, if* $\mathcal{R}$ τ*-evolves to* $\mathcal{S}$*,*
- $\mathcal{R}$ evolves visibly *to* $\mathcal{S}$*, denoted by* $\mathcal{R} \stackrel{v}{\rightarrowtail} \mathcal{S}$*, if* $\mathcal{R}$ a*-evolves to* $\mathcal{S}$ *for all* $a \in \mathcal{L}\backslash\{\tau\}$*.*

Our notion of evolution is the 'asymmetric' version of *progression* in [8]: $\mathcal{R}$ progresses to $\mathcal{S}$ in the sense of [8] iff $\mathcal{R}$ evolves to $\mathcal{S}$ and $\mathcal{R}^{-1}$ evolves to $\mathcal{S}^{-1}$.

In the following, we build a theory of up-to techniques to reason about simulations. This leads to simpler developments, and we show at the end of each section how to use the results to obtain proof techniques for bisimulation.

In the definition below, and in the remainder of the paper, we implicitly refer to *weak* relations. There are several equivalent definitions of bisimilarity. The following directly gives the standard way to prove a bisimilarity result between two processes P and Q: exhibit a bisimulation $\mathcal{R}$ containing the pair (P,Q).

Definition 1.3 (simulation, bisimulation, expansion). *Let* $\mathcal{R}$ *be a relation,* $\mathcal{R}$ *is a* simulation *(resp.* silent simulation*) if* $\mathcal{R} \rightarrowtail \mathcal{R}$ *(resp.* $\mathcal{R} \stackrel{\tau}{\rightarrowtail} \mathcal{R}$*).*
$\mathcal{R}$ *is a* bisimulation *if* $\mathcal{R}$ *and* $\mathcal{R}^{-1}$ *are simulations. Two processes* P *and* Q *are* bisimilar*, written* $P \approx Q$*, if* $P\ \mathcal{R}\ Q$ *for some bisimulation* $\mathcal{R}$*.*

Expansion*, denoted by* $\succsim$*, is the largest relation such that* $\succsim^{-1}$ *is a simulation, and, whenever* $P \succsim Q$*,*

1. $P \stackrel{\tau}{\rightarrow} P'$ *implies* $Q \stackrel{\tau}{\rightarrow} Q'$ *and* $P' \succsim Q'$ *for some* Q'*, or* $P' \succsim Q$*;*
2. $P \stackrel{a}{\rightarrow} P'$ *implies* $Q \stackrel{a}{\rightarrow} Q'$ *and* $P' \precsim Q'$ *for some* Q'*.*

1.2 The Difficulty in the Weak Case

We now adapt the theory of up-to techniques of [8] to the weak case, and show where the difficulties arise. We let $\mathcal{F}, \mathcal{G}$ range over *functions* from relations to relations. We say that $\mathcal{F}$ *contains* $\mathcal{G}$, written $\mathcal{G} \subseteq \mathcal{F}$, if $\mathcal{G}(\mathcal{R}) \subseteq \mathcal{F}(\mathcal{R})$ for any

relation $\mathcal{R}$. Given a relation $\mathcal{S}$, we define *identity* ($\mathcal{U}$), *constant-to-$\mathcal{S}$* ($\tilde{\mathcal{S}}$), *$\mathcal{S}$-left-chaining* ($\mathcal{S}\bullet$) and *$\mathcal{S}$-right-chaining* ($\bullet\mathcal{S}$) as follows:

$$\mathcal{U}(\mathcal{R}) \triangleq \mathcal{R} \qquad \tilde{\mathcal{S}}(\mathcal{R}) \triangleq \mathcal{S} \qquad \mathcal{S}\bullet(\mathcal{R}) \triangleq \mathcal{S}\mathcal{R} \qquad \bullet\mathcal{S}(\mathcal{R}) \triangleq \mathcal{R}\mathcal{S}$$

We define four *constructors*, i.e., functions from functions to functions: *composition* ($\circ$), *union* ($\cup$), *iteration* ($*$) and *chaining* ($\frown$), as follows:

$$(\mathcal{F}\circ\mathcal{G})(\mathcal{R}) \triangleq \mathcal{F}(\mathcal{G}(\mathcal{R})) \qquad (\mathcal{F}^0)(\mathcal{R}) \triangleq \mathcal{R}$$
$$(\mathcal{F}\cup\mathcal{G})(\mathcal{R}) \triangleq \mathcal{F}(\mathcal{R}) \cup \mathcal{G}(\mathcal{R}) \qquad (\mathcal{F}^{n+1})(\mathcal{R}) \triangleq \mathcal{F}^n(\mathcal{R}) \cup \mathcal{F}(\mathcal{F}^n(\mathcal{R}))$$
$$(\mathcal{F}\frown\mathcal{G})(\mathcal{R}) \triangleq \mathcal{F}(\mathcal{R})\mathcal{G}(\mathcal{R}) \qquad (\mathcal{F}^*)(\mathcal{R}) \triangleq \bigcup_{n\geq 0}\mathcal{F}^n(\mathcal{R})$$

Definition 1.4 (monotonicity). *A function $\mathcal{F}$ is* monotonic *if $\mathcal{R}\subseteq\mathcal{S}$ entails $\mathcal{F}(\mathcal{R})\subseteq\mathcal{F}(\mathcal{S})$ and the following conditions hold:*

$$(1)\ \begin{cases}\mathcal{R} \rightarrowtail^{\tau} \mathcal{S}\\ \mathcal{R}\subseteq\mathcal{S}\end{cases} \Rightarrow \mathcal{F}(\mathcal{R}) \rightarrowtail^{\tau} \mathcal{F}(\mathcal{S}) \qquad (2)\ \begin{cases}\mathcal{R} \rightarrowtail \mathcal{S}\\ \mathcal{R}\subseteq\mathcal{S}\end{cases} \Rightarrow \mathcal{F}(\mathcal{R}) \rightarrowtail^{v} \mathcal{F}(\mathcal{S})$$

This slightly strengthens the notion of *respectfulness* found in [8], in which the two kinds of transitions are treated uniformly. While the results of this section would hold using respectful functions, we will need this separation between silent and visible actions in Sect. 2.2.

Proposition 1.5 (correctness of monotonic functions). *Let $\mathcal{F}$ be a monotonic function. If $\mathcal{R} \rightarrowtail \mathcal{F}(\mathcal{R})$, then $\mathcal{F}^*(\mathcal{R})$ is a simulation.*

This proposition ensures that a monotonic function provides a sound up-to technique: whenever we can prove that $\mathcal{R}$ evolves to $\mathcal{F}(\mathcal{R})$, then $\mathcal{R}$ is contained in $\mathcal{F}^*(\mathcal{R})$, which is a simulation. We now exhibit some monotonic functions, and show how to combine them to obtain more powerful techniques.

Lemma 1.6. *Let $\mathcal{S}$ be a simulation, $\mathcal{U}$, $\tilde{\mathcal{S}}$, $\bullet\mathcal{S}$ and $\gtrsim\bullet$ are monotonic functions.*

In the sequel, we will say that a constructor *respects* a predicate P over functions, if, given arguments that satisfy P, it returns a function satisfying P.

Lemma 1.7. *Constructors $\circ$, $\cup$ and $*$ respect monotonicity.*

We can now apply our framework to reason about bisimulation relations, and revisit a result from [9]. We show that the proof becomes elementary.

Theorem 1.8. *If $\mathcal{R} \rightarrowtail \gtrsim \mathcal{R}^{=}\approx$ and $\mathcal{R}^{-1} \rightarrowtail \gtrsim (\mathcal{R}^{-1})^{=}\approx$, then $\mathcal{R}\subseteq\approx$.*

Proof. Using the previous results, $\mathcal{F}(\mathcal{R}) \triangleq \gtrsim \mathcal{R}^{=}\approx$ is monotonic, and $\mathcal{F}^*(\mathcal{R})$ and $\mathcal{F}^*(\mathcal{R}^{-1})$ are simulations. Then $\approx\mathcal{F}^*(\mathcal{R})$ and $\mathcal{F}^*(\mathcal{R}^{-1})\approx$ are simulations. We check that $(\approx\mathcal{F}^*(\mathcal{R}))^{-1} = \mathcal{F}^*(\mathcal{R}^{-1})\approx$, so that $\mathcal{R} \subseteq \approx\mathcal{F}^*(\mathcal{R}) \subseteq \approx$. □

The transitivity problem. The $\approx$-left-chaining function is not monotonic. As a consequence, the chaining constructor does not respect monotonicity in general. Indeed, when trying to prove the monotonicity of $\approx\bullet$, we lack some hypotheses about silent transitions to close the corresponding diagram.

2 A Smooth Theory for the Weak Case

2.1 A Weaker Notion of Monotonicity

When looking at the counterexample given in the Introduction, we can observe that the problem is related to silent transitions: unlike visible transitions, they can be cancelled by $\approx$. We now exploit this observation to relax the definition of monotonicity, which leads to a smoother theory, where reasoning *up to weak bisimilarity* is allowed, but on visible actions only.

Definition 2.1 (weak monotonicity). *A function $\mathcal{F}$ is* weakly monotonic *if $\mathcal{R} \subseteq \mathcal{S}$ entails $\mathcal{F}(\mathcal{R}) \subseteq \mathcal{F}(\mathcal{S})$ and the following conditions hold:*

$$(1)\ \ \mathcal{R} \stackrel{\tau}{\rightarrowtail} \mathcal{R} \Rightarrow \mathcal{F}(\mathcal{R}) \stackrel{\tau}{\rightarrowtail} \mathcal{F}(\mathcal{R}) \qquad (2) \begin{cases} \mathcal{R} \stackrel{\tau}{\rightarrowtail} \mathcal{R}, \mathcal{R} \stackrel{\upsilon}{\rightarrowtail} \mathcal{S} \\ \mathcal{S} \stackrel{\tau}{\rightarrowtail} \mathcal{S},\ \ \mathcal{R} \subseteq \mathcal{S} \end{cases} \Rightarrow \mathcal{F}(\mathcal{R}) \stackrel{\upsilon}{\rightarrowtail} \mathcal{F}(\mathcal{S})$$

The main difference w.r.t. Definition 1.4 is in clause (1): instead of respecting silent evolutions, a weakly monotonic function has to respect silent simulations. On the visible side (2), we suppose that $\mathcal{R}$ and $\mathcal{S}$ are silent simulations. The immediate consequence of these modifications appears in the following result: the up-to function may only be used on visible evolutions, and the candidate relation $\mathcal{R}$ has to be a silent simulation.

Proposition 2.2 (correctness of weakly monotonic functions). *Let $\mathcal{F}$ be weakly monotonic. If $\mathcal{R} \stackrel{\tau}{\rightarrowtail} \mathcal{R}$, and $\mathcal{R} \stackrel{\upsilon}{\rightarrowtail} \mathcal{F}(\mathcal{R})$, then $\mathcal{F}^*(\mathcal{R})$ is a simulation.*

Now we study the class of weakly monotonic functions: the following lemma ensures that the functions given by Lemma 1.6 can be used in the setting of weakly monotonic functions. Furthermore, weakly monotonic functions can be composed using the most important constructors:

Lemma 2.3. *Any monotonic function is weakly monotonic. Composition ($\circ$), union ($\cup$), iteration ($*$) and chaining ($\frown$) respect weak monotonicity.*

The closure under the chaining constructor naturally suggests the use of interesting up-to techniques, and in particular *up to transitivity*, given by $\mathcal{F}(\mathcal{R}) = \mathcal{R}^\star$, and *up to weak bisimilarity*, using $\mathcal{F}(\mathcal{R}) = \approx \mathcal{R} \approx$.

2.2 Combining Monotonicity and Weak Monotonicity

In introducing weakly monotonic functions, we have restricted the use of up-to techniques to visible steps. We show how to develop further this approach by combining a monotonic function and a weakly monotonic function so as to employ constrained up-to techniques on silent steps, and full-fledged up-to techniques on visible steps.

Proposition 2.4 (unified up-to technique). *Let $\mathcal{F}$ be monotonic and $\mathcal{G}$ be weakly monotonic, and suppose further that $\mathcal{F} \subseteq \mathcal{G}$.*

If $\mathcal{R} \stackrel{\tau}{\rightarrowtail} \mathcal{F}(\mathcal{R})$ and $\mathcal{R} \stackrel{\upsilon}{\rightarrowtail} \mathcal{G}(\mathcal{R})$, then $(\mathcal{G}^*)^*(\mathcal{R})$ is a simulation.

In this result, we have to iterate $\mathcal{G}$ twice for technical reasons (see [5] for details). The following theorem is the counterpart of Theorem 1.8 in the richer setting we have introduced:

Theorem 2.5. *If* $\begin{cases} \mathcal{R} \rightarrowtail^{\tau} \gtrsim \mathcal{R}^{=} \approx \\ \mathcal{R} \rightarrowtail^{v} (\mathcal{R} \cup \approx)^{\star} \end{cases}$ *and* $\begin{cases} \mathcal{R}^{-1} \rightarrowtail^{\tau} \gtrsim \mathcal{R}^{-1=} \approx \\ \mathcal{R}^{-1} \rightarrowtail^{v} (\mathcal{R}^{-1} \cup \approx)^{\star} \end{cases}$ *then* $\mathcal{R} \subseteq \approx$.

We thus have a modular theory of up-to techniques for weak bisimulation that follows the approach for the strong case in [8]. Technically, the main improvement over previous works is the ability to exploit weaker hypotheses when reasoning about visible steps: for instance, *up to transitivity* ($\mathcal{R} \rightarrowtail^{v} \mathcal{R}^{\star}$) and *up to weak bisimilarity* ($\mathcal{R} \rightarrowtail^{v} \approx \mathcal{R} \approx$) techniques entail valid proof methods.

3 Beyond Expansion

3.1 Controlled Relations

In this section, we enrich our framework with the possibility to use alternatives to $\gtrsim$ (which is the best we can do using Theorem 2.5) to handle τ transitions in bisimulation proofs. We define a class of relations that are controlled w.r.t. silent transitions, meaning that they prevent silent steps from being cancelled in an up-to bisimulation game.

The left-chaining functions associated to such relations are not weakly monotonic, and we thus have to depart from the theory we have developed so far. Roughly, a controlled relation is defined as a relation that induces a correct proof technique when used as a left-chaining up-to technique. The following technical definition introduces a uniform way to plug a non weakly monotonic left-chaining function into our setting.

Definition 3.1 (controlled relation). *We says that* $\mathcal{B}$ *is a* controlled relation *if the following holds for all relations* $\mathcal{R}$, $\mathcal{S}$*:*

$$(1)\ \mathcal{R} \rightarrowtail^{\tau} \mathcal{B}^{\star}\mathcal{R} \ \Rightarrow\ \mathcal{B}^{\star}\mathcal{R} \rightarrowtail^{\tau} \mathcal{B}^{\star}\mathcal{R} \qquad (2) \begin{cases} \mathcal{R} \rightarrowtail^{\tau} \mathcal{B}^{\star}\mathcal{R} \\ \mathcal{R} \rightarrowtail^{v} \mathcal{S}, \quad \mathcal{S} \rightarrowtail^{\tau} \mathcal{S} \end{cases} \Rightarrow\ \mathcal{B}^{\star}\mathcal{R} \rightarrowtail^{v} \mathcal{B}^{\star}\mathcal{S}\,.$$

Remark 3.2. Note that a controlled relation need not be a simulation. However, by taking $\mathcal{R} = \mathcal{S} = \mathcal{I}$, we see that if $\mathcal{B}$ is controlled, then $\mathcal{B}^{\star}$ is a simulation. Also, the union of two controlled relations is not necessarily a controlled relation. Thus, this does not a priori induce a notion of *controlled bisimilarity*.

We say that $\mathcal{B}$ is a *controlled bisimulation* if it is a controlled relation contained in bisimilarity.

We now show how controlled relations can be used in simulation proofs.

Definition 3.3 (transparency). *Given a relation* $\mathcal{B}$ *and a function* $\mathcal{F}$, $\mathcal{F}$ *is* $\mathcal{B}$-transparent *if* $\mathcal{F}(\mathcal{B}^{\star}\mathcal{R}) \subseteq \mathcal{B}^{\star}\mathcal{F}(\mathcal{R})$ *for any relation* $\mathcal{R}$.

$\mathcal{F}$ *is* transparent *if it is* $\mathcal{B}$*-transparent for any relation* $\mathcal{B}$.

Proposition 3.4 (up to controlled relation). *Let $\mathcal{F}$ and $\mathcal{G}$ be two functions, and $\mathcal{B}$ a relation such that: $\mathcal{B}$ is a controlled relation, $\mathcal{F}$ is monotonic and $\mathcal{B}$-transparent, $\mathcal{G}$ is weakly monotonic. Suppose moreover that $\mathcal{G}$ contains $\mathcal{F}$ and $\mathcal{B}^\star\bullet$. If $\mathcal{R} \rightarrowtail^{\tau} \mathcal{B}^\star\mathcal{F}(\mathcal{R})$ and $\mathcal{R} \rightarrowtail^{v} \mathcal{G}(\mathcal{R})$, then $(\mathcal{G}^*)^*(\mathcal{R})$ is a simulation.*

Lemma 3.5. *The identity and all $\mathcal{S}$-right-chaining functions are transparent. If $\mathcal{B} \subseteq \mathcal{S}$ then the constant-to-$\mathcal{S}$ function is $\mathcal{B}$-transparent.*

The composition, union and iteration constructors respect $\mathcal{B}$-transparency.

In practise, we will work with $\mathcal{S} = \approx$ and require that $\mathcal{B} \subseteq \approx$, so that condition $\mathcal{B} \subseteq \mathcal{S}$ will be satisfied.

Also notice that $\gtrsim\bullet$, the expansion-left-chaining function, is not transparent in general. This hence prevents us from encompassing the up to expansion proof technique in the statement of the following theorem.

Theorem 3.6. *Let $\mathcal{B}$ be a controlled bisimulation.*

$$\text{If } \begin{cases} \mathcal{R} \rightarrowtail^{\tau} \mathcal{B}^\star\mathcal{R}^{=}\approx \\ \mathcal{R} \rightarrowtail^{v} (\mathcal{R} \cup \approx)^\star \end{cases} \text{ and } \begin{cases} \mathcal{R}^{-1} \rightarrowtail^{\tau} \mathcal{B}^\star\mathcal{R}^{-1=}\approx \\ \mathcal{R}^{-1} \rightarrowtail^{v} (\mathcal{R}^{-1} \cup \approx)^\star \end{cases} \text{ then } \mathcal{R} \subseteq \approx.$$

This theorem is the counterpart of Theorem 2.5 using a controlled bisimulation instead of $\gtrsim$. A refined version of this result, in which two distinct controlled bisimulations are used for the silent evolutions of $\mathcal{R}$ and $\mathcal{R}^{-1}$, also holds. This can be useful in particular because the class of controlled bisimulations is not closed under union, as explained in Remark 3.2.

The remainder of the section is devoted to the construction of controlled relations.

3.2 Relaxed Expansion

Definition 3.7 (relaxed expansion). *A relation $\mathcal{E}$ is a* relaxed expansion *if whenever $P\ \mathcal{E}\ Q$,*

1. *$P \xrightarrow{\tau} P'$ implies $Q \xrightarrow{\tau} Q'$ and $P'\ \mathcal{E}\ Q'$ for some Q' or $P'\ \mathcal{E}\ Q$,*
2. *$P \xrightarrow{a} P'$ implies $Q \xrightarrow{a}\xrightarrow{\tau}\!\!\!\!\rightarrow Q'$ and $P'\ \mathcal{E}\ Q'$ for some Q'.*

Relaxed expansion, denoted by $\gtrapprox$, is the union of all relaxed expansions $\mathcal{E}$ such that $\mathcal{E}^{-1}$ is a simulation.

When $P \gtrapprox Q$ and $P \xrightarrow{a} P'$, Q has to do immediately a transition along a, but then can do as many silent transitions as necessary. The intuition behind the definition of relaxed expansion is that, using this possibility, Q can do some 'preliminary internal computation' in order to be able to remain faster than P until the next visible action.

Lemma 3.8. *$\gtrapprox$ is a relaxed expansion, and we have: $\gtrsim \subsetneq \gtrapprox \subsetneq \approx$.*

Proof. The first point and the inclusions are straightforward. We illustrate the strictness of the inclusions using CCS processes: $a.b \gtrapprox a.\tau.b$ holds but not $a.b \gtrsim a.\tau.b$, and $a \approx \tau.a$ holds but not $a \gtrapprox \tau.a$. □

Theorem 3.9. *A relaxed expansion is a controlled relation.* $\gtrsim$ *is a controlled bisimulation.*

In general, $\gtrsim$ is not a congruence: for instance, in CCS, $a.b \gtrsim a.\tau.b$ holds but not $\overline{a} \mid a.b \not\gtrsim \overline{a} \mid a.\tau.b$. We remark that $\gtrsim$ is very close to *almost weak bisimilarity,* defined in [9]; the definition of $\gtrsim$ only fits better to our setting.

3.3 Introducing Termination Guarantees

We now show how to obtain controlled relations using termination guarantees. The theorems below follow from general results about commuting diagrams, presented in Sect. 4. Their proofs are thus deferred to that section.

Theorem 3.10. *Let* $\mathcal{B}$ *be a relation such that* $\mathcal{B} \rightarrowtail \mathcal{B}^+$ *and* $\mathcal{B}$ *terminates. Then* $\mathcal{B}$ *is a controlled relation.*

Theorem 3.11. *Let* $\mathcal{B}$ *be a relation such that* $\mathcal{B} \rightarrowtail \mathcal{B}^\star$ *and* $\mathcal{B}^+ \xrightarrow{\tau}{}^+$ *terminates. Then* $\mathcal{B}$ *is a controlled relation.*

Unlike $\gtrsim$, where the control on silent moves is fixed by the co-inductive definition of the relation, in these two results we start with a relation that roughly respects the – too permissive – weak bisimulation game, and constrain it a posteriori, in such a way that it cannot cancel silent steps indefinitely. For example, the erroneous up-to relation $\mathcal{B} = \{(a, \tau.a)\}$ is rejected because $\mathcal{B}$ evolves to $\mathcal{I} = \mathcal{B}^0$, and $\mathcal{B}^+ \xrightarrow{\tau}{}^+ = \{(a, a)\}$ obviously does not terminate.

There are processes that are not related by $\gtrsim$, but by a relation satisfying the conditions of the previous theorems: consider $(a \mid (\nu b)b, \tau.a)$ or $(a + a, \tau.a)$.

Like for controlled relations, there is no direct way to define the greatest relation satisfying the requirements in Theorems 3.10 and 3.11, the main reason being that the union of terminating relations does not terminate in general. Also remark that the termination of $\mathcal{B}^+ \xrightarrow{\tau}{}^+$ does not entail the termination of $\mathcal{B}$ or $\xrightarrow{\tau}$. Theorem 3.11 can thus be applied to systems exhibiting infinite chains of τ transitions (e.g., π or CCS with replication).

We can use the up-to techniques we have defined previously to show the evolution condition in the above theorems ($\mathcal{B} \rightarrowtail \mathcal{B}^+$ or $\mathcal{B} \rightarrowtail \mathcal{B}^\star$). However one has to be careful, because the simulation relation obtained with these techniques is $\mathcal{F}^*(\mathcal{B})$. Depending on $\mathcal{F}$, this relation may be reflexive, which discards Theorem 3.10, or just quite complex, so that proving the termination of $\mathcal{F}^*(\mathcal{B})$ or $\mathcal{F}^*(\mathcal{B})^+ \xrightarrow{\tau}{}^+$ may be delicate.

4 Results about Commuting Diagrams

In this section, we work in the more general setting of *diagrams*, commonly found in rewriting theory. In addition to $\mathcal{R}, \mathcal{S}$ we let $\rightarrow, \hookrightarrow$ and $\rightsquigarrow$ range over relations. As before, $\rightarrow^+$ (resp. $\twoheadrightarrow$) is the transitive (resp. reflexive transitive) closure of $\rightarrow$. We shall say that four relations $(\mathcal{R}, \rightarrow, \mathcal{S}, \hookrightarrow)$ form a *diagram*,

denoted $(\mathcal{R}, \to) \gg (\mathcal{S}, \hookrightarrow)$, if whenever $P \ \mathcal{R} \ Q$ and $P \to P'$, there is Q' such that $P' \ \mathcal{S} \ Q'$ and $Q \hookrightarrow Q'$ (in our proofs, we shall sometimes adopt the usual graphical notation for diagrams). We say that two relations $\mathcal{R}$ and $\to$ *commute* if $(\mathcal{R}, \to) \gg (\mathcal{R}, \to)$. Notice that a relation $\mathcal{R}$ is a simulation iff $\mathcal{R}$ commutes with $\stackrel{\alpha}{\twoheadrightarrow}$ for all $\alpha \in \mathcal{L}$.

4.1 A First Termination Argument

Lemma 4.1. *Let $\mathcal{B}$, $\to$ be two relations such that $\mathcal{B}$ terminates.*
If $(\mathcal{B}, \to) \gg (\mathcal{B}^+, \twoheadrightarrow)$, then $\mathcal{B}^+$ and $\twoheadrightarrow$ commute.

Remark 4.2. The commutation hypothesis $(\mathcal{B}, \to) \gg (\mathcal{B}^+, \twoheadrightarrow)$ cannot be weakened to $(\mathcal{B}, \to) \gg (\mathcal{B}^\star, \twoheadrightarrow)$, or to "whenever $P \ \mathcal{B} \ Q$ and $P \to P'$, $P' = Q$ or there is Q' such that $P' \ \mathcal{B}^+ \ Q'$ and $Q \twoheadrightarrow Q'$". Indeed, if we define

$$\begin{array}{l} \mathcal{B} \triangleq \{\ (2,3), (3,4), (1,0)\ \} \\ \to \triangleq \{\ (3,2), (2,1), (1,0)\ \} \end{array} \qquad 0 \overset{\mathcal{B}}{\underset{\leftarrow}{\leftarrow}} 1 \leftarrow 2 \underset{\mathcal{B}}{\overset{\mathcal{B}}{\rightleftarrows}} 3 \xrightarrow{\mathcal{B}} 4$$

$\mathcal{B}$ terminates and satisfies the two alternative hypotheses; $2 \ \mathcal{B}^\star \ 4$ and $2 \to 1$, but there is no i s.t. $4 \twoheadrightarrow i$ and $1 \ \mathcal{B}^\star \ i$.

A similar result: "if $\mathcal{B}$ terminates and $(\mathcal{B}, \to) \gg (\mathcal{B}^+, \twoheadrightarrow)$, then $\mathcal{B}^\star$ and $\twoheadrightarrow$ commute" is given in [10, Exercise 1.3.2]. However we are interested in showing the stronger result below, in which diagrams can be composed with other relations (this is necessary to obtain controlled simulations).

Lemma 4.3. *Let $\mathcal{B}, \to, \hookrightarrow$ be three relations such that $\mathcal{B}$ terminates.*
If $(\mathcal{B}, \to) \gg (\mathcal{B}^+, \twoheadrightarrow)$ and $(\mathcal{B}, \hookrightarrow) \gg (\mathcal{B}^+, \twoheadrightarrow\hookrightarrow)$, then $\mathcal{B}^+$ and $\twoheadrightarrow\hookrightarrow$ commute.

Proof. By induction over the well-founded relation $\mathcal{B}^{-1}$ with the predicate $\phi(P')$: "For all P, Q such that $P \twoheadrightarrow\hookrightarrow P'$ and $P \ \mathcal{B}^+ \ Q$, there is Q' such that $Q \twoheadrightarrow\hookrightarrow Q'$ and $P' \ \mathcal{B}^+ \ Q'$". □

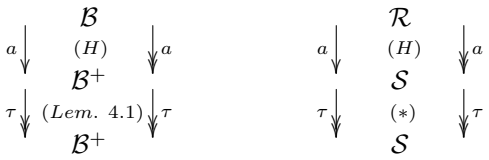
Proposition 4.4. *Let $\mathcal{B}, \to, \hookrightarrow, \mathcal{R}, \mathcal{S}, \rightsquigarrow$ be six relations such that $\mathcal{B}$ terminates.*
If $\begin{cases} (\mathcal{B}, \to) \gg (\mathcal{B}^+, \twoheadrightarrow) \\ (\mathcal{B}, \hookrightarrow) \gg (\mathcal{B}^+, \twoheadrightarrow\hookrightarrow) \end{cases}$ *and* $\begin{cases} (\mathcal{R}, \to) \gg (\mathcal{B}^\star\mathcal{R}, \twoheadrightarrow) \\ (\mathcal{R}, \hookrightarrow) \gg (\mathcal{B}^\star\mathcal{S}, \twoheadrightarrow\rightsquigarrow) \end{cases}$

then $(\mathcal{B}^\star\mathcal{R}, \twoheadrightarrow\hookrightarrow) \gg (\mathcal{B}^\star\mathcal{S}, \twoheadrightarrow\rightsquigarrow)$.

We can now give the first deferred proof from the previous section:

Proof (of Theorem 3.10).

1. Suppose $\mathcal{R} \rightarrowtail^{\tau} \mathcal{B}^\star\mathcal{R}$, we apply Proposition 4.4, taking $\stackrel{\tau}{\to}$ for $\to$, and the identity relation for $\hookrightarrow$, $\rightsquigarrow$, and $\mathcal{S}$.
2. Suppose furthermore $\mathcal{R} \rightarrowtail^{v} \mathcal{S}$ and $\mathcal{S} \rightarrowtail^{\tau} \mathcal{S}$. Lemma 4.1 ensures that $\mathcal{B}^+$ is a silent simulation. We close the diagram marked with a (*) below with a simple induction

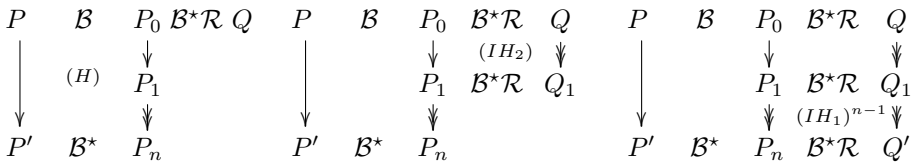


We then apply Proposition 4.4, using $\xrightarrow{\tau}$ for $\to$, $\xrightarrow{a}\xrightarrow{\tau}$ for $\hookrightarrow$ and $\rightsquigarrow$. □

4.2 A Generalisation of Newman's Lemma

Lemma 4.5. *Let $\mathcal{B}, \to, \mathcal{R}$ be three relations such that $\mathcal{B}^+ \to^+$ terminates. If $(\mathcal{B}, \to) \gg (\mathcal{B}^\star, \twoheadrightarrow)$ and $(\mathcal{R}, \to) \gg (\mathcal{B}^\star\mathcal{R}, \twoheadrightarrow)$, then $\mathcal{B}^\star\mathcal{R}$ and $\twoheadrightarrow$ commute.*

Proof. It suffices to prove $(\mathcal{B}^\star\mathcal{R}, \to) \gg (\mathcal{B}^\star\mathcal{R}, \twoheadrightarrow)$: the commutation result then follows by a simple induction. We use an induction over the well-founded order induced by the termination of $\mathcal{B}^+ \to^+$, with the predicate $\phi(P)$: "For all P', Q such that $P \to P'$ and $P\ \mathcal{B}^\star\mathcal{R}\ Q$, there is Q' such that $Q \twoheadrightarrow Q'$ and $P'\ \mathcal{B}^\star\mathcal{R}\ Q'$" (IH_1). Then we do a second induction on the derivation of $P\ \mathcal{B}^\star\mathcal{R}\ Q$ (IH_2). From the first hypothesis, we get P_n such that the leftmost diagram below holds (we show the interesting case where $P_0 \to^+ P_n$). We use the internal induction to obtain Q_1 in the central diagram; this is possible since any process P'' such that $P_0\ \mathcal{B}^+ \to^+ P''$ satisfies $P\ \mathcal{B}^+ \to^+ P''$: the external induction hypothesis is preserved. Finally, using a third induction on the derivation $P_1 \twoheadrightarrow P_n$, we close the diagram by applying $n-1$ times the external induction hypothesis (all processes between P_1 and P_n satisfy $P\ \mathcal{B}^+ \to^+ P_i$).



□

By taking $\mathcal{R} = \mathcal{I}$ in this lemma, we obtain the following corollary:

Corollary 4.6. *Let $\mathcal{B}, \to$ be two relations such that $\mathcal{B}^+ \to^+$ terminates. If $(\mathcal{B}, \to) \gg (\mathcal{B}^\star, \twoheadrightarrow)$, then $\mathcal{B}^\star$ and $\twoheadrightarrow$ commute.*

By taking $\mathcal{B} = \to$, we get Newman's lemma: "Local confluence and termination entail confluence". A different generalisation of this confluence lemma to commutation can be found in [2, Lemma 4.26]. However, the latter result is weaker than ours since it requires the termination of $\mathcal{B} \cup \to$, and thus the termination of both $\mathcal{B}$ and $\to$.

Remark 4.7 (up-to techniques and commuting diagrams). The previous corollary admits a direct and elegant proof using the decreasing diagram techniques of van Oostrom et al. [2, Theorem 4.25]. The details of this proof are given in [5]. However, results like Lemma 4.5 and Proposition 4.8 cannot be proved within the setting of [2], because they express properties beyond 'pure commutation'.

Fournet [3] and others have been using results from [2] to validate up-to techniques for *barbed equivalences*. This is not directly comparable to the present work, since in that setting, commutation results apply directly (visible actions are not taken into account). Moreover, these works do not exploit results based on termination guarantees on the relations between processes.

Proposition 4.8. *Let* $\mathcal{B}, \rightarrow, \mathcal{R}, \hookrightarrow, \mathcal{S}, \rightsquigarrow$ *be six relations s.t.* $\mathcal{B}^+ \rightarrow^+$ *terminates. If* $\begin{cases} (\mathcal{B}, \rightarrow) \gg (\mathcal{B}^\star, \twoheadrightarrow) \\ (\mathcal{B}, \hookrightarrow) \gg (\mathcal{B}^\star, \twoheadrightarrow\hookrightarrow) \end{cases}$ *and* $\begin{cases} (\mathcal{R}, \rightarrow) \gg (\mathcal{B}^\star\mathcal{R}, \twoheadrightarrow) \\ (\mathcal{R}, \hookrightarrow) \gg (\mathcal{B}^\star\mathcal{S}, \twoheadrightarrow\rightsquigarrow) \end{cases}$

then $(\mathcal{B}^\star\mathcal{R}, \twoheadrightarrow\hookrightarrow) \gg (\mathcal{B}^\star\mathcal{S}, \twoheadrightarrow\rightsquigarrow)$.

Like in the proof of Theorem 3.10, we use Proposition 4.8 and Corollary 4.6 to establish Theorem 3.11.

5 Concluding Remarks

Applications of our proof techniques. We have analysed two example systems where existing methods do not really help in establishing bisimilarity results, while the techniques we have presented are applicable, and indeed simplify the proofs. One of these examples comes from the work reported in [4] (which presents a direct bisimilarity proof). For lack of space, we do not present these here; the interested reader can refer to the long version of this paper [5]. More experience on case studies has to be developed in order to have a better understanding of how our techniques can be best combined, and how to tune the distinction between visible and internal computation steps.

A theorem prover formalisation of our results. All results in this paper have been formally checked in the Coq proof assistant [7], and the descriptions of the proofs we give actually closely follow the proof scripts (available from [6]). This is of particular interest for the proofs in Sect. 4, which require non trivial and error-prone reasoning, especially when reasoning about nested inductions.

Results about decreasing diagrams. Due to the presence of labelled transitions, results about decreasing diagrams from [2] are not applicable directly in our setting. We plan to study how the theory of [2] can be adapted to keep track of visible actions. This could be a way to provide an abstract approach for the definition of 'up to transitivity' techniques based on termination guarantees.

Acknowledgements. We would like to thank Davide Sangiorgi for his comments and suggestions, and Daniel Hirschkoff for helpful discussions and a great help during the redaction process.

References

1. S. Arun-Kumar and M. Hennessy. An efficiency preorder for processes. *Acta Informatica*, 29(9):737–760, 1992.

2. M. Bezem, J. W. Klop, and V. van Oostrom. Diagram techniques for confluence. *Information and Computation*, 141(2):172–204, 1998.
3. C. Fournet. *The Join-Calculus: a Calculus for Distributed Mobile Programming.* PhD thesis, Ecole Polytechnique, 1998.
4. D. Hirschkoff, D. Pous, and D. Sangiorgi. An Efficient Abstract Machine for Safe Ambients. Technical Report 2004–63, LIP – ENS Lyon, 2004. An extended abstract appeared in the proceedings of COORDINATION'05.
5. D. Pous. Up-to Techniques for Weak Bisimulation. Technical Report 2005–16, LIP – ENS Lyon, 2005.
6. D. Pous. Web appendix of this paper, 2005.
   Available at `http://perso.ens-lyon.fr/damien.pous/upto`.
7. INRIA projet Logical. The Coq proof assistant. `http://coq.inria.fr/`.
8. D. Sangiorgi. On the Bisimulation Proof Method. *Mathematical Structures in Computer Science*, 8:447–479, 1998.
9. D. Sangiorgi and R. Milner. The problem of "Weak Bisimulation up to". In *Proc. CONCUR '92*, volume 630 of *Lecture Notes in Computer Science*, pages 32–46. Springer Verlag, 1992.
10. TeReSe. *Term Rewriting Systems.* Cambridge University Press, 2003.