New Up-To Techniques for Weak Bisimulation

Damien Pous

New Up-to Techniques for Weak Bisimulation

Damien Pous [1]

ENS Lyon, France

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, the irregularities that appear in the weak case make it difficult to give a unified presentation.

We propose a uniform and modular theory of up-to techniques for weak bisimulation that captures most of the existing proof technology and introduces new techniques.

Some proofs rely on nontrivial – and new – commutation results based on termination guarantees. All results presented in this paper have been formally proved using the Coq proof assistant.

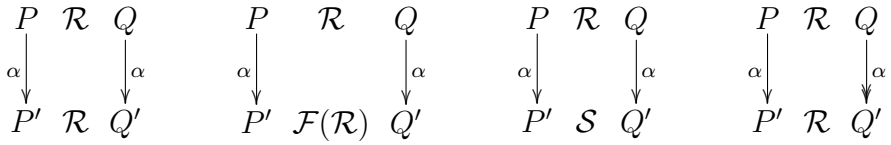
Key words: weak bisimilarity, up-to techniques, termination, commutation.

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 $P \xrightarrow{\alpha} P'$ (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: whenever P and Q are related by $\mathcal{R}$ and $P \xrightarrow{\alpha} P'$, there must exist some

[1] This work has been supported by the french initiative "Action Concertée Nouvelles Interfaces des Mathématiques GEOCAL". Author's version of the paper published by Elsevier in Theoretical Computer Science, available at `http://dx.doi.org/10.1016/j.tcs.2007.02.060`, 2007.

Q' such that $Q \xrightarrow{\alpha} Q'$ and $\mathcal{R}$ relates P' and Q' (and symmetrically for the transitions of Q).



Bisimulation is the most popular technique to establish bisimilarity between two processes: 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 $\mathcal{R}$ is contained in the bisimilarity. 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 [10], where a 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 the *strong* version of bisimulation. When analysing nontrivial systems, however, one is 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 $P \xrightarrow{\alpha} P'$ 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 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 [11]. We suppose that the reader is familiar with CCS, and define $\mathcal{R} \triangleq \{\langle \tau.a, 0\rangle\}$. 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 $\langle a, 0\rangle$. Now since we are reasoning up to $\approx$, and since $a \approx \tau.a$, we are allowed to replace this pair with $\langle \tau.a, 0\rangle$, 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 [11,3], 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 [5], 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 [5]) 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. This theory slightly departs from that proposed in [12, Section 2.4.3.3], and it enjoys nice properties in terms of generality and modularity. We then introduce new useful proof techniques for weak bisimilarity that can be used in that framework.

We start by adapting the work of [10] 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 most of the existing technology for weak bisimulation proofs. Beyond that, we validate some proof principles, such as 'up to 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 coinductively 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. Like all other results in the paper, except for the example of Section 5, they have been formally checked in the Coq proof assistant [9].

Outline of the paper. In Section 1, we introduce some necessary background and show where the approach of [10] breaks when adapted to the weak case. We develop our theory of up-to techniques for weak bisimulation in Section 2, introducing monotonic and weakly monotonic functions. In Section 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 Section 4, which are formulated as commutation results. Section 5 illustrates the use of our framework on a simple example. We give final remarks in Section 6.

This is an extended version of [6]. Additional material includes the details of proofs, a proposal for an up to context technique, as well as the example in Section 5.

1 The Problem of "Weak Bisimulation Up to"

1.1 Labelled Transition Systems, Relations, Evolution

We consider a labelled transition system (LTS) $\langle \mathcal{P}, \mathcal{L}, \rightarrow \rangle$, 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 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 closures of the relation $\mathcal{R}$. $P\mathcal{R}Q$ stands for $\langle P, Q \rangle \in \mathcal{R}$. The composition of two relations $\mathcal{R}$ and $\mathcal{S}$, written $\mathcal{RS}$, is defined by $\mathcal{RS} \triangleq \{\langle P, Q \rangle \ / \ P\mathcal{R}T \text{ and } T\mathcal{S}Q \text{ for some process } T\}$. We will also need the inverse of a relation: $\mathcal{R}^{-1} \triangleq \{\langle P, Q \rangle \ / \ Q\mathcal{R}P\}$. $\mathcal{I}$ will denote the identity relation, $\{\langle P, P \rangle \ / \ P \in \mathcal{P}\}$. 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 $\forall i, P_i \mathcal{R} P_{i+1}$.

Given an action α, the set of transitions along α induces a relation denoted by $\xrightarrow{\alpha}$: $\xrightarrow{\alpha} \triangleq \{\langle P, Q \rangle \ / \ \langle P, \alpha, Q \rangle \in \rightarrow\}$.

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 $\mathcal{R}$.

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

Notice that unlike in [10], $\stackrel{\tau}{\Longrightarrow}$ is reflexive.

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 $P\mathcal{R}Q$, $P \stackrel{\alpha}{\longrightarrow} P'$ implies $Q \stackrel{\alpha}{\Longrightarrow} Q'$ 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 $\mathcal{R} \stackrel{\mathrm{v}}{\rightarrowtail} \mathcal{S}$, 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* [12, Definition 2.4.48]: $\mathcal{R}$ progresses to $\mathcal{S}$ in the sense of [12] 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.

The following two lemmas will be useful in the proofs below. The first one states some properties of evolutions w.r.t. union and containment of relations. The second one focuses on properties of relations that evolve to themselves.

Lemma 1.3. *Let $(\mathcal{R}_i)_{i\in I}$ be an arbitrary family of relations, let $\mathcal{R}, \mathcal{S}, \mathcal{S}'$ be three relations, and let α be an action.*

(1) If for any $i \in I$, $\mathcal{R}_i$ α-evolve to $\mathcal{S}$, then $\bigcup_{i\in I} \mathcal{R}_i$ α-evolve to $\mathcal{S}$.
(2) If $\mathcal{R}$ α-evolve to $\mathcal{S}$ and $\mathcal{S} \subseteq \mathcal{S}'$, then $\mathcal{R}$ α-evolve to $\mathcal{S}'$.

Proof. Straightforward from the definitions. ■

Lemma 1.4. *Let $\mathcal{R}$ be a relation and suppose that $P\mathcal{R}Q$.*

(1) If $\mathcal{R} \stackrel{\tau}{\rightarrowtail} \mathcal{R}$ and $P \stackrel{\tau}{\Longrightarrow} P'$, then there is Q' such that $Q \stackrel{\tau}{\Longrightarrow} Q'$ and $P'\mathcal{R}Q'$.
(2) If $\mathcal{R} \rightarrowtail \mathcal{R}$ and $P \stackrel{a}{\Longrightarrow} P'$, then there is Q' such that $Q \stackrel{a}{\Longrightarrow} Q'$ and $P'\mathcal{R}Q'$.

Proof. (1) By induction on the derivation $P \stackrel{\tau}{\Longrightarrow} P'$: if $P = P'$ we take $Q' = Q$. Otherwise, we have $P \stackrel{\tau}{\longrightarrow} P_1 \stackrel{\tau}{\Longrightarrow} P'$ and since $\mathcal{R} \stackrel{\tau}{\rightarrowtail} \mathcal{R}$, there exists Q_1 such that $Q \stackrel{\tau}{\Longrightarrow} Q_1$ and $P_1\mathcal{R}Q_1$. The induction hypothesis then gives Q' such that $Q_1 \stackrel{\tau}{\Longrightarrow} Q'$ and $P'\mathcal{R}Q'$ and we check that $Q \stackrel{\tau}{\Longrightarrow} Q'$.

(2) Suppose that $P\mathcal{R}Q$ and $P \stackrel{\tau}{\twoheadrightarrow} P_1 \stackrel{a}{\rightarrow} P_1' \stackrel{\tau}{\twoheadrightarrow} P'$. By the previous point, we find Q_1 such that $Q \stackrel{\tau}{\twoheadrightarrow} Q_1$ and $P_1\mathcal{R}Q_1$ ($\mathcal{R} \rightarrowtail \mathcal{R}$ entails in particular $\mathcal{R} \stackrel{\tau}{\rightarrowtail} \mathcal{R}$). Since $\mathcal{R} \stackrel{\mathrm{v}}{\rightarrowtail} \mathcal{R}$, there exists Q_2 such that $Q_2 \stackrel{a}{\twoheadrightarrow} Q_2$ and $P_2\mathcal{R}Q_2$. By another application of the previous point, we obtain Q' such that $Q_2 \stackrel{\tau}{\twoheadrightarrow} Q'$ and $P'\mathcal{R}Q'$. We finally check that $Q \stackrel{a}{\twoheadrightarrow} Q'$. ■

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 relation $\mathcal{R}$ containing the pair $\langle P, Q\rangle$.

Definition 1.5 (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 $\precsim$, is the largest relation such that $\precsim^{-1}$ is a simulation, and, whenever $P \precsim Q$,
  · $P \stackrel{\tau}{\rightarrow} P'$ implies $Q \stackrel{\tau}{\rightarrow} Q'$ and $P' \precsim Q'$ for some Q', or $P' \precsim Q$;
  · $P \stackrel{a}{\rightarrow} P'$ implies $Q \stackrel{a}{\rightarrow} Q'$ and $P' \precsim Q'$ for some Q'.

Definition 1.6 (Functions, Constructors)**.** 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* ($\bigcup$), *iteration* (ω) and *chaining* ($^\frown$), as follows:

$$(\mathcal{F} \circ \mathcal{G})(\mathcal{R}) \triangleq \mathcal{F}(\mathcal{G}(\mathcal{R})) \qquad (\mathcal{F}^0)(\mathcal{R}) \triangleq \mathcal{R}$$
$$(\mathcal{F}^\frown\mathcal{G})(\mathcal{R}) \triangleq \mathcal{F}(\mathcal{R})\mathcal{G}(\mathcal{R}) \qquad (\mathcal{F}^{n+1})(\mathcal{R}) \triangleq \mathcal{F}^n(\mathcal{R}) \cup \mathcal{F}(\mathcal{F}^n(\mathcal{R}))$$
$$\left(\bigcup_{i\in I} \mathcal{F}_i\right)(\mathcal{R}) \triangleq \bigcup_{i\in I} \mathcal{F}_i(\mathcal{R}) \qquad (\mathcal{F}^\omega)(\mathcal{R}) \triangleq \bigcup_{n\geq 0} \mathcal{F}^n(\mathcal{R})$$

1.2 The Difficulty in the Weak Case

We now adapt the theory of up-to techniques of [10] to the weak case, and show where the difficulties arise.

Definition 1.7 (Monotonicity)**.** A function $\mathcal{F}$ is *monotonic* if the following conditions hold:

(1) $\mathcal{R} \subseteq \mathcal{S}$ entails $\mathcal{F}(\mathcal{R}) \subseteq \mathcal{F}(\mathcal{S})$;
(2) $\mathcal{R} \subseteq \mathcal{S}$ and $\mathcal{R} \rightarrowtail\!\!\!\!\!\xrightarrow{\tau} \mathcal{S}$ entail $\mathcal{F}(\mathcal{R}) \rightarrowtail\!\!\!\!\!\xrightarrow{\tau} \mathcal{F}(\mathcal{S})$; and
(3) $\mathcal{R} \subseteq \mathcal{S}$ and $\mathcal{R} \rightarrowtail \mathcal{S}$ entail $\mathcal{F}(\mathcal{R}) \rightarrowtail\!\!\!\!\!\xrightarrow{\mathrm{v}} \mathcal{F}(\mathcal{S})$.

This slightly strengthens the notion of *safe function* [12, Definition 2.4.49], in which the two kinds of transitions are handled uniformly. While the results of this section would hold using safe functions, we will need this separation between silent and visible actions in Section 2.2 (see Remark 2.6). This separation is not total however: notice that in (3), the hypothesis ranges over both visible and silent evolutions ($\mathcal{R} \rightarrowtail \mathcal{S}$).

Proposition 1.8 (Correctness of Monotonic Functions)**.**

Let $\mathcal{F}$ be a monotonic function. If $\mathcal{R} \rightarrowtail \mathcal{F}(\mathcal{R})$, then $\mathcal{F}^\omega(\mathcal{R})$ is a simulation.

Proof. We show by induction that $\mathcal{F}^n(\mathcal{R}) \rightarrowtail \mathcal{F}^{n+1}(\mathcal{R})$:

- when $n = 0$, we use the hypothesis and Lemma 1.3: $\mathcal{R} \rightarrowtail \mathcal{F}(\mathcal{R}) \subseteq \mathcal{F}^1(\mathcal{R})$;
- otherwise, $n > 0$:

$$\begin{aligned}
\mathcal{F}^{n-1}(\mathcal{R}) &\rightarrowtail \mathcal{F}^n(\mathcal{R}) && \text{(by induction)}\\
\mathcal{F}(\mathcal{F}^{n-1}(\mathcal{R})) &\rightarrowtail \mathcal{F}(\mathcal{F}^n(\mathcal{R})) && \text{(by monotonicity of } \mathcal{F})\\
\mathcal{F}^{n-1}(\mathcal{R}) \cup \mathcal{F}(\mathcal{F}^{n-1}(\mathcal{R})) &\rightarrowtail \mathcal{F}^n(\mathcal{R}) \cup \mathcal{F}(\mathcal{F}^n(\mathcal{R})) && \text{(by Lemma 1.3)}\\
\mathcal{F}^n(\mathcal{R}) &\rightarrowtail \mathcal{F}^{n+1}(\mathcal{R}) && \text{(by definition)}
\end{aligned}$$

We conclude by using Lemma 1.3: for all n, $\mathcal{F}^n(\mathcal{R}) \rightarrowtail \mathcal{F}^\omega(\mathcal{R})$ and we have:

$$\mathcal{F}^\omega(\mathcal{R}) = \bigcup_{n \geq 0} \mathcal{F}^n(\mathcal{R}) \rightarrowtail \mathcal{F}^\omega(\mathcal{R}) \ . \qquad \blacksquare$$

$\blacksquare$

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 $\mathcal{F}^\omega(\mathcal{R})$, which is a simulation. We now exhibit some monotonic functions, and show how to combine them to obtain more powerful techniques.

Lemma 1.9. *Let $\mathcal{S}$ be a simulation, $\mathcal{U}$, $\tilde{\mathcal{S}}$, $\bullet\mathcal{S}$ and $\gtrsim\!\bullet$ are monotonic functions.*

Proof. The cases of $\mathcal{U}$, $\tilde{\mathcal{S}}$ and $\bullet\mathcal{S}$ are immediate, we give the proof for $\gtrsim\!\bullet$: suppose that $\mathcal{R} \subseteq \mathcal{S}$ and $\mathcal{R} \rightarrowtail\!\!\!\!\!\xrightarrow{\tau} \mathcal{S}$. That $\gtrsim\!\mathcal{R} \subseteq \gtrsim\!\mathcal{S}$ is trivial; we show that $\gtrsim\!\mathcal{R} \rightarrowtail\!\!\!\!\!\xrightarrow{\tau} \gtrsim\!\mathcal{S}$: suppose that $P \gtrsim P_0 \mathcal{R} Q$ and $P \xrightarrow{\tau} P'$. By definition of $\gtrsim$ we have:

- either $P' \gtrsim P_0$ and we check that $P' \gtrsim\!\mathcal{S} Q$;

- or $P_0 \xrightarrow{\tau} P_0'$ and $P' \gtrsim P_0'$ for some P_0'. Since $\mathcal{R} \stackrel{\tau}{\rightarrowtail} \mathcal{S}$, we find Q' such that $Q \stackrel{\tau}{\twoheadrightarrow} Q'$ and $P_0'\mathcal{S}Q'$. We finally check that $P' {\gtrsim} \mathcal{S} Q'$.

The case of a visible evolution is handled similarly. ■

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.

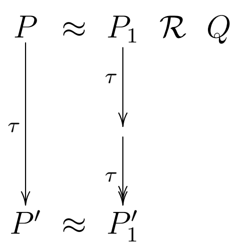
Lemma 1.10. *Composition* ($\circ$)*, union* ($\bigcup$) *and iteration* (ω) *are constructors that respect monotonicity.*

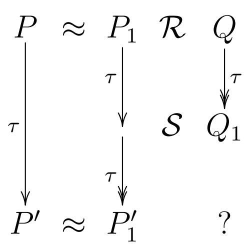
We can now apply our framework to reason about bisimulation relations, and revisit a result from [11]. We show that the proof becomes elementary.

Theorem 1.11. *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 $\mathcal{F}^{\omega}(\mathcal{R})$ and $\mathcal{F}^{\omega}(\mathcal{R}^{-1})$ are simulations, using Prop. 1.8. It follows that ${\approx}\mathcal{F}^{\omega}(\mathcal{R})$ and $\mathcal{F}^{\omega}(\mathcal{R}^{-1}){\approx}$ are simulations. We finally check that $({\approx}\mathcal{F}^{\omega}(\mathcal{R}))^{-1} = \mathcal{F}^{\omega}(\mathcal{R}^{-1}){\approx}$, so that $\mathcal{R} \subseteq {\approx}\mathcal{F}^{\omega}(\mathcal{R}) \subseteq {\approx}$. ■

The transitivity problem. The $\approx$-left-chaining function is not monotonic. As a consequence, the chaining constructor does not respect monotonicity in general. To see why, let us try to prove the monotonicity of ${\approx}\bullet$. Given $\mathcal{R}$ and $\mathcal{S}$ such that $\mathcal{R} \stackrel{\tau}{\rightarrowtail} \mathcal{S}$ and $\mathcal{R} \subseteq \mathcal{S}$, we have to show ${\approx}\mathcal{R} \stackrel{\tau}{\rightarrowtail} {\approx}\mathcal{S}$. For that, we have to close the leftmost diagram below. Our hypothesis allows us to close the first step of the transition $P_1 \stackrel{\tau}{\twoheadrightarrow} P_1'$, and obtain the second diagram. However, from this point, we are stuck, since we have no hypothesis on the silent evolution of $\mathcal{S}$.





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 the following conditions hold:

(1) $\mathcal{R} \subseteq \mathcal{S}$ entails $\mathcal{F}(\mathcal{R}) \subseteq \mathcal{F}(\mathcal{S})$;
(2) $\mathcal{R} \overset{\tau}{\rightarrowtail} \mathcal{R}$ entails $\mathcal{F}(\mathcal{R}) \overset{\tau}{\rightarrowtail} \mathcal{F}(\mathcal{R})$; and
(3) $\mathcal{R} \overset{\tau}{\rightarrowtail} \mathcal{R}$, $\mathcal{R} \subseteq \mathcal{S}$, $\mathcal{S} \overset{\tau}{\rightarrowtail} \mathcal{S}$, and $\mathcal{R} \overset{\mathrm{v}}{\rightarrowtail} \mathcal{S}$ entail $\mathcal{F}(\mathcal{R}) \overset{\mathrm{v}}{\rightarrowtail} \mathcal{F}(\mathcal{S})$.

The main difference w.r.t. Definition 1.7 is in clause (2): instead of respecting silent evolutions, a weakly monotonic function has to respect silent simulations. On the visible side (3), 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 actions, 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 $\mathcal{R} \overset{\tau}{\rightarrowtail} \mathcal{R}$, and $\mathcal{R} \overset{\mathrm{v}}{\rightarrowtail} \mathcal{F}(\mathcal{R})$, then $\mathcal{F}^\omega(\mathcal{R})$ is a simulation.

Proof. $\mathcal{R} \overset{\tau}{\rightarrowtail} \mathcal{R}$ and (2) in the weak monotonicity of $\mathcal{F}$ give $\mathcal{F}^n(\mathcal{R}) \overset{\tau}{\rightarrowtail} \mathcal{F}^n(\mathcal{R})$ for all n, by induction on n. Then, by a second induction on n, we get for all n, $\mathcal{F}^n(\mathcal{R}) \overset{\mathrm{v}}{\rightarrowtail} \mathcal{F}^{n+1}(\mathcal{R})$. We conclude with Lemma 1.3. ■

Now we study the class of weakly monotonic functions: the following lemma ensures that the functions given by Lemma 1.9 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* ($\bigcup$)*, iteration* (ω) *and chaining* ($\frown$) *respect weak monotonicity.*

Proof. We prove that chaining respects weak monotonicity. Let $\mathcal{F}$ and $\mathcal{G}$ be two weakly monotonic functions.

(1) Straightforward.
(2) Suppose $\mathcal{R} \rightarrowtail^{\tau} \mathcal{R}$, then $\mathcal{F}(\mathcal{R}) \rightarrowtail^{\tau} \mathcal{F}(\mathcal{R})$ and $\mathcal{G}(\mathcal{R}) \rightarrowtail^{\tau} \mathcal{G}(\mathcal{R})$ by weak monotonicity of $\mathcal{F}$ and $\mathcal{G}$. We get the leftmost diagram below, that we can close using Lemma 1.4 (rightmost diagram).

$$\begin{array}{ccccc} P & \mathcal{F}(\mathcal{R}) & P_1 & \mathcal{G}(\mathcal{R}) & Q \\ {\scriptstyle\tau}\downarrow & & {\scriptstyle\tau}\downarrow & & \\ P' & \mathcal{F}(\mathcal{R}) & P_1' & & \end{array} \qquad \begin{array}{ccccc} P & \mathcal{F}(\mathcal{R}) & P_1 & \mathcal{G}(\mathcal{R}) & Q \\ {\scriptstyle\tau}\downarrow & & {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau} \\ P' & \mathcal{F}(\mathcal{R}) & P_1' & \mathcal{G}(\mathcal{R}) & Q' \end{array}$$

(3) Suppose $\mathcal{R} \rightarrowtail^{\tau} \mathcal{R}$, $\mathcal{R} \rightarrowtail^{\mathrm{v}} \mathcal{S}$, $\mathcal{S} \rightarrowtail^{\tau} \mathcal{S}$ and $\mathcal{R} \subseteq \mathcal{S}$. By weak monotonicity of $\mathcal{F}$, we have $\mathcal{F}(\mathcal{R}) \rightarrowtail^{\mathrm{v}} \mathcal{F}(\mathcal{S})$; $\mathcal{G}$ is weakly monotonic, so that $\mathcal{G}(\mathcal{R}) \rightarrowtail^{\mathrm{v}} \mathcal{G}(\mathcal{S})$, $\mathcal{G}(\mathcal{R}) \rightarrowtail^{\tau} \mathcal{G}(\mathcal{R})$ and $\mathcal{G}(\mathcal{S}) \rightarrowtail^{\tau} \mathcal{G}(\mathcal{S})$. With Lemma 1.4 and simple diagram chasing arguments, we prove $\mathcal{F}(\mathcal{R})\mathcal{G}(\mathcal{R}) \rightarrowtail^{\mathrm{v}} \mathcal{F}(\mathcal{S})\mathcal{G}(\mathcal{S})$. ■

The closure of weakly monotonic functions 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 $\mathcal{F}(\mathcal{R}) = \approx\mathcal{R}\approx$. An example of such use is given by the following theorem.

Theorem 2.4. *Let $\mathcal{R}$ be a relation.*

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

Proof. Let $\mathcal{F}(\mathcal{R}) \triangleq \approx \cup (\mathcal{R}^\frown\mathcal{R})$. We have $(\mathcal{R} \cup \approx)^\star = \mathcal{F}^\omega(\mathcal{R})$, and we check using Lemma 2.3 that $\mathcal{F}$ and $\mathcal{F}^\omega$ are weakly monotonic. Therefore, by applying Proposition 2.2, both $(\mathcal{R} \cup \approx)^\star$ and $(\mathcal{R}^{-1} \cup \approx)^\star$ are simulations. ■

2.2 Combining Monotonicity and Weak Monotonicity

When 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 2.5 (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 $\mathcal{R} \rightarrowtail^{\tau} \mathcal{F}(\mathcal{R})$ and $\mathcal{R} \rightarrowtail^{\mathrm{v}} \mathcal{G}(\mathcal{R})$, then $\mathcal{G}^{\omega\omega}(\mathcal{R})$ is a simulation.

Proof. We successively establish the following results:

$$\mathcal{R} \subseteq \mathcal{F}^\omega(\mathcal{R}) \subseteq \mathcal{G}^\omega(\mathcal{R}) \tag{1}$$
$$\mathcal{F}^\omega(\mathcal{R}) \rightarrowtail\!\!\!\!\!\!\rightarrow^{\tau} \mathcal{F}^\omega(\mathcal{R}) \tag{2}$$
$$\mathcal{F}^\omega(\mathcal{R}) \rightarrowtail\!\!\!\!\!\!\rightarrow^{\mathrm{v}} \mathcal{G}^\omega(\mathcal{F}^\omega(\mathcal{R})) \tag{3}$$
$$\mathcal{G}^{\omega\omega}(\mathcal{R}) = \mathcal{G}^{\omega\omega}(\mathcal{F}^\omega(\mathcal{R})) \tag{4}$$

Since $\mathcal{G}$ is weakly monotonic, so is $\mathcal{G}^\omega$, so that Proposition 2.2, applied with (2) and (3) to the candidate relation $\mathcal{F}^\omega(\mathcal{R})$ will ensure that $\mathcal{G}^{\omega\omega}(\mathcal{F}^\omega(\mathcal{R}))$ is a simulation. The result will finally follow from (4).

(1) By induction, we prove $\forall n, \mathcal{R} \subseteq \mathcal{F}^n(\mathcal{R}) \subseteq \mathcal{G}^n(\mathcal{R})$.
(2) We prove $\forall n, \mathcal{F}^n(\mathcal{R}) \rightarrowtail\!\!\!\!\!\!\rightarrow^{\tau} \mathcal{F}^{n+1}(\mathcal{R})$, by induction on n, using the monotonicity of $\mathcal{F}$ and $\mathcal{R} \rightarrowtail\!\!\!\!\!\!\rightarrow^{\tau} \mathcal{F}(\mathcal{R})$.
(3) We actually show that $\mathcal{F}^\omega(\mathcal{R}) \rightarrowtail\!\!\!\!\!\!\rightarrow^{\mathrm{v}} \mathcal{G}^\omega(\mathcal{R})$, which is sufficient by using Lemma 1.3. We prove $\forall n, \mathcal{F}^n(\mathcal{R}) \rightarrowtail \mathcal{G}^{n+1}(\mathcal{R})$ by induction on n:
   - $n = 0$: the hypotheses $\mathcal{F} \subseteq \mathcal{G}$, $\mathcal{R} \rightarrowtail\!\!\!\!\!\!\rightarrow^{\tau} \mathcal{F}(\mathcal{R})$ and $\mathcal{R} \rightarrowtail\!\!\!\!\!\!\rightarrow^{\mathrm{v}} \mathcal{G}(\mathcal{R})$ entail that $\mathcal{R} \rightarrowtail \mathcal{G}(\mathcal{R}) \subseteq \mathcal{G}^1(\mathcal{R})$.
   - $n > 0$: the induction hypothesis is $\mathcal{F}^{n-1}(\mathcal{R}) \rightarrowtail \mathcal{G}^n(\mathcal{R})$. By using the monotonicity of $\mathcal{F}$, we get $\mathcal{F}^n(\mathcal{R}) \rightarrowtail \mathcal{G}^n(\mathcal{R}) \cup \mathcal{F}(\mathcal{G}^n(\mathcal{R})) \subseteq \mathcal{G}^{n+1}(\mathcal{R})$.
(4) We have immediately $\mathcal{G}^{\omega\omega}(\mathcal{R}) \subseteq \mathcal{G}^{\omega\omega}(\mathcal{F}^\omega(\mathcal{R}))$. To show the converse, we prove first $\forall n, (\mathcal{G}^\omega)^n(\mathcal{G}^\omega(\mathcal{R})) \subseteq (\mathcal{G}^\omega)^{n+1}(\mathcal{R})$ by induction on n, and it follows that $\mathcal{G}^{\omega\omega}(\mathcal{F}^\omega(\mathcal{R})) \subseteq \mathcal{G}^{\omega\omega}(\mathcal{G}^\omega(\mathcal{R})) \subseteq \mathcal{G}^{\omega\omega}(\mathcal{R})$. ■

Remark 2.6. The proof of the above proposition justifies the separation we imposed between silent and visible evolutions in Definition 1.7 (monotonicity): it makes it possible to show that $\mathcal{F}^\omega(\mathcal{R})$ is a silent simulation, without having to look at the visible evolutions of $\mathcal{R}$.

Remark 2.7. While in practise, all functions we will manipulate will satisfy $\mathcal{G}^{\omega\omega} = \mathcal{G}^\omega$ or even $\mathcal{G}^\omega = \mathcal{G}$, one could in principle define monotonic functions such that this is not true. Indeed, consider the following function, defined over sets of natural numbers $(\mathbb{N})$ [2]:

$$f : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$$
$$X \mapsto \begin{cases} \mathbb{N} & \text{if } \mathbb{N}\backslash\{0\} \subseteq X, \\ X \cup \{\min\ (\mathbb{N}\backslash(X \cup \{0\}))\} & \text{otherwise.} \end{cases}$$

It is monotonic (w.r.t. $\subseteq$), but $f^\omega(\{1\}) = \mathbb{N}\backslash\{0\} \neq \mathbb{N} = f^{\omega\omega}(\{1\})$.

The following theorem subsumes Theorems 1.11 and 2.4: the richer setting we have introduced makes it possible to combine these two results.

[2] We thank Emmanuel Jeandel for this counter-example.

Theorem 2.8. *Let $\mathcal{R}$ be a relation.*

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

Proof. $\mathcal{F}(\mathcal{R}) \triangleq \gtrsim \mathcal{R}^{=} \approx$ and $\mathcal{G}(\mathcal{R}) \triangleq (\mathcal{R} \cup \approx)^{\star}$ satisfy the conditions of Proposition 2.5 ($\gtrsim \subseteq \approx$), so that $\mathcal{G}(\mathcal{R})$ and $\mathcal{G}(\mathcal{R}^{-1})$ are simulations ($\mathcal{G} = \mathcal{G}^{\omega\omega}$). Since $\mathcal{G}(\mathcal{R})^{-1} = \mathcal{G}(\mathcal{R}^{-1})$, $\mathcal{G}(\mathcal{R})$ is a bisimulation, and $\mathcal{R} \subseteq \mathcal{G}(\mathcal{R}) \subseteq \approx$. ■

We thus have a modular theory of up-to techniques for weak bisimulation that follows the approach for the strong case in [10]. Technically, the main improvement over previous works [12] is the ability to exploit weaker hypotheses when reasoning about visible steps: for instance, *up to transitivity* ($\mathcal{R} \rightarrowtail^{\mathrm{v}} \mathcal{R}^{\star}$) and *up to weak bisimilarity* ($\mathcal{R} \rightarrowtail^{\mathrm{v}} \approx \mathcal{R} \approx$) techniques entail valid proof methods.

2.3 An 'Up to Context' Proof Technique

An important family of up-to techniques that has not been discussed yet is 'up to context'. When the states of the LTS are described by a syntax, such techniques make it possible to remove common sub-terms of the processes being compared along the bisimulation game, and thus help reducing the size of the relation one has to exhibit.

As explained below, we cannot present in our setting all up to context proof techniques that have been widely used in CCS and the π-calculus [10,12]. We can however define a class of up to context techniques that should be useful in other systems.

We denote by $\widetilde{P}$ a vector of processes, and by P^i the i-th component of such vector. We call *(polyadic) context of arity n* a function from vectors of size n to processes (we adopt an approach that allows us to abstract over the details of the underlying syntax). We let C, D range over contexts, and denote by $C[\widetilde{P}]$ the application of a context C to a vector of processes $\widetilde{P}$ (we shall implicitly assume that the size of $\widetilde{P}$ and the arity of C are equal). We let $\mathcal{C}, \mathcal{D}$ range over families of contexts. Given a family $\mathcal{C}$ of contexts, we define the *closure up to $\mathcal{C}$* function by

$$\mathcal{C}(\mathcal{R}) \triangleq \left\{ \ \left\langle C[\widetilde{P}], C[\widetilde{Q}] \right\rangle \ / \ C \in \mathcal{C} \text{ and } \forall i, P^i \mathcal{R} Q^i \right\} \ .$$

In the following technical definition, we use notations $\xrightarrow{\epsilon}$ and $\xrightarrow{\epsilon}\!\!\!\!\rightarrow$ as synonyms for the identity relation $\mathcal{I}$ (we suppose $\epsilon \notin \mathcal{L}$). Furthermore, we write $\widetilde{P} \xrightarrow{\widetilde{\delta}} \widetilde{P'}$ (resp. $\widetilde{P} \xrightarrow{\widetilde{\delta}}\!\!\!\!\rightarrow \widetilde{P'}$) for $\forall i, P^i \xrightarrow{\delta^i} P'^i$ (resp. $\forall i, P^i \xrightarrow{\delta^i}\!\!\!\!\rightarrow P'^i$).

Definition 2.9 (Faithfulness)**.** Let $\mathcal{C}$ be a family of contexts. We say that $\mathcal{C}$ is *faithful* if for all $C \in \mathcal{C}$, whenever $C[\widetilde{P}] \xrightarrow{\alpha} R$, there are $C' \in \mathcal{C}$, $\widetilde{P'}$, and a vector $\widetilde{\delta}$ whose components are in $\mathcal{L} \cup \{\epsilon\}$ such that:

(1) $R = C'[\widetilde{P'}]$ and $\widetilde{P} \xrightarrow{\widetilde{\delta}} \widetilde{P'}$;
(2) for all $\widetilde{Q}, \widetilde{Q'}$ such that $\widetilde{Q} \xrightarrow{\widetilde{\delta}} \widetilde{Q'}$ and $C[\widetilde{Q}] \xrightarrow{\alpha} C'[\widetilde{Q'}]$;
(3) if $\alpha = \tau$ then the components of $\widetilde{\delta}$ are taken in $\{\tau, \epsilon\}$.

A context C is *faithful* if it belongs to a faithful family of contexts.

This is the direct adaptation to the weak case of the notion of faithfulness in [10,12], to which we add the restriction (3) for silent evolutions. We return to this additional clause below.

Proposition 2.10. *The closure up to a faithful family of contexts is monotonic.*

Proof. We consider the case of contexts of arity 1, and prove separately the three implications of Definition 1.7.

(1) Straightforward.
(2) Suppose $\mathcal{R} \rightarrowtail\!\!\!\!\!\rightarrow^{\tau} \mathcal{S}$, $\mathcal{R} \subseteq \mathcal{S}$, $P\mathcal{C}(\mathcal{R})Q$, with $P = C[P_0], Q = C[Q_0], P_0\mathcal{R}Q_0$ and $P \xrightarrow{\tau} P'$. By faithfulness, there is C', P'_0 and δ such that $P' = C'[P'_0]$ and $P_0 \xrightarrow{\delta} P'_0$. From (3), δ is either τ or ϵ:
   - $\delta = \epsilon$: using (2), $C[Q_0] \xrightarrow{\tau} C'[Q_0]$ and since $\mathcal{R} \subseteq \mathcal{S}$, we have $P_0\mathcal{S}Q_0$.
   - $\delta = \tau$: since $P_0\mathcal{R}Q_0$ and $\mathcal{R} \rightarrowtail\!\!\!\!\!\rightarrow^{\tau} \mathcal{S}$ there is Q'_0 such that $Q_0 \xrightarrow{\tau} Q'_0$ and $P'_0\mathcal{S}Q'_0$. Using (2), we get $C[Q_0] \xrightarrow{\tau} C'[Q'_0]$.
(3) Suppose $\mathcal{R} \rightarrowtail \mathcal{S}$, $\mathcal{R} \subseteq \mathcal{S}$, $P\mathcal{C}(\mathcal{R})Q$, with $P = C[P_0], Q = C[Q_0], P_0\mathcal{R}Q_0$ and $P \xrightarrow{a} P'$. By faithfulness, there is C', P'_0 and δ such that $P' = C'[P'_0]$ and $P_0 \xrightarrow{\delta} P'_0$.
   - $\delta = \epsilon$ is similar to the previous case
   - $\delta = \alpha \in \mathcal{L}$: since $P_0\mathcal{R}Q_0$ and $\mathcal{R} \rightarrowtail \mathcal{S}$ there is Q'_0 such that $Q_0 \xrightarrow{\alpha} Q'_0$ and $P'_0\mathcal{S}Q'_0$. Using (2), we get $C[Q_0] \xrightarrow{a} C'[Q'_0]$. ■

This result ensures that we can use Theorem 2.8 to reason up to faithful contexts both on visible and silent steps.

In the strong up-to theory of [10], all CCS contexts are faithful, as well as all *non input-guarded* π-calculus contexts (i.e. those where the argument process is not placed under an input prefix). This is not the case in our setting: closure by parallel composition (given by $C_Q[P] = P|Q$) does not obey to our definition of faithfulness. This is due to the restriction (3): when $C[P] \xrightarrow{\tau} R$ we require that the context either does the silent action itself (like $C[P] = \tau.P$), or delegates it to P (like $C[P] = P$), but the silent action cannot follow from

an interaction between the context and a visible action of P (in CCS, e.g., $C[P] = \overline{a}|P$ and $P = a.P'$). This restriction is a consequence of the separation between silent and visible actions in Definition 1.7: in order to prove $\mathcal{C}(\mathcal{R}) \stackrel{\tau}{\rightarrowtail\!\!\!\!\succ} \mathcal{C}(\mathcal{S})$, we only suppose $\mathcal{R} \stackrel{\tau}{\rightarrowtail\!\!\!\!\succ} \mathcal{S}$ (while working in the setting of [10] would mean supposing $\mathcal{R} \rightarrowtail\!\!\!\!\succ \mathcal{S}$). Therefore, when we observe the silent evolution of a process $C[P]$, we have no hypothesis to reason about the case where P does a visible transition. Formulating our results with the original definition of faithfulness would have been possible up to Proposition 2.5 and Theorem 2.8, that inherently exploit a separation between visible and silent transitions, and thus render clause (3) necessary in Definition 2.9 (Remark 2.6).

To comment further on this restriction, let us remark that one of the main motivations of this work is to provide useful proof techniques to reason about rather large systems, such as in [5,8]. In such settings, it is often the case that the system is defined without labels: only internal reductions are defined; visible labels are then added in order to help reasoning about those reductions. Hence, the internal behaviour of a system (its silent actions) is not defined in a compositional way as synchronisations between visible transitions of its sub-components, and it seems likely that clause (3) does not prevent the use of up to context proof techniques in such situations.

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 2.8) 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. Intuitively, 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 say that $\mathcal{B}$ is a *controlled relation* if the following conditions hold for all relations $\mathcal{R}$, $\mathcal{S}$:

(1) $\mathcal{R} \stackrel{\tau}{\rightarrowtail\!\!\!\!\succ} \mathcal{B}^\star\mathcal{R}$ entails $\mathcal{B}^\star\mathcal{R} \stackrel{\tau}{\rightarrowtail\!\!\!\!\succ} \mathcal{B}^\star\mathcal{R}$; and

(2) $\mathcal{R} \rightarrowtail^{\tau} \mathcal{B}^\star\mathcal{R}$, $\mathcal{S} \rightarrowtail^{\tau} \mathcal{S}$ and $\mathcal{R} \rightarrowtail^{\mathrm{v}} \mathcal{S}$ entail $\mathcal{B}^\star\mathcal{R} \rightarrowtail^{\mathrm{v}} \mathcal{B}^\star\mathcal{S}$.

Remark 3.2. Note that a controlled relation needs 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 generic 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 $\mathcal{B}$.

This transparency property is necessary to compute fixpoints in the proof of the following proposition.

Proposition 3.4 (Up to Controlled relation)**.** *Let $\mathcal{F}$ and $\mathcal{G}$ be two functions, and $\mathcal{B}$ a relation such that:*

(i) $\mathcal{F}$ is monotonic and $\mathcal{B}$-transparent,
(ii) $\mathcal{G}$ is weakly monotonic and contains $\mathcal{F}$ and $\mathcal{B}^\star\bullet$.
(iii) $\mathcal{B}$ is a controlled relation,

If $\mathcal{R} \rightarrowtail^{\tau} \mathcal{B}^\star\mathcal{F}(\mathcal{R})$ and $\mathcal{R} \rightarrowtail^{\mathrm{v}} \mathcal{G}(\mathcal{R})$, then $\mathcal{G}^{\omega\omega}(\mathcal{R})$ is a simulation.

Proof. We successively establish the following results:

$$\mathcal{R} \subseteq \mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R}) \subseteq \mathcal{B}^\star\mathcal{G}^\omega(\mathcal{R}) \subseteq \mathcal{G}^\omega(\mathcal{R}) \tag{1}$$
$$\mathcal{F}^\omega(\mathcal{R}) \rightarrowtail^{\tau} \mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R}) \tag{2}$$
$$\mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R}) \rightarrowtail^{\tau} \mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R}) \tag{3}$$
$$\mathcal{G}^\omega(\mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R})) \rightarrowtail^{\tau} \mathcal{G}^\omega(\mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R})) \tag{4}$$
$$\mathcal{F}^\omega(\mathcal{R}) \rightarrowtail^{\mathrm{v}} \mathcal{G}^\omega(\mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R})) \tag{5}$$
$$\mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R}) \rightarrowtail^{\mathrm{v}} \mathcal{G}^\omega(\mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R})) \tag{6}$$
$$\mathcal{G}^{\omega\omega}(\mathcal{R}) = \mathcal{G}^{\omega\omega}(\mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R})) \tag{7}$$

Since $\mathcal{G}$ is weakly monotonic, so is $\mathcal{G}^\omega$, so that Proposition 2.2, applied with (3) and (6) to the candidate relation $\mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R})$ will ensure that $\mathcal{G}^{\omega\omega}(\mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R}))$ is a simulation. The result will finally follow from (7).

(1) By induction, $\forall n, \mathcal{R} \subseteq \mathcal{B}^\star\mathcal{F}^n(\mathcal{R}) \subseteq \mathcal{B}^\star\mathcal{G}^n(\mathcal{R}) \subseteq \mathcal{G}^{n+1}(\mathcal{R})$.
(2) By induction, and using (i), we prove $\forall n, \mathcal{F}^n(\mathcal{R}) \rightarrowtail^{\tau} \mathcal{B}^\star\mathcal{F}^{n+1}(\mathcal{R})$.

(3) We apply the first point in the definition of a controlled relation (Definition 3.1) with $\mathcal{F}^\omega(\mathcal{R})$ and (2).
(4) We use the weak monotonicity of $\mathcal{G}$ (ii) and (3) to prove by induction $\forall n, \mathcal{G}^n(\mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R})) \stackrel{\tau}{\rightarrowtail} \mathcal{G}^n(\mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R}))$.
(5) We actually show $\mathcal{F}^\omega(\mathcal{R}) \stackrel{\mathrm{v}}{\rightarrowtail} \mathcal{G}^\omega(\mathcal{R})$, by proving $\forall n, \mathcal{F}^n(\mathcal{R}) \rightarrowtail \mathcal{G}^{n+2}(\mathcal{R})$ by induction:
   - $n = 0$: the visible case is immediate; for the silent case, using (ii), we have that $\mathcal{R} \stackrel{\tau}{\rightarrowtail} \mathcal{B}^\star\mathcal{F}(\mathcal{R}) \subseteq \mathcal{B}^\star\mathcal{G}(\mathcal{R}) \subseteq \mathcal{G}^2(\mathcal{R})$.
   - $n > 0$: the inductive hypothesis is $\mathcal{F}^{n-1}(\mathcal{R}) \rightarrowtail \mathcal{G}^{n+1}(\mathcal{R})$. Using (ii) and the monotonicity of $\mathcal{F}$, we obtain $\mathcal{F}^n(\mathcal{R}) \rightarrowtail \mathcal{G}^{n+1}(\mathcal{R}) \cup \mathcal{F}(\mathcal{G}^{n+1}(\mathcal{R})) \subseteq \mathcal{G}^{n+2}(\mathcal{R})$.
(6) We apply the second point in the definition of a controlled relation (Definition 3.1) with $\mathcal{F}^\omega(\mathcal{R})$, $\mathcal{G}^\omega(\mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R}))$, (3), (4) and (5).
(7) We have $\mathcal{G}^{\omega\omega}(\mathcal{B}^\star\mathcal{F}^\omega(\mathcal{R})) \subseteq \mathcal{G}^{\omega\omega}(\mathcal{G}^\omega(\mathcal{R})) \subseteq \mathcal{G}^{\omega\omega}(\mathcal{R})$. ■

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

Given a family of contexts $\mathcal{C}$, if $\mathcal{C}(\mathcal{B}) \subseteq \mathcal{B}$ (i.e. "$\mathcal{B}$ is a $\mathcal{C}$-congruence"), then the closure up to $\mathcal{C}$ function is $\mathcal{B}$-transparent.

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

The chaining constructor does not respect $\mathcal{B}$-transparency, but this would be of little use anyway: Proposition 3.4 indeed requires the transparency of a monotonic function, which rules out the chaining constructor, that does not respect monotonicity.

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.*

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

Proof. $\mathcal{B}$, $\mathcal{F}(\mathcal{R}) \triangleq \mathcal{R}^{=}\approx$ and $\mathcal{G}(\mathcal{R}) \triangleq (\mathcal{R} \cup \approx)^\star$ satisfy the conditions of Proposition 3.4, so that $\mathcal{G}(\mathcal{R})$ and $\mathcal{G}(\mathcal{R}^{-1})$ are simulations ($\mathcal{G} = \mathcal{G}^{\omega\omega}$). Since $\mathcal{G}(\mathcal{R})^{-1} = \mathcal{G}(\mathcal{R}^{-1})$, $\mathcal{G}(\mathcal{R})$ is a bisimulation, and $\mathcal{R} \subseteq \mathcal{G}(\mathcal{R}) \subseteq \approx$. ■

This theorem is the counterpart of Theorem 2.8, 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. Making the distinction can be useful in particular because the class of controlled bisimulations is not closed under union, as explained in Remark 3.2.

If we need the closure under a family of contexts given by $\mathcal{R} \overset{\tau}{\rightarrowtail} \mathcal{B}^\star\mathcal{C}(\mathcal{R})\approx$ and $\mathcal{R} \overset{\mathrm{v}}{\rightarrowtail} (\mathcal{C}(\mathcal{R}) \cup \approx)^\star$, we have to ensure that the controlled bisimulation $\mathcal{B}$ is a $\mathcal{C}$-congruence (see Lemma 3.5), which can be quite difficult. In such cases, one can restrict the family of contexts used on silent actions to $\mathcal{D} \subseteq \mathcal{C}$, with $\mathcal{R} \overset{\tau}{\rightarrowtail} \mathcal{B}^\star\mathcal{D}(\mathcal{R})\approx$, in order to weaken the congruence condition.

The previous remarks lead to the following proposition. Although in our experience in bisimulation proofs, we have not encountered a situation where this result is needed in its full generality, we give it to illustrate the modularity of our setting.

Proposition 3.7. *Let $\mathcal{B}_1$, $\mathcal{B}_2$ be two controlled bisimulations, and $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{C}$ be three faithful families of contexts. Suppose moreover that $\mathcal{D}_1$ (resp. $\mathcal{D}_2$) is $\mathcal{B}_1$-transparent (resp. $\mathcal{B}_2$-transparent), and that $\mathcal{C}$ contains both $\mathcal{D}_1$ and $\mathcal{D}_2$.*

$$\textit{If } \begin{cases} \mathcal{R} \overset{\tau}{\rightarrowtail} \mathcal{B}_1^\star\mathcal{D}_1(\mathcal{R}^=)\approx \\ \mathcal{R} \overset{\mathrm{v}}{\rightarrowtail} (\mathcal{C}(\mathcal{R}) \cup \approx)^\star \end{cases} \quad \textit{and} \quad \begin{cases} \mathcal{R}^{-1} \overset{\tau}{\rightarrowtail} \mathcal{B}_2^\star\mathcal{D}_2(\mathcal{R}^{-1=})\approx \\ \mathcal{R}^{-1} \overset{\mathrm{v}}{\rightarrowtail} (\mathcal{C}(\mathcal{R}^{-1}) \cup \approx)^\star \end{cases} \quad \textit{then } \mathcal{R} \subseteq \approx \ .$$

The following lemma gives a way to prove that a controlled relation is a controlled bisimulation.

Lemma 3.8. *If $\mathcal{B}$ is a controlled relation and $\mathcal{B}^{-1} \rightarrowtail \mathcal{B}^{-1} \cup \approx$, then $\mathcal{B}$ is a controlled bisimulation.*

Proof. With Lemma 1.3, $\mathcal{B}^{-1} \cup \approx$ is a simulation; from Remark 3.2, $\mathcal{B}^\star$ as well, so that $\mathcal{B}^\star \cup \approx$ is a bisimulation. ■

The remainder of the section is devoted to the construction of controlled relations. We propose first a coinductively defined preorder, derived from the expansion preorder; we then give two sufficient conditions based on termination guarantees.

3.2 Relaxed Expansion

The expansion preorder is quite constrained on visible transitions: whenever $P \gtrsim Q$ and P does a visible transition, Q has to answer exactly with that visible transition. We show that, as far as up-to techniques are concerned, we can allow Q to do some silent transitions after this visible transition.

Definition 3.9 (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 3.10. *$\gtrapprox$ is a relaxed expansion, and the following strict inclusions hold:*

$$\succ \;\subsetneq\; \gtrapprox \;\subsetneq\; \approx .$$

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 $a.b \succ a.\tau.b$, and $a \approx \tau.a$ holds but not $a \gtrapprox \tau.a$. ■

Relaxed expansion cannot be captured in the framework of weakly monotonic functions (Proposition 2.5): $\gtrapprox\bullet$ is not weakly monotonic. However, we can show that it is a controlled relation, so that it can be used with Proposition 3.4 or Theorem 3.6.

Theorem 3.11. *A relaxed expansion is a controlled relation. $\gtrapprox$ is a controlled bisimulation.*

Proof. We show that if $\mathcal{E}$ is a relaxed expansion, then it is also the case for $\mathcal{E}^\star$. Both points of Definition 3.1 follow easily. ■

In general, $\gtrapprox$ is not a congruence: for instance, in CCS, $a.b \gtrapprox a.\tau.b$ holds but not $\overline{a} \mid a.b \gtrapprox \overline{a} \mid a.\tau.b$. This is somewhat related to the problem of up to parallel composition, discussed in Subsection 2.3: as contexts may turn a visible action into a silent one, the stress we put on visible actions in the definition of $\gtrapprox$ is lost when adding parallel components.

[11] defines *almost weak bisimilarity*. This relation is very close to $\gtrapprox$, but coarser; it is a controlled bisimulation, and it is not a congruence in general. We preferred our version because it fits better within the style of the definitions of behavioural equivalences in our presentation.

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

Theorem 3.12. *Let $\mathcal{B}$ be a relation.*

If $\mathcal{B} \rightarrowtail \mathcal{B}^+$ and $\mathcal{B}$ terminates, then $\mathcal{B}$ is a controlled relation.

Theorem 3.13. *Let $\mathcal{B}$ be a relation.*

If $\mathcal{B} \rightarrowtail \mathcal{B}^\star$ and $\mathcal{B}^+ \xrightarrow{\tau}{}^+$ terminates, then $\mathcal{B}$ is a controlled relation.

Unlike for the case of $\gtrsim$, where the control on silent moves is fixed by the coinductive definition of the relation, in these two results we start with a relation that intuitively 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 $\mathcal{B} = \{\langle a, \tau.a\rangle\}$ is rejected because $\mathcal{B}$ evolves to $\mathcal{I} = \mathcal{B}^0$, and $\mathcal{B}^+ \xrightarrow{\tau}{}^+ = \{\langle a, a\rangle\}$ obviously does not terminate.

Theorems 3.12 and 3.13 provide up-to techniques that are incomparable with "up to expansion". There are processes that are not related by $\gtrsim$, but by a relation satisfying the conditions of the previous theorems: consider $\langle a \mid (\nu b)b, \tau.a\rangle$ or $\langle a + a, \tau.a\rangle$. Conversely, $\gtrsim$ cannot be captured by the above results: it does not fit in Theorem 3.12 because it is reflexive, and, since $a \gtrsim a|\tau \xrightarrow{\tau} a$, Theorem 3.12 is ruled out as well.

Like for controlled relations, there is no direct way to define the greatest relation satisfying the requirements of Theorems 3.12 or 3.13, 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 3.13 can thus be applied to systems exhibiting infinite chains of τ transitions.

Remark 3.14 (Controlled relations up-to)**.** 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 $\mathcal{F}^\omega(\mathcal{B})$. Depending on $\mathcal{F}$, this relation may be reflexive, which discards Theorem 3.12; in other cases, it might just be too tedious to prove the termination of $\mathcal{F}^\omega(\mathcal{B})$ or $\mathcal{F}^\omega(\mathcal{B})^+ \xrightarrow{\tau}{}^+$.

The theorems above give sufficient conditions for a relation to be a controlled. However, they can also be used directly, in order to prove that a relation is

contained in weak bisimilarity:

Corollary 3.15. *Let $\mathcal{R}$ be a relation.*

$$\textit{If } \mathcal{R}^{-1} \rightarrowtail \mathcal{R}^{-1} \cup \approx \textit{ and } \begin{cases} \mathcal{R} \rightarrowtail \mathcal{R}^{\star} \textit{ and } \mathcal{R}^{+} \xrightarrow{\tau}{}^{+} \textit{ terminates} \\ \textit{or } \mathcal{R} \rightarrowtail \mathcal{R}^{+} \textit{ and } \mathcal{R} \textit{ terminates,} \end{cases} \quad \textit{then } \mathcal{R} \subseteq \approx \ .$$

4 Results about Commuting Diagrams

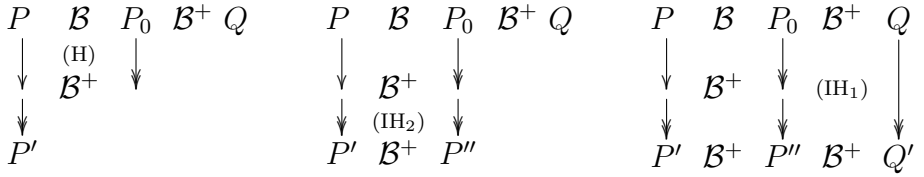
In this section, we work in the more general setting of *commuting diagrams*, commonly found in rewriting theory. In addition to $\mathcal{R}, \mathcal{S}$ we let $\rightarrow, \hookrightarrow$ and $\rightsquigarrow$ range over relations. As before, $\rightarrow^+$ (resp. $\twoheadrightarrow$) is the transitive (resp. reflexive transitive) closure of $\rightarrow$. We shall say that four relations $(\mathcal{R}, \rightarrow, \mathcal{S}, \hookrightarrow)$ form a *diagram*, denoted $(\mathcal{R}, \rightarrow) \gg (\mathcal{S}, \hookrightarrow)$, if whenever $P \mathcal{R} Q$ and $P \rightarrow P'$, there is Q' such that $P' \mathcal{S} Q'$ and $Q \hookrightarrow Q'$ (in our proofs, we shall often adopt the usual graphical notation for diagrams). We say that two relations $\mathcal{R}$ and $\rightarrow$ *commute* if $(\mathcal{R}, \rightarrow) \gg (\mathcal{R}, \rightarrow)$. Notice that a relation $\mathcal{R}$ is a simulation iff $\mathcal{R}$ commutes with $\xrightarrow{\alpha}\!\!\!\!\twoheadrightarrow$ for all $\alpha \in \mathcal{L}$.

4.1 A First Termination Argument

Lemma 4.1. *Let $\mathcal{B}$, $\rightarrow$ be two relations such that $\mathcal{B}$ terminates.*

$$\textit{If } (\mathcal{B}, \rightarrow) \gg (\mathcal{B}^+, \twoheadrightarrow), \textit{ then } \mathcal{B}^+ \textit{ and } \twoheadrightarrow \textit{ commute.}$$

Proof. Let $\phi(P')$ be the following predicate over processes: "For all P, Q such that $P \twoheadrightarrow P'$ and $P \mathcal{B}^+ Q$, there is Q' such that $Q \twoheadrightarrow Q'$ and $P' \mathcal{B}^+ Q'$". We prove that ϕ is true for any process by induction over the well-founded relation $\mathcal{B}^{-1}$, which leads to the induction hypothesis (IH_1): $\forall P'',\ P' \mathcal{B}^+ P'' \Rightarrow \phi(P'')$. Then we do a second induction on the derivation $P \twoheadrightarrow P'$, leading to a second induction hypothesis: (IH_2). The interesting case is represented on the first following diagram, where we close the first step using the hypothesis. We use the internal induction to obtain the second diagram, and the main induction to close the whole diagram (we check that $P' \mathcal{B}^+ P''$).



■

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

$$\mathcal{B} \triangleq \{\langle 2,3\rangle,\ \langle 3,4\rangle,\ \langle 1,0\rangle\} \qquad 0 \overset{\mathcal{B}}{\rightleftarrows} 1 \leftarrow 2 \overset{\mathcal{B}}{\circlearrowright} 3 \xrightarrow{\mathcal{B}} 4$$
$$\to \triangleq \{\langle 3,2\rangle,\ \langle 2,1\rangle,\ \langle 1,0\rangle\}$$

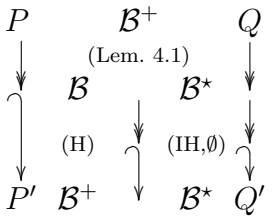
$\mathcal{B}$ terminates and satisfies the two alternative hypotheses; $2\mathcal{B}^\star 4$ and $2 \to 1$, but there is no i such that $4 \twoheadrightarrow i$ and $1\mathcal{B}^\star i$.

Lemma 4.1 has been first proposed in [4, p.47], and is more commonly stated as "if $\mathcal{B}$ terminates and $(\mathcal{B}, \to) \gg (\mathcal{B}^+, \twoheadrightarrow)$, then $\mathcal{B}^\star$ and $\twoheadrightarrow$ commute" ([13, Exercise 1.3.15]) However we are interested in showing the stronger results 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. As previously, we reason by well-founded induction, 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.*

$$\textit{If } \begin{cases} (\mathcal{B}, \to) \gg (\mathcal{B}^+, \twoheadrightarrow) \\ (\mathcal{B}, \hookrightarrow) \gg (\mathcal{B}^+, \twoheadrightarrow\hookrightarrow) \end{cases} \textit{ and } \begin{cases} (\mathcal{R}, \to) \gg (\mathcal{B}^\star\mathcal{R}, \twoheadrightarrow) \\ (\mathcal{R}, \hookrightarrow) \gg (\mathcal{B}^\star\mathcal{S}, \twoheadrightarrow\rightsquigarrow) \end{cases}$$
$$\textit{then } (\mathcal{B}^\star\mathcal{R}, \twoheadrightarrow\hookrightarrow) \gg (\mathcal{B}^\star\mathcal{S}, \twoheadrightarrow\rightsquigarrow)\ .$$

Proof. We reason by well-founded induction, with the predicate $\phi(P')$: "For all P, P_1, P_2, Q such that $P \twoheadrightarrow P_1 \hookrightarrow P'$ and $P\mathcal{B}^\star P_2\mathcal{R}Q$, there is Q' such that $Q \twoheadrightarrow\rightsquigarrow Q'$ and $P'\mathcal{B}^\star\mathcal{S}Q'$". If $P\mathcal{B}^+P_2$, we conclude with Lemma 4.3 and the induction hypothesis. Otherwise, $(P = P_2)$ we do an internal structural

induction over the derivation $P \twoheadrightarrow P_1$. Again, we use Lemma 4.3, and a case study allows us to conclude using the induction hypotheses. ■

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

Proof of Theorem 3.12. Let $\mathcal{B}$ be a relation such that $\mathcal{B} \rightarrowtail \mathcal{B}^+$ and $\mathcal{B}$ terminates. We show that $\mathcal{B}$ satisfies the requirement of Definition 3.1:

(1) Suppose $\mathcal{R} \overset{\tau}{\rightarrowtail} \mathcal{B}^\star\mathcal{R}$, we apply Proposition 4.4, taking $\xrightarrow{\tau}$ for $\rightarrow$, and the identity relation for $\hookrightarrow$, $\rightsquigarrow$, and $\mathcal{R}$ for $\mathcal{S}$.
(2) Suppose furthermore $\mathcal{R} \overset{\lambda}{\rightarrowtail} \mathcal{S}$ and $\mathcal{S} \overset{\tau}{\rightarrowtail} \mathcal{S}$. Lemma 4.1 ensures that $\mathcal{B}^+$ is a silent simulation. We apply Proposition 4.4, using $\xrightarrow{\tau}$ for $\rightarrow$, and $\xrightarrow{a}\xrightarrow{\tau}\!\!\!\!\rightarrow$ for $\hookrightarrow$ and $\rightsquigarrow$. Lemma 4.1 ensures that $\mathcal{B}^+$ is a silent simulation, and we check that the following diagrams can be closed:

$$\begin{array}{ccc} & \mathcal{B} & \\ {\scriptstyle a}\downarrow & \text{(H)} & \downarrow{\scriptstyle a} \\ & \mathcal{B}^+ & \\ {\scriptstyle \tau}\downarrow & \text{(Lem. 4.1)} & \downarrow{\scriptstyle \tau} \\ & \mathcal{B}^+ & \end{array} \qquad \begin{array}{ccc} & \mathcal{R} & \\ {\scriptstyle a}\downarrow & \text{(H)} & \downarrow{\scriptstyle a} \\ & \mathcal{S} & \\ {\scriptstyle \tau}\downarrow & \text{(Lem. 1.3)} & \downarrow{\scriptstyle \tau} \\ & \mathcal{S} & \end{array}$$

■

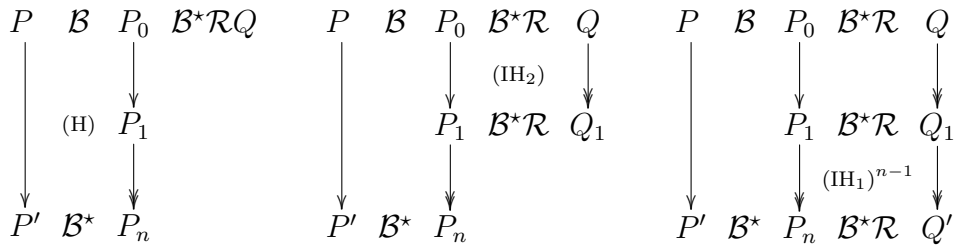
4.2 A Generalisation of Newman's Lemma

Lemma 4.5. *Let $\mathcal{B}, \rightarrow, \mathcal{R}$ be three relations such that $\mathcal{B}^+ \rightarrow^+$ terminates.*

If $(\mathcal{B}, \rightarrow) \gg (\mathcal{B}^\star, \twoheadrightarrow)$ and $(\mathcal{R}, \rightarrow) \gg (\mathcal{B}^\star\mathcal{R}, \twoheadrightarrow)$, then $\mathcal{B}^\star\mathcal{R}$ and $\twoheadrightarrow$ commute.

Proof. It suffices to prove $(\mathcal{B}^\star\mathcal{R}, \rightarrow) \gg (\mathcal{B}^\star\mathcal{R}, \twoheadrightarrow)$: the commutation result then follows by a simple induction. We use an induction over the well-founded order induced by the termination of $\mathcal{B}^+ \rightarrow^+$, with the predicate $\phi(P)$: "For all P', Q such that $P \rightarrow P'$ and $P\mathcal{B}^\star\mathcal{R}Q$, there is Q' such that $Q \twoheadrightarrow Q'$ and $P'\mathcal{B}^\star\mathcal{R}Q'$" ($\mathrm{IH}_1$). 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 $P_0 \rightarrow^+ P_n$). We use the internal induction to obtain Q_1 in the central diagram; this is possible since any process P'' such that $P_0 \mathcal{B}^+ \rightarrow^+ P''$ satisfies $P \mathcal{B}^+ \rightarrow^+ P''$: 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 commutation result:

Corollary 4.6. *Let $\mathcal{B}, \to$ be two relations such that $\mathcal{B}^+{\to}^+$ terminates.*

$$\textit{If } (\mathcal{B}, \to) \gg (\mathcal{B}^\star, \twoheadrightarrow), \textit{ then } \mathcal{B}^\star \textit{ and } \twoheadrightarrow \textit{ commute.}$$

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 $\to$.

Notice that the previous corollary admits a direct and elegant proof using the decreasing diagram techniques of van Oostrom et al. [2]:

Proof using decreasing diagram techniques. Take $A \triangleq \{\mathcal{B}_P \,/\, P \in \mathcal{P}\} \uplus \mathcal{P}$, and define the following relations:

$$\begin{array}{lll} \succ & \triangleq \{\langle P, \mathcal{B}_Q\rangle \,/\, P\mathcal{B} \twoheadrightarrow Q\} & \qquad \to_{\mathcal{B}_P} \triangleq \{\langle P, Q\rangle \,/\, P\mathcal{B}Q\} \\ & \quad \cup\ \{\langle \mathcal{B}_P, Q\rangle \,/\, P \to \mathcal{B}^\star Q\} & \qquad \to_P \triangleq \{\langle P, Q\rangle \,/\, P \to Q\} \end{array}$$

Then, since $\mathcal{B}^+{\to}^+$ terminates, $\succ$ is well-founded and we can apply the decreasing diagram technique, as presented in [2, Theorem 4.25] for commutation results:

$$\mathcal{B}^\star = (\cup_P \to_{\mathcal{B}_P})^\star \text{ and } \twoheadrightarrow = (\cup_P \to_P)^\star \text{ commute.}$$ ■

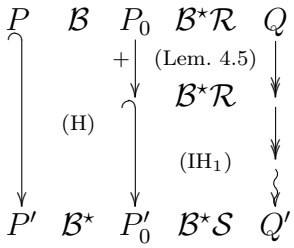
■

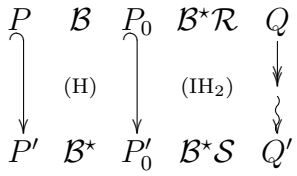
Remark 4.7. Results like Lemma 4.5 and Proposition 4.8 cannot be proved within the setting of [2], because they express properties beyond 'pure commutation'. A solution would be to rewrite the decreasing diagram proofs using stronger invariants – this is discussed in the concluding remarks.

Proposition 4.8. *Let $\mathcal{B}, \to, \mathcal{R}, \hookrightarrow, \mathcal{S}, \rightsquigarrow$ be six relations such that $\mathcal{B}^+ \to^+$ terminates.*

$$\textit{If } \begin{cases} (\mathcal{B}, \to) \gg (\mathcal{B}^\star, \twoheadrightarrow) \\ (\mathcal{B}, \hookrightarrow) \gg (\mathcal{B}^\star, \twoheadrightarrow\hookrightarrow) \end{cases} \quad \textit{and} \quad \begin{cases} (\mathcal{R}, \to) \gg (\mathcal{B}^\star\mathcal{R}, \twoheadrightarrow) \\ (\mathcal{R}, \hookrightarrow) \gg (\mathcal{B}^\star\mathcal{S}, \twoheadrightarrow\rightsquigarrow) \end{cases}$$
$$\textit{then } (\mathcal{B}^\star\mathcal{R}, \twoheadrightarrow\hookrightarrow) \gg (\mathcal{B}^\star\mathcal{S}, \twoheadrightarrow\rightsquigarrow) \ .$$

Proof. It suffices to prove $(\mathcal{B}^\star\mathcal{R}, \hookrightarrow) \gg (\mathcal{B}^\star\mathcal{S}, \twoheadrightarrow\rightsquigarrow)$: with Lemma 4.5, this yields the expected result. Again, we use a well-founded induction over the relation $\mathcal{B}^+ \to^+$, with the predicate $\phi(P)$: "For all P', Q such that $P \hookrightarrow P'$ and $P\mathcal{B}^\star\mathcal{R}Q$, there is Q' such that $Q \twoheadrightarrow\rightsquigarrow Q'$ and $P'\mathcal{B}^\star\mathcal{S}Q'$" ($\mathrm{IH}_1$), followed by an induction on the derivation $P\mathcal{B}^\star\mathcal{R}Q$ (IH_2). The interesting cases are represented on the following diagrams.





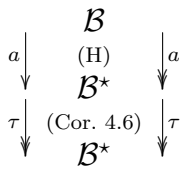
■

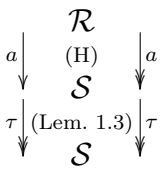
We can finally give the second deferred proof from the previous section. This proof closely follows the lines of the proof of Theorem 3.12, but uses the previous results:

Proof of Theorem 3.13. Let $\mathcal{B}$ be a relation such that $\mathcal{B} \rightarrowtail \mathcal{B}^\star$ and $\mathcal{B}^+ \xrightarrow{\tau}{}^+$ terminates. We show that $\mathcal{B}$ satisfies the requirement of Definition 3.1:

(1) Suppose $\mathcal{R} \rightarrowtail \xrightarrow{\tau} \mathcal{B}^\star\mathcal{R}$, we apply Proposition 4.8, taking $\xrightarrow{\tau}$ for $\to$, and the identity relation for $\hookrightarrow$, $\rightsquigarrow$, and $\mathcal{R}$ for $\mathcal{S}$.

(2) Suppose furthermore $\mathcal{R} \rightarrowtail \xrightarrow{\nu} \mathcal{S}$ and $\mathcal{S} \rightarrowtail \xrightarrow{\tau} \mathcal{S}$. We apply Proposition 4.8, using $\xrightarrow{\tau}$ for $\to$, and $\xrightarrow{a}\xrightarrow{\tau}\!\!\!\!\twoheadrightarrow$ for $\hookrightarrow$ and $\rightsquigarrow$. Corollary 4.6 ensures that $\mathcal{B}^\star$ is a silent simulation, and we check that the following diagrams can be closed:





■

A theorem prover formalisation of our results. The proofs about diagrams sometimes require nontrivial inductive reasoning, and it is easy to make mistakes when nesting several inductions.

These results, as well as all other results above in this paper have been formally checked using the Coq proof assistant [9]. These developments are available from [7] and the descriptions of the proofs we give actually closely follow the proof scripts. Also notice that since we work in a completely abstract setting, our development fits well to the technology offered by the calculus of inductive constructions for inductive reasoning about transition systems.

5 Application: Validating a Caching Technique

The up-to techniques presented in the paper in Sections 1 and 2 were for the most part already known. The uniform presentation we have given makes it possible to encompass the new techniques presented in Section 3.

Illustrating when the latter techniques turn out to be useful is not so easy: in most simple bisimulation proofs, expansion is sufficient in order to reason in a modular way. The only actual case where we found that expansion could not be used is a complex proof of correctness for an optimisation of a distributed abstract machine [5]. Due to the complexity of the system being analysed, the resulting proof of weak bisimilarity is rather involved, and goes beyond the scope of this paper. [8] presents a study of this example, where we use Theorem 3.13 in order to give a modular proof.

Here we illustrate the use of Theorem 3.12 by analysing a caching technique. This example could be expressed using CCS or π processes, however for the sake of clarity we give here a direct definition under the form of a simple LTS.

We study a system whose purpose is to serve *requests* for information by giving appropriate *answers*. In the simple version, the system accepts a request, computes the corresponding answer (for example, by searching for it in a database), and returns it. The optimised version of the system maintains a *cache*, in which previously computed answers can be stored, as well as some answers that the system might want to compute in advance (e.g., one could think of predicting requests that are deemed to be liable, in view of previous sessions).

Processes are pairs $[R \,\|\, C]$, where R is a set of *requests*, and C is a set of *cached values*. In both cases, we denote by $x::S$ the addition of an element x

to a set S, and by $\#S$ the size of the set S. The rules are given below:

$$[R \parallel C] \xrightarrow{a_r} [r::R \parallel C] \qquad [r::R \parallel r::C] \xrightarrow{b_r} [R \parallel r::C]$$
$$[R \parallel C] \xrightarrow{\tau} [R \parallel r::C] \qquad [R \parallel s::C] \xrightarrow{\tau} [R \parallel r::C]$$

The first visible action, a_r is the reception of a request r. The two transitions at the bottom are silent: they show how a value can be added or replaced in the cache. Once the answer to this request is available, it can be sent using the second visible action, b_r.

Within a large proof of some property of the system, we would like to be able to reason *up to the cache*, which means manipulating relations where all processes have an empty cache.

It can be proved that for any set of requests R, $[R \parallel C] \approx [R \parallel \emptyset]$. However, this is not sufficient to obtain an up-to technique: the cache is filled using silent actions, for which reasoning up to bisimilarity is not allowed. It does neither hold that $[R \parallel C] \gtrsim [R \parallel \emptyset]$ for any R: if R and C both contain a value r, $[R \parallel C]$ can do a visible action by completing the request r, while $[R \parallel \emptyset]$ has to compute r before being able to do the corresponding visible action. With Theorem 3.12, we prove that $\mathcal{B} \triangleq \{\langle [R \parallel C], [R \parallel C'] \rangle \ / \ \#C > \#C'\}$ is a controlled bisimulation, which gives a way to reason 'up to the cache'.

6 Concluding Remarks

An up-to theory for strong bisimilarity is defined [10], and has already been extended to weak bisimilarity in [12, Section 2.4.3.3]. Unlike in [12], the framework we have introduced here is based on a separation between visible and silent transitions. This make it possible to provide flexible and powerful proof techniques on visible transitions. For instance, reasoning up to weak bisimilarity is possible as long as it is restricted to visible actions (Theorem 2.4). This result is present in [12, Exercise 2.4.64], but cannot be obtained as an instance of the general framework presented in [12]: the distinction between visible and silent transitions is required. By contrast, our setting does not fully encompass the standard up to context technique, while this technique fits in the framework of [12] (Lemma 2.4.52), and can thus nicely be combined with other techniques, like up to expansion (Exercise 2.4.67).

The main improvement over [12] in this work is the introduction of controlled relations, that allows us to use the new techniques given by Theorems 3.12 and 3.13 in our modular setting.

Due to the presence of labelled transitions, results about decreasing diagrams from [2] are not applicable directly in our setting. As announced in Remark 4.7, we could easily adapt these results by strengthening the invariants used in order to keep track of visible, preserved, actions. We would then obtain the result corresponding to Theorem 3.6, but at the cost of less modularity (Proposition 3.7 cannot be adapted, at least directly). We plan to study whether this theory could be extended in a more fundamental way, by generalising the notions of silent and visible actions. This could be a way to provide an abstract approach for the definition of 'up to transitivity' techniques based on termination guarantees.

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.

Experience on case studies (such as the one in [5,8]) has to be developed in order to have a better understanding of how our techniques can be best combined, and how the distinction between visible and internal computation steps should be tuned.

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] A. Geser. *Relative Termination.* PhD thesis, Universität Passau, Germany, 1990.

[5] D. Hirschkoff, D. Pous, and D. Sangiorgi. A Correct Abstract Machine for Safe Ambients. In *Proc. COORDINATION '05*, volume 3454 of *Lecture Notes in Computer Science*, pages 17–32. Springer Verlag, 2005.

[6] D. Pous. Up-to Techniques for Weak Bisimulation. In *Proc. 32th ICALP*, volume 3580 of *Lecture Notes in Computer Science*, pages 730–741. Springer Verlag, 2005.

[7] D. Pous. Web appendix of this paper, 2005. `http://perso.ens-lyon.fr/damien.pous/upto`.

[8] D. Pous. On Bisimulation Proofs for the Analysis of Distributed Abstract Machines. To appear in *Proc. TGC '06*. Springer Verlag, 2006.

[9] INRIA projet Logical. The Coq proof assistant. `http://coq.inria.fr/`.

[10] D. Sangiorgi. On the Bisimulation Proof Method. *Journal of Mathematical Structures in Computer Science*, 8:447–479, 1998.

[11] D. Sangiorgi and R. Milner. The problem of "Weak Bisimulation up to". In *Proc. 3rd CONCUR*, volume 630 of *Lecture Notes in Computer Science*, pages 32–46. Springer Verlag, 1992.

[12] D. Sangiorgi and D. Walker. *The π-calculus: a Theory of Mobile Processes*. Cambridge University Press, 2001.

[13] TeReSe. *Term Rewriting Systems*. Cambridge University Press, 2003.