

# Equivalence Checking for Infinite Systems using Parameterized Boolean Equation Systems

Taolue Chen<sup>1 \*</sup>, Bas Ploeger<sup>2 \*\*</sup>, Jaco van de Pol<sup>1,2</sup>, and Tim A.C. Willemse<sup>2 \*\*\*</sup>

<sup>1</sup> CWI, Department of Software Engineering,

P.O. Box 94079, 1090 GB Amsterdam, The Netherlands

<sup>2</sup> Eindhoven University of Technology, Design and Analysis of Systems Group,

P.O. Box 513, 5600 MB Eindhoven, The Netherlands

**Abstract.** In this paper, we provide a transformation from the branching bisimulation problem for infinite, concurrent, data-intensive systems in linear process format, into solving Parameterized Boolean Equation Systems. We prove correctness and illustrate the approach with two examples. We also provide small adaptations to obtain similar transformations for strong and weak bisimulations and simulation equivalences.

## 1 Introduction

A standard approach for verifying the correctness of a computer system or a communication protocol is the *equivalence-based methodology*. This framework was introduced by Milner [23] and has been intensively explored in process algebra. One proceeds by establishing two descriptions (models) for one system: a *specification* and an *implementation*. The former describes the desired high-level behavior, while the latter provides lower-level details indicating how this behavior is to be achieved. Then an implementation is said to be correct, if it behaves “the same as” its specification. Similarly, one could check whether the implementation has “at most” the behavior allowed by the specification. Several *behavioral equivalences and preorders* have been introduced to relate specifications and implementations, supporting different notions of observability. These include strong, weak [24], and branching bisimulation [11, 4].

*Equivalence Checking for Finite Systems.* Checking strong bisimulation of finite systems can be done very efficiently. The basic algorithm is the well-known *partition refinement* algorithm [26]. For weak bisimulation checking, one could compute the transitive closure of  $\tau$ -transitions, and thus lift the algorithms for strong bisimulation to the weak one. This is viable but costly, since it might incur a quadratic blow-up w.r.t.

---

\* This author is partially supported by Dutch Bsik project BRICKS, 973 Program of China (2002CB312002), NSF of China (60233010, 60273034, 60403014), 863 Program of China (2005AA113160, 2004AA112090).

\*\* This author is partially supported by the Netherlands Organisation for Scientific Research (NWO) under VoLTS grant number 612.065.410.

\*\*\* This author is partially supported by the Netherlands Organisation for Scientific Research (NWO) under BRICKS/FOCUS grant number 642.000.602.

the original LTSs. Instead, one could employ the more efficient solution by [15] for checking branching bisimulation, as branching and weak bisimulation often coincide.

Alternatively, one can transform several bisimulation relations into Boolean Equation Systems (BES). Various encodings have been proposed in the literature [1, 7, 22], leading to efficient tools. In [1] it is shown that the BESs obtained from equivalence relations have a special format; the encodings of [22] even yield alternation free BESs (cf. definition of alternation depth in [21]) for up to five different behavioral equivalences. Solving alternation free BESs can be done very efficiently. However, finiteness of the graphs is crucial for the encodings yielding alternation free BESs.

It is interesting to note that the  $\mu$ -calculus model checking problem for finite systems can also be transformed to the problem of solving a BES [1, 21]. Hence, a BES solver, e.g. [22], provides a uniform engine for verification by model checking and equivalence checking for finite systems.

*Our Contribution.* In this paper, we focus on equivalence checking for *infinite* systems. Generally for concurrent systems with data, the induced labeled transition system (LTS) is no longer *finite*, and the traditional algorithms fail for *infinite* transition graphs. The symbolic approach needed for infinite systems depends on the specification format. We use *Linear Process Equations* (LPEs), which originate from  $\mu$ CRL [14], a process algebra with abstract data types, and describe the system by a finite set of guarded, nondeterministic transitions. LPEs are Turing complete, and many formalisms can be compiled to LPEs without considerable blow-up. Therefore, our methods essentially also apply to LOTOS [5], timed automata [2], I/O-automata [20], finite control  $\pi$ -calculus [25], UNITY [6], etc.

The solution we propose in this paper is inspired by [12], where the question whether an LPE satisfies a *first-order*  $\mu$ -calculus formula is transformed into a *Parameterized Boolean Equation System* (PBES). PBESs extend boolean equation systems with data parameters and quantifiers. Heuristics, techniques [17], and tool support [16] have been developed for solving PBESs. This is still subject to ongoing research. Also in [28] such equation systems are used for model checking systems with data and time. In general, solving PBESs cannot be completely automated.

We propose to check branching bisimilarity of infinite systems by solving recursive equations. In particular, we show how to generate a PBES from two LPEs. The resulting PBES has alternation depth two. We prove that the PBES has a positive solution if and only if the two (infinite) systems are branching bisimilar. Moreover, we illustrate the technique by two examples on queues, and show similar transformations for strong and Milner's weak bisimulation [24] and branching simulation equivalence [10].

There are good reasons to translate branching bisimulation for infinite systems to solving PBESs, even though both problems are undecidable. The main reason is that solving PBESs is a more fundamental problem, as it boils down to solving equations between predicates. The other reason is that model checking  $\mu$ -calculus with data has already been mapped to PBESs. Hence all efforts in solving PBESs (like [17]) can now be freely applied to the bisimulation problem as well.

*Related Work.* We already mentioned related work on finite systems, especially [1, 22]. There are several approaches on which we want to comment in more detail.

The cones and foci method [9] rephrases the question whether two LPEs are bisimilar in terms of proof obligations on data objects. Basically, the user must first identify invariants, a focus condition, and a state mapping. In contrast, generating a PBES requires no human ingenuity, although solving the PBES still may. Furthermore, our solution is considerably more general, because it lifts two severe limitations of the cones and foci method. The first limitation is that the cones and foci method only works in case the branching bisimulation is functional (this means that a state in the implementation can only be related to a unique state in the specification). Another severe limitation of the cones and foci method is that it cannot handle specifications with  $\tau$ -transitions. In some protocols (e.g. the bounded retransmission protocol [13]) this condition is not met and thus the cones and foci method fails. In our example on unbounded queues, both systems perform  $\tau$  steps, and their bisimulation is not functional.

Our work can be seen as the generalization of [19] to weak and branching equivalences. In [19], Lin proposes Symbolic Transition Graphs with Assignments (STGA) as a new model for message-passing processes. An algorithm is also presented which computes bisimulation formulae for finite state STGAs, in terms of the greatest solutions of a *predicate equation system*. This corresponds to an alternation free PBES, and thus it can only deal with strong bisimulation.

The extension of Lin’s work for strong bisimulation to weak and branching equivalences is not straightforward. This is testified by the encoding of weak bisimulation in predicate systems by Kwak *et al.* [18]. However, their encoding is not generally correct for STGA, as they use a conjunction over the complete  $\tau$ -closure of a state. This only works in case that the  $\tau$ -closure of every state is finite, which is generally not the case for STGA, also not for our LPEs. Alternation depth 2 seems unavoidable but does not occur in [18]. Note that for finite LTS a conjunction over the  $\tau$ -closure is possible [22], but leads to a quadratic blow-up of the BES in the worst case.

*Structure of the Paper.* The paper is set up as follows. In Section 2, we provide background knowledge on linear process equations, bisimulation equivalences and fixpoint theory. In Section 3, PBESs are reviewed. Section 4 is devoted to the presentation of the translation algorithm and the justification of its correctness. In Section 5, we provide two examples to illustrate the use of our algorithm. In Section 6, we demonstrate how to adapt the algorithm for branching bisimulation to strong and weak bisimulations and simulation equivalence. The paper is concluded in Section 7.

## 2 Preliminaries

### 2.1 Linear Processes

Linear process equations have been proposed as a *symbolic* representation of general (infinite) labeled transition systems. In an LPE, the behavior of a process is denoted as a state vector of typed variables, accompanied by a set of condition-action-effect rules. LPEs are widely used in  $\mu$ CRL [14], a language for specifying concurrent systems and protocols in an algebraic style. We mention that  $\mu$ CRL has complete automatic tool support to generate LPEs from  $\mu$ CRL specifications.

**Definition 1 (Linear Process Equation).** A linear process equation is a parameterized equation taking the form

$$M(d : D) = \sum_{a \in \text{Act}} \sum_{e_a : E_a} h_a(d, e_a) \implies a(f_a(d, e_a)) \cdot M(g_a(d, e_a))$$

where  $f_a : D \times E_a \rightarrow D_a$ ,  $g_a : D \times E_a \rightarrow D$  and  $h_a : D \times E_a \rightarrow \mathbb{B}$  for each  $a \in \text{Act}$ . Note that here  $D$ ,  $D_a$  and  $E_a$  are general data types and  $\mathbb{B}$  is the boolean type.

In the above definition, the LPE  $M$  specifies that if in the current state  $d$  the condition  $h_a(d, e_a)$  holds for any  $e_a$  of sort  $E_a$ , then an action  $a$  carrying data parameter  $f_a(d, e_a)$  is possible and the effect of executing this action is the new state  $g_a(d, e_a)$ . The values of the condition, action parameter and new state may depend on the current state and a summation variable  $e_a$ .

For simplicity and without loss of generality, we restrict ourselves to a single variable at the left-hand side in all our theoretical considerations and to the use of non-terminating processes. That is, we do not consider processes that, apart from executing an infinite number of actions, also have the possibility to perform a finite number of actions and then terminate successfully. Including multiple variables and termination in our theory does not pose any theoretical challenges, but is omitted from our exposition for brevity. The operational semantics of LPEs is defined in terms of *labeled transition systems*.

**Definition 2 (Labeled Transition System).** The labeled transition system of an LPE (as defined in Definition 1) is a quadruple  $\mathcal{M} = \langle \mathcal{S}, \Sigma, \rightarrow, s_0 \rangle$ , where

- $\mathcal{S} = \{d \mid d \in D\}$  is the (possibly infinite) set of states;
- $\Sigma = \{a(d) \mid a \in \text{Act} \wedge d \in D_a\}$  is the (possibly infinite) set of labels;
- $\rightarrow = \{(d, a(d'), d'') \mid a \in \text{Act} \wedge \exists e_a \in E_a. h_a(d, e_a) \wedge d' = f_a(d, e_a) \wedge d'' = g_a(d, e_a)\}$  is the transition relation;
- $s_0 = d_0 \in \mathcal{S}$ , for a given  $d_0 \in D$ , is the initial state.

For an LPE  $M$ , we usually write  $d \xrightarrow{a(d')} M d''$  to denote the fact that  $(d, a(d'), d'')$  is in the transition relation of the LTS of  $M$ . We will omit the subscript  $M$  when it is clear from the context. Following Milner [24], the derived transition relation  $\Rightarrow$  is defined as the reflexive, transitive closure of  $\rightarrow$  (i.e.  $(\rightarrow)^*$ ), and  $\overset{\alpha}{\Rightarrow}$ ,  $\hat{\overset{\alpha}{\Rightarrow}}$  and  $\bar{\overset{\alpha}{\Rightarrow}}$  are defined in the standard way as follows:

$$\overset{\alpha}{\Rightarrow} \stackrel{\text{def}}{=} \Rightarrow \overset{\alpha}{\Rightarrow} \quad \hat{\overset{\alpha}{\Rightarrow}} \stackrel{\text{def}}{=} \begin{cases} \Rightarrow & \text{if } \alpha = \tau \\ \overset{\alpha}{\Rightarrow} & \text{otherwise.} \end{cases} \quad \bar{\overset{\alpha}{\Rightarrow}} \stackrel{\text{def}}{=} \begin{cases} \rightarrow \cup \text{Id} & \text{if } \alpha = \tau \\ \overset{\alpha}{\rightarrow} & \text{otherwise.} \end{cases}$$

## 2.2 Bisimulation equivalences

We now introduce several well-known equivalences. The definitions below are with respect to an arbitrary, given labeled transition system  $\mathcal{M} = \langle \mathcal{S}, \Sigma, \rightarrow, s_0 \rangle$ .

**Definition 3 (Strong Bisimulation).** A binary relation  $\mathcal{R}$  is a strong bisimulation, iff it is symmetric and whenever  $s\mathcal{R}t$ , for all  $\alpha$ , if  $s \xrightarrow{\alpha} s'$ , then  $t \xrightarrow{\alpha} t'$  for some  $t'$  such that  $s'\mathcal{R}t'$ .

Strong bisimilarity, denoted by  $\leftrightarrow_s$ , is the largest strong bisimulation.

**Definition 4 (Branching (Bi)simulations).** A binary relation  $\mathcal{R} \subseteq S \times S$  is a semi-branching simulation, iff whenever  $s\mathcal{R}t$  then for all  $\alpha \in \Sigma$  and  $s' \in S$ , if  $s \xrightarrow{\alpha} s'$ , then  $t \Rightarrow t' \xrightarrow{\alpha} t''$  for some  $t', t'' \in S$  such that  $s\mathcal{R}t'$  and  $s'\mathcal{R}t''$ . We say that:

- $\mathcal{R}$  is a semi-branching bisimulation, if both  $\mathcal{R}$  and  $\mathcal{R}^{-1}$  are semi-branching simulations.
- $s$  is branching bisimilar to  $t$ , denoted by  $s \leftrightarrow_b t$ , iff there exists a semi-branching bisimulation  $\mathcal{R}$ , such that  $s\mathcal{R}t$ .
- $s$  is branching simulation equivalent to  $t$ , iff there exist  $\mathcal{R}$  and  $\mathcal{Q}$ , such that  $s\mathcal{R}t$  and  $t\mathcal{Q}s$  and both  $\mathcal{R}$  and  $\mathcal{Q}$  are semi-branching simulations.

Note that although a semi-branching simulation is not necessarily a branching simulation, it is shown in [4] that this definition of branching bisimilarity coincides with the original definition in [11]. Therefore, in the sequel we take the liberty to use *semi-branching* and *branching* interchangeably. In the theoretical considerations in this paper, semi-branching relations are more convenient as they allow for shorter and clearer proofs of our theorems.

**Definition 5 (Weak Bisimulation).** A binary relation  $\mathcal{R} \subseteq S \times S$  is an (early) weak bisimulation, iff it is symmetric and whenever  $s\mathcal{R}t$  then for all  $\alpha \in \Sigma$  and  $s' \in S$ , if  $s \xrightarrow{\alpha} s'$ , then  $t \xRightarrow{\alpha} t'$  for some  $t' \in S$  such that  $s'\mathcal{R}t'$ .

Weak bisimilarity, denoted by  $\leftrightarrow_w$ , is the largest weak bisimulation.

### 2.3 Fixpoints and Complete Lattices

A *partial order* on a set  $U$  is a binary relation  $\leq \subseteq U \times U$  which is *reflexive*, *antisymmetric* and *transitive*. For any function  $f : U \rightarrow U$ ,  $f$  is called *monotonic*, if and only if  $\forall x, y \in U. x \leq y \implies f(x) \leq f(y)$ . Given a set  $X \subseteq U$ , we define its set of *lower bounds* as  $\{y \in U \mid \forall x \in X. y \leq x\}$ . The operator  $\bigwedge X$  denotes the *greatest lower bound* (g.l.b.) of the set  $X$ . The set of *upper bounds* and the *least upper bound* (l.u.b., denoted by  $\bigvee X$ ), are defined symmetrically. A *complete lattice* is a set  $L$  and a partial order  $\leq$  on  $L$  such that for any  $X \subseteq L$ ,  $\bigwedge X$  exists. In particular, for any set  $S$ ,  $(\wp(S), \subseteq)$  always constitutes a complete lattice, where  $\wp(S)$  is the standard powerset construction.

Let  $(L, \leq)$  be a complete lattice and let  $f : L \rightarrow L$  be a monotonic function. The least fixpoint of  $f$  is the least element  $x$  such that  $f(x) = x$ , or, equivalently, such that  $f(x) \leq x$ . The dual holds for the greatest fixpoint, the greatest element  $x$  such that  $f(x) = x$ . The well-known Knaster-Tarski theorem [27] states that the set of fixpoints of  $f$  in  $L$  is also a complete lattice. Since complete lattices cannot be empty, the theorem in particular guarantees the *existence* of at least one fixpoint of  $f$ , and even the existence of a least (or greatest) fixpoint. In particular, the least fixpoint ( $\mu$ ) and the greatest fixpoint ( $\nu$ ) of any monotonic function  $f : L \rightarrow L$  can be defined as:

$\mu f = \bigwedge\{x \mid f(x) \leq x\}$  and  $\nu f = \bigvee\{x \mid x \leq f(x)\}$ . From now on we use  $\sigma$  to denote either  $\mu$  or  $\nu$  and we abbreviate  $\sigma(\lambda x.f(x))$  as  $\sigma x.f(x)$ .

### 3 Parameterized Boolean Equation Systems

A Parameterized Boolean Equation System (PBES) is a sequence of equations of the form

$$\sigma X(d : D) = \phi$$

where  $X$  is a predicate variable (from a set  $\mathcal{P}$  of predicate variables) that binds a data variable  $d$  (from a set  $\mathcal{D}$  of data variables) that may occur freely in the *predicate formula*  $\phi$ . Apart from data variable  $d$ ,  $\phi$  can contain data terms, boolean connectives, quantifiers over (possibly infinite) data domains, and predicate variables. Predicate formulae  $\phi$  are formally defined as follows:

**Definition 6 (Predicate Formula).** A predicate formula is a formula  $\phi$  in positive form, defined by the following grammar:

$$\phi ::= b \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \forall d : D. \phi \mid \exists d : D. \phi \mid X(e)$$

where  $b$  is a data term of sort  $\mathbb{B}$ , possibly containing data variables  $d \in \mathcal{D}$ . Furthermore,  $X \in \mathcal{P}$  is a (parameterized) predicate variable and  $e$  is a data term.

Note that negation does not occur in predicate formulae, except as an operator in data terms. We use  $b \implies \phi$  as a shorthand for  $\neg b \vee \phi$  for terms  $b$  of sort  $\mathbb{B}$ .

The semantics of predicates is dependent on the semantics of data terms. For a closed term  $e$ , we assume an interpretation function  $\llbracket e \rrbracket$  that maps  $e$  to the data element it represents. For open terms, we use a *data environment*  $\varepsilon$  that maps each variable from  $\mathcal{D}$  to a data value of the right sort. The interpretation of an open term  $e$  is denoted as  $\llbracket e \rrbracket \varepsilon$  in the standard way.

**Definition 7 (Semantics).** Let  $\theta : \mathcal{P} \rightarrow \wp(D)$  be a predicate environment and  $\varepsilon : \mathcal{D} \rightarrow D$  be a data environment. The interpretation of a predicate formula  $\phi$  in the context of environment  $\theta$  and  $\varepsilon$ , written as  $\llbracket \phi \rrbracket \theta \varepsilon$ , is either true or false, determined by the following induction:

$$\begin{aligned} \llbracket b \rrbracket \theta \varepsilon &= \llbracket b \rrbracket \varepsilon \\ \llbracket \phi_1 \wedge \phi_2 \rrbracket \theta \varepsilon &= \llbracket \phi_1 \rrbracket \theta \varepsilon \text{ and } \llbracket \phi_2 \rrbracket \theta \varepsilon \\ \llbracket \phi_1 \vee \phi_2 \rrbracket \theta \varepsilon &= \llbracket \phi_1 \rrbracket \theta \varepsilon \text{ or } \llbracket \phi_2 \rrbracket \theta \varepsilon \\ \llbracket \forall d : D. \phi \rrbracket \theta \varepsilon &= \text{for all } v \in D, \llbracket \phi \rrbracket \theta(\varepsilon[v/d]) \\ \llbracket \exists d : D. \phi \rrbracket \theta \varepsilon &= \text{there exists } v \in D, \llbracket \phi \rrbracket \theta(\varepsilon[v/d]) \\ \llbracket X(e) \rrbracket \theta \varepsilon &= \text{true if } \llbracket e \rrbracket \varepsilon \in \theta(X) \text{ and false otherwise} \end{aligned}$$

**Definition 8 (Parameterized Boolean Equation System).** A parameterized boolean equation system is a finite sequence of equations of the form  $\sigma X(d : D) = \phi$  where  $\phi$  is a predicate formula in which at most  $d$  may occur as a free data variable. The empty equation system is denoted by  $\epsilon$ .

In the remainder of this paper, we abbreviate parameterized boolean equation system to *equation system*. We say an equation system is *closed* whenever every predicate variable occurring at the right-hand side of some equation occurs at the left-hand side of some equation. The *solution* to an equation system is defined in the context of a predicate environment, as follows.

**Definition 9 (Solution to an Equation System).** *Given a predicate environment  $\theta$  and an equation system  $\mathcal{E}$ , the solution  $\llbracket \mathcal{E} \rrbracket \theta$  to  $\mathcal{E}$  is an environment that is defined as follows, where  $\sigma$  is the greatest or least fixpoint, defined over the complete lattice  $\wp(D)$ .*

$$\begin{aligned} \llbracket \epsilon \rrbracket \theta &= \theta \\ \llbracket (\sigma X (d : D) = \phi) \mathcal{E} \rrbracket \theta &= \llbracket \mathcal{E} \rrbracket (\theta \left[ \sigma \mathcal{X} \in \wp(D) . \lambda v \in D . \llbracket \phi \rrbracket (\llbracket \mathcal{E} \rrbracket \theta [\mathcal{X}/X]) [v/d]/X \right]) \end{aligned}$$

For *closed* equation systems, the solution for the binding predicate variables does not depend on the given environment  $\theta$ . In such cases, we refrain from writing the environment explicitly.

## 4 Translation for Branching Bisimulation

We define a translation that encodes the problem of finding the largest branching bisimulation in the problem of solving an equation system.

**Definition 10.** *Let  $M$  and  $S$  be LPEs of the following form:*

$$\begin{aligned} M(d : D^M) &= \sum_{a \in \text{Act}} \sum_{e_a \in E_a^M} h_a^M(d, e_a) \implies a(f_a^M(d, e_a)) . M(g_a^M(d, e_a)) \\ S(d : D^S) &= \sum_{a \in \text{Act}} \sum_{e_a \in E_a^S} h_a^S(d, e_a) \implies a(f_a^S(d, e_a)) . S(g_a^S(d, e_a)) \end{aligned}$$

*Given initial states  $d : D^M$  and  $d' : D^S$ , the equation system that corresponds to the branching bisimulation between LPEs  $M(d)$  and  $S(d')$  is constructed by the function *brbisim* (see Algorithm 1).*

The main function *brbisim* returns an equation system in the form  $\nu E_2 \mu E_1$  where the bound predicate variables in  $E_2$  are denoted by  $X$  and that in  $E_1$  are denoted by  $Y$ . Intuitively,  $E_2$  is used to characterize the (branching) bisimulation while  $E_1$  is used to absorb the  $\tau$  actions. The equation system's predicate formulae are constructed from the syntactic ingredients from LPEs  $M$  and  $S$ . Note that although we talk about the model ( $M$ ) and the specification ( $S$ ), the two systems are treated completely symmetrically. As we will show in Theorem 2, the solution for  $X^{M,S}$  in the resulting equation system gives the largest branching bisimulation relation between  $M$  and  $S$  as a predicate on  $D^M \times D^S$ .

---

**Algorithm 1** Generation of a PBES for Branching Bisimulation
 

---

*brbisim* =  $\nu E_2 \mu E_1$ , **where**

$$\begin{aligned} E_2 &:= \{ X^{M,S}(d : D^M, d' : D^S) = \text{match}^{M,S}(d, d') \wedge \text{match}^{S,M}(d', d) , \\ &\quad X^{S,M}(d' : D^S, d : D^M) = X^{M,S}(d, d') \} \\ E_1 &:= \{ Y_a^{p,q}(d : D^p, d' : D^q, e : E_a^p) = \text{close}_a^{p,q}(d, d', e) \\ &\quad \mid a \in \text{Act} \wedge (p, q) \in \{(M, S), (S, M)\} \} \end{aligned}$$

Where we use the following abbreviations, for all  $a \in \text{Act} \wedge (p, q) \in \{(M, S), (S, M)\}$ :

$$\text{match}^{p,q}(d : D^p, d' : D^q) = \bigwedge_{a \in \text{Act}} \forall e : E_a^p. (h_a^p(d, e) \implies Y_a^{p,q}(d, d', e));$$

$$\begin{aligned} \text{close}_a^{p,q}(d : D^p, d' : D^q, e : E_a^p) &= \exists e' : E_a^q. (h_a^q(d', e') \wedge Y_a^{p,q}(d, g_a^q(d', e'), e)) \\ &\quad \vee (X^{p,q}(d, d') \wedge \text{step}_a^{p,q}(d, d', e)); \end{aligned}$$

$$\begin{aligned} \text{step}_a^{p,q}(d : D^p, d' : D^q, e : E_a^p) &= (a = \tau \wedge X^{p,q}(g_a^p(d, e), d')) \vee \\ &\quad \exists e' : E_a^q. h_a^q(d', e') \wedge (f_a^p(d, e) = f_a^q(d', e')) \wedge X^{p,q}(g_a^p(d, e), g_a^q(d', e')); \end{aligned}$$


---

#### 4.1 Correctness of Transformation.

In this section we confirm the relation between the branching bisimulation problem and the problem of solving an equation system. Before establishing the correctness of the transformation presented above, we first provide a fixpoint characterization for (semi-) branching bisimilarity, which we exploit in the correctness proof of our algorithm. For brevity, given any LPEs  $M$  and  $S$ , and any binary relation  $\mathcal{B}$  over  $D^M \times D^S$ , we define a functional  $\mathcal{F}$  as

$$\begin{aligned} \mathcal{F}(\mathcal{B}) &= \{ (d, d') \mid \forall a \in \text{Act}, e_a \in E_a^M. h_a^M(d, e_a) \implies \\ &\quad \exists d'_2, d'_3. d' \Rightarrow_S d'_2 \wedge d'_2 \xrightarrow{a(f_a^M(d, e_a))}_S d'_3 \wedge (d, d'_2) \in \mathcal{B} \wedge (g_a^M(d, e_a), d'_3) \in \mathcal{B}, \\ &\quad \text{and } \forall a \in \text{Act}, e'_a \in E_a^S. h_a^S(d', e'_a) \implies \\ &\quad \exists d_2, d_3. d \Rightarrow_M d_2 \wedge d_2 \xrightarrow{a(f_a^S(d', e'_a))}_M d_3 \wedge (d_2, d') \in \mathcal{B} \wedge (d_3, g_a^S(d', e'_a)) \in \mathcal{B} \} \end{aligned}$$

We claim that branching bisimilarity is the *maximal* fixpoint of functional  $\mathcal{F}$  (i.e.  $\nu B. \mathcal{F}(B)$ ).

**Lemma 1.**  $\leftrightarrow_b = \nu B. \mathcal{F}(B)$ .

*Proof.* The following two obvious facts follow directly from the definitions:

- (i)  $\mathcal{F}$  is monotonic;
- (ii)  $\mathcal{B}$  is a semi-branching bisimulation if and only if  $\mathcal{F}(\mathcal{B}) = \mathcal{B}$  and thus  $\leftrightarrow_b = \bigcup \{ \mathcal{B} \mid \mathcal{F}(\mathcal{B}) = \mathcal{B} \}$ .

Then we have

1. By (ii), for any  $\mathcal{B}$ ,  $\mathcal{F}(\mathcal{B}) = \mathcal{B}$  implies  $\mathcal{B} \subseteq \leftrightarrow_b$ .
2. We show  $\leftrightarrow_b \subseteq \mathcal{F}(\leftrightarrow_b)$ . For any  $(d, d') \in \leftrightarrow_b$ , there exists some  $\mathcal{B}$  such that  $\mathcal{F}(\mathcal{B}) = \mathcal{B}$  and  $(d, d') \in \mathcal{B}$ . It follows that  $(d, d') \in \mathcal{F}(\mathcal{B})$ . Since (i),  $\mathcal{F}(\mathcal{B}) \subseteq \mathcal{F}(\leftrightarrow_b)$ . It follows that  $(d, d') \in \mathcal{F}(\leftrightarrow_b)$ . Hence,  $\leftrightarrow_b \subseteq \mathcal{F}(\leftrightarrow_b)$ .



By the Knaster-Tarski theorem [27] and (i), we have  $\nu\mathcal{F} = \bigcup\{\mathcal{B} \mid \mathcal{B} \subseteq \mathcal{F}(\mathcal{B})\}$ . Since  $\leftrightarrow_b \subseteq \mathcal{F}(\leftrightarrow_b)$ ,  $\leftrightarrow_b \subseteq \nu B.\mathcal{F}(B)$ . By (1),  $\nu B.\mathcal{F}(B) \subseteq \leftrightarrow_b$ . It follows that  $\leftrightarrow_b = \nu B.\mathcal{F}(B)$ .  $\square$

For proving the correctness of our translation, we first solve  $\mu E_1$  given an arbitrary solution for  $X$ .

**Theorem 1.** *For any LPEs  $M$  and  $S$ , let  $\mu E_1$  be generated by Algorithm 1, let  $\eta$  be an arbitrary predicate environment, and let  $\theta = \llbracket \mu E_1 \rrbracket \eta$ . Then for any action  $a$ , and any  $d, d'$  and  $e$ , we have  $(d, d', e) \in \theta(Y_a^{M,S})$  if and only if*

$$\exists d_2, d_3. d' \Rightarrow_S d_2 \wedge d_2 \xrightarrow{a(f_a^M(d,e))}_S d_3 \wedge (d, d_2) \in \eta(X^{M,S}) \wedge (g_a^M(d, e), d_3) \in \eta(X^{M,S})$$

*Proof.* We drop the superscripts  $M, S$  when no confusion arises. We define sets  $\mathcal{R}_i^{a,d,e} \subseteq D^S$ , for any  $a \in Act$ ,  $d, e, i \geq 0$ , and depending on  $\eta(X)$ , as follows:

$$\begin{cases} \mathcal{R}_0^{a,d,e} = \{d' \mid \exists d_3. d' \xrightarrow{a(f_a^M(d,e))}_S d_3 \wedge (d, d') \in \eta(X) \wedge (g_a^M(d, e), d_3) \in \eta(X)\} \\ \mathcal{R}_{i+1}^{a,d,e} = \{d' \mid \exists d_2. d' \xrightarrow{\tau}_S d_2 \wedge d_2 \in \mathcal{R}_i^{a,d,e}\} \end{cases}$$

And let  $\mathcal{R}^{a,d,e} = \bigcup_{i \geq 0} \mathcal{R}_i^{a,d,e}$ . Obviously, by definition of  $\Rightarrow$ , we have

$$\begin{aligned} \mathcal{R}^{a,d,e} = \{d' \mid \exists d_2, d_3. d' \Rightarrow_S d_2 \wedge d_2 \xrightarrow{a(f_a^M(d,e))}_S d_3 \wedge (d, d_2) \in \eta(X) \\ \wedge (g_a^M(d, e), d_3) \in \eta(X)\} \end{aligned}$$

We will prove, using an approximation method, that this coincides with the minimal solution of  $Y_a^{M,S}$ . More precisely, we claim:

$$((d, d', e) \in \theta(Y_a^{M,S})) = (d' \in \mathcal{R}^{a,d,e})$$

Recall that according to the algorithm,  $Y_a$  is of the form

$$Y_a(d, d', e) = (X(d, d') \wedge \Xi) \vee \exists e'_\tau. (h_\tau^S(d', e'_\tau) \wedge Y_a(d, g_\tau^S(d', e'_\tau), e)) \quad (1)$$

where  $\Xi$  (generated by function *step*) is of the form

$$\begin{aligned} (a = \tau \wedge X(g_\tau^M(d, e), d')) \vee \\ \exists e'_a. h_a^S(d', e'_a) \wedge (f_a^M(d, e) = f_a^S(d', e'_a)) \wedge X(g_a^M(d, e), g_a^S(d', e'_a)) \end{aligned}$$

Note that, using the operational semantics for LPE  $S$ ,

$$\llbracket X(d, d') \wedge \Xi \rrbracket \eta = \exists d''. (d, d') \in \eta(X) \wedge (g_a^M(d, e), d'') \in \eta(X) \wedge d' \xrightarrow{a(f_a^M(d,e))}_S d''$$

Hence,

$$\llbracket X(d, d') \wedge \Xi \rrbracket \eta = (d' \in \mathcal{R}_0^{a,d,e}) \quad (2)$$

We next show by induction on  $n$ , that the finite approximations  $Y_a^n(d, d', e)$  of equation (1) can be characterized by the following equation:

$$Y_a^n(d, d', e) = (d' \in \bigcup_{0 \leq i < n} \mathcal{R}_i^{a,d,e})$$

The basis is trivial ( $Y_a = \emptyset$ ). For the induction step, it suffices to note that

$$\begin{aligned} & \{d' \mid Y_a^{n+1}(d, d', e)\} \\ & \stackrel{*}{=} \{d' \mid ((d, d') \in \eta(X) \wedge \llbracket \Xi \rrbracket \eta) \vee \exists e'_\tau. (h_\tau^S(d', e'_\tau) \wedge g_\tau^S(d', e'_\tau) \in \bigcup_{0 \leq i < n} \mathcal{R}_i^{a,d,e})\} \\ & = \{d' \mid (d, d') \in \eta(X) \wedge \llbracket \Xi \rrbracket \eta\} \cup \bigcup_{0 \leq i < n} \{d' \mid \exists e'_\tau. (h_\tau^S(d', e'_\tau) \wedge g_\tau^S(d', e'_\tau) \in \mathcal{R}_i^{a,d,e})\} \\ & \stackrel{\star}{=} \mathcal{R}_0^{a,d,e} \cup \bigcup_{0 \leq i < n} \mathcal{R}_{i+1}^{a,d,e} \\ & = \bigcup_{0 \leq i < n+1} \mathcal{R}_i^{a,d,e}, \end{aligned}$$

where the step (\*) uses the induction hypothesis, and the step (★) uses equation (2) above, and the definition of  $\mathcal{R}_i^{a,d,e}$ .

Next we compute the first infinitary approximation  $Y_a^\omega$  of equation (1):

$$\begin{aligned} \{d' \mid Y_a^\omega(d, d', e)\} &= \bigcup_{n \geq 0} \{d' \mid Y_a^n(d, d', e)\} \\ &= \bigcup_{n \geq 0} \bigcup_{0 \leq i < n} \mathcal{R}_i^{a,d,e} \\ &= \bigcup_{i \geq 0} \mathcal{R}_i^{a,d,e} \end{aligned}$$

It remains to show that the solution is stable, i.e.  $Y^\omega$  is a solution of equation (1). This can be readily checked as follows:

$$\begin{aligned} & \{d' \mid ((d, d') \in \eta(X) \wedge \llbracket \Xi \rrbracket \eta) \vee \exists e'_\tau. (h_\tau^S(d', e'_\tau) \wedge g_\tau^M(d', e'_\tau) \in \mathcal{R}^{a,d,e})\} \\ &= \mathcal{R}_0 \cup \bigcup_{i \geq 1} \mathcal{R}_i^{a,d,e} \\ &= \mathcal{R}^{a,d,e} \end{aligned}$$

Hence we have found the correct minimal solution of  $\mu E_1$ . □

Finally, the correctness of the algorithm follows from the following theorem.

**Theorem 2.** *Let  $\nu E_2 \mu E_1$  be the equation system generated by Algorithm 1 on  $M$  and  $S$  and  $\theta = \llbracket \nu E_2 \mu E_1 \rrbracket$ . Then for all  $d$  and  $d'$  we have  $M(d) \leftrightarrow_b S(d')$  if and only if  $(d, d') \in \theta(X^{M,S})$ .*

*Proof.* Recall that according to the algorithm,  $X^{M,S}$  is of the form

$$\begin{aligned} X^{M,S}(d, d') &= \bigwedge_{a \in Act} \forall e_a. (h_a^M(d, e_a) \implies Y_a^{M,S}(d, d', e_a)) \\ &\quad \wedge \bigwedge_{a \in Act} \forall e'_a. (h_a^S(d', e'_a) \implies Y_a^{S,M}(d', d, e'_a)) \end{aligned}$$

By symmetry, w.l.o.g. we only consider  $\bigwedge_{a \in Act} \forall e_a. (h_a^M(d, e_a) \implies Y_a^{M,S}(d, d', e_a))$ .  
We define  $G : D^M \times D^S \rightarrow D^M \times D^S$  as

$$G(\mathcal{B}) = \{(d, d') \mid \bigwedge_{a \in Act} \forall e_a. (h_a^M(d, e_a) \implies (d, d', e_a) \in \eta(Y_a^{M,S}))\}$$

where  $\eta = \llbracket \mu E_1 \rrbracket [\mathcal{B} / X^{M,S}]$ .

Note that by [17, Lemma 5],  $G$  is monotonic, and thus the maximal fixpoint of  $G$  exists which is denoted by  $\nu B.G(B)$ . According to the semantics of PBES (cf. Definition 9), we have

$$\nu B.G(B) = \{(d, d') \mid (d, d') \in \theta(X^{M,S})\}$$

Recall that the functional  $\mathcal{F}$  is defined as

$$\begin{aligned} \mathcal{F}(\mathcal{B}) &= \{(d, d') \mid \forall a \in Act, e_a \in E_a. h_a^M(d, e_a) \implies \\ &\quad \exists d_2, d_3. d' \Rightarrow d_2 \wedge d_2 \xrightarrow{\overline{a(f_a^M(d, e_a))}}_S d_3 \wedge (d, d_2) \in \mathcal{B} \wedge (g_a^M(d, e_a), d_3) \in \mathcal{B}\} \end{aligned}$$

We claim that for any  $\mathcal{B}$ ,

$$\mathcal{F}(\mathcal{B}) = G(\mathcal{B})$$

To see this, first let us note that by Theorem 1

$$\eta(Y_a^{M,S}) = \{d' \mid \exists d_2, d_3. d' \Rightarrow d_2 \wedge d_2 \xrightarrow{\overline{a(f_a^M(d, e))}}_S d_3 \wedge \mathcal{B}(d, d_2) \wedge \mathcal{B}(g_a^M(d, e), d_3)\}$$

It follows that

$$\begin{aligned} G(\mathcal{B}) &= \{(d, d') \mid \bigwedge_{a \in Act} \forall e_a. (h_a^M(d, e_a) \implies (d, d', e_a) \in \eta(Y_a^{M,S}))\} \\ &= \{(d, d') \mid \bigwedge_{a \in Act} \forall e_a. (h_a^M(d, e_a) \implies \exists d_2, d_3. d' \Rightarrow d_2 \wedge d_2 \xrightarrow{\overline{a(f_a^M(d, e))}}_S d_3 \wedge \\ &\quad \mathcal{B}(d, d_2) \wedge \mathcal{B}(g_a^M(d, e), d_3))\} \\ &= \mathcal{F}(\mathcal{B}) \end{aligned}$$

It follows from Lemma 1 that

$$\Leftrightarrow_b = \nu \mathcal{F} = \nu B.G(B) = \{(d, d') \mid (d, d') \in \theta(X^{M,S})\}$$

from which it is not difficult to see that  $(d, d') \in \theta(X)$  if and only if  $M(d) \Leftrightarrow_b S(d')$ .  $\square$

## 5 Examples

In this section we demonstrate the potential of the technique outlined in the previous section by applying it to two examples. To compute the solutions to the resulting PBESs, we strongly rely on techniques for solving and manipulating PBESs like adding invariants, symbolic approximations and strengthening equations. For a detailed account of these techniques, we refer to [17].

*Data sorts.* Let  $D$  be an arbitrary data sort (possibly infinite sized) which is equipped with an equality relation, and let  $\mathcal{Q}$  denote the data sort of queues over  $D$  with infinite capacity. We use list enumeration to denote queues containing specific elements, e.g.  $[]$  and  $[d, e]$  denote the empty queue and the queue containing  $d$  and  $e$  for any  $d, e \in D$ , respectively. Operations on queues include  $q \# q'$ , denoting the natural concatenation of queues  $q$  and  $q'$ ,  $|q|$  denoting the length of queue  $q$  and functions  $hd : \mathcal{Q} \rightarrow D$  and  $tl : \mathcal{Q} \rightarrow \mathcal{Q}$  which yield the head and tail of a queue, respectively.

### 5.1 Two Buffers and a Queue

In this example, we show that two one-place buffers in sequence behave branching bisimilar to a queue of capacity two. The behavior of the buffers is given by the LPE  $B$  and that of the queue by the LPE  $Q$ . Processes  $B$  and  $Q$  can communicate with their environments via parameterized actions  $r(d)$  (read  $d$  from the environment) and  $s(d)$  (write  $d$  to the environment). The  $\tau$  actions represent the internal communication of data from one buffer to the next.

$$\begin{aligned} B(b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D) = & \\ & \sum_{d:D} \neg b_1 \implies r(d) \cdot B(\top, d, b_2, d_2) \\ & + b_1 \wedge \neg b_2 \implies \tau \cdot B(\perp, d_1, \top, d_1) \\ & + b_2 \implies s(d_2) \cdot B(b_1, d_1, \perp, d_2) \end{aligned}$$

$$\begin{aligned} Q(q : \mathcal{Q}) = & \\ & \sum_{d:D} |q| < 2 \implies r(d) \cdot Q([d] \# q) \\ & + |q| > 0 \implies s(hd(q)) \cdot Q(tl(q)) \end{aligned}$$

To check whether these processes are branching bisimilar, they are translated to the following PBES using Algorithm 1:

$$\begin{aligned}
\nu X^{B,Q}(b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D, q : \mathcal{Q}) = & \\
& (\neg b_1 \implies \forall d : D . Y_r^{B,Q}(b_1, d_1, b_2, d_2, q, d)) \wedge \\
& ((b_1 \wedge \neg b_2) \implies Y_r^{B,Q}(b_1, d_1, b_2, d_2, q)) \wedge \\
& (b_2 \implies Y_s^{B,Q}(b_1, d_1, b_2, d_2, q)) \wedge \\
& (|q| < 2 \implies \forall d : D . Y_r^{Q,B}(q, b_1, d_1, b_2, d_2, d)) \wedge \\
& (|q| > 0 \implies Y_s^{Q,B}(q, b_1, d_1, b_2, d_2)) \\
\nu X^{Q,B}(q : \mathcal{Q}, b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D) = & X^{B,Q}(b_1, d_1, b_2, d_2, q) \\
\mu Y_r^{B,Q}(b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D, q : \mathcal{Q}, e : D) = & \\
& X^{B,Q}(b_1, d_1, b_2, d_2, q) \wedge |q| < 2 \wedge X^{B,Q}(\top, e, b_2, d_2, [e] \# q) \\
\mu Y_s^{B,Q}(b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D, q : \mathcal{Q}) = & \\
& X^{B,Q}(b_1, d_1, b_2, d_2, q) \wedge |q| > 0 \wedge d_2 = hd(q) \wedge X^{B,Q}(b_1, d_1, \perp, d_2, tl(q)) \\
\mu Y_r^{Q,B}(b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D, q : \mathcal{Q}) = & \\
& X^{B,Q}(b_1, d_1, b_2, d_2, q) \wedge X^{B,Q}(\perp, d_1, \top, d_1, q) \\
\mu Y_r^{Q,B}(q : \mathcal{Q}, b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D, e : D) = & \\
& (b_1 \wedge \neg b_2 \wedge Y_r^{Q,B}(q, \perp, d_1, \top, d_1, e)) \vee \\
& (X^{Q,B}(q, b_1, d_1, b_2, d_2) \wedge \neg b_1 \wedge X^{Q,B}([e] \# q, \top, e, b_2, d_2)) \\
\mu Y_s^{Q,B}(q : \mathcal{Q}, b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D) = & \\
& (b_1 \wedge \neg b_2 \wedge Y_s^{Q,B}(q, \perp, d_1, \top, d_1)) \vee \\
& (X^{Q,B}(q, b_1, d_1, b_2, d_2) \wedge b_2 \wedge hd(q) = d_2 \wedge X^{Q,B}(tl(q), b_1, d_1, \perp, d_2))
\end{aligned}$$

We first solve the equations for  $Y_r^{Q,B}$  and  $Y_s^{Q,B}$  by approximation:

$$\begin{aligned}
Y_{r,0}^{Q,B}(q : \mathcal{Q}, b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D, e : D) &= \perp \\
Y_{r,1}^{Q,B}(q : \mathcal{Q}, b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D, e : D) &= \\
&X^{Q,B}(q, b_1, d_1, b_2, d_2) \wedge \neg b_1 \wedge X^{Q,B}([e] \# q, \top, e, b_2, d_2) \\
Y_{r,2}^{Q,B}(q : \mathcal{Q}, b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D, e : D) &= \\
&(b_1 \wedge \neg b_2 \wedge X^{Q,B}(q, \perp, d_1, \top, d_1) \wedge X^{Q,B}([e] \# q, \top, e, \top, d_1)) \vee \\
&(X^{Q,B}(q, b_1, d_1, b_2, d_2) \wedge \neg b_1 \wedge X^{Q,B}([e] \# q, \top, e, b_2, d_2)) \\
Y_{r,3}^{Q,B}(q : \mathcal{Q}, b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D, e : D) &= \\
&(b_1 \wedge \neg b_2 \wedge X^{Q,B}(q, \perp, d_1, \top, d_1) \wedge X^{Q,B}([e] \# q, \top, e, \top, d_1)) \vee \\
&(X^{Q,B}(q, b_1, d_1, b_2, d_2) \wedge \neg b_1 \wedge X^{Q,B}([e] \# q, \top, e, b_2, d_2)) \\
\\
Y_{s,0}^{Q,B}(q : \mathcal{Q}, b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D) &= \perp \\
Y_{s,1}^{Q,B}(q : \mathcal{Q}, b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D) &= \\
&X^{Q,B}(q, b_1, d_1, b_2, d_2) \wedge b_2 \wedge hd(q) = d_2 \wedge X^{Q,B}(tl(q), b_1, d_1, \perp, d_2) \\
Y_{s,2}^{Q,B}(q : \mathcal{Q}, b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D) &= \\
&(b_1 \wedge \neg b_2 \wedge X^{Q,B}(q, \perp, d_1, \top, d_1) \wedge hd(q) = d_1 \wedge X^{Q,B}(tl(q), \perp, d_1, \perp, d_2)) \\
&\vee (X^{Q,B}(q, b_1, d_1, b_2, d_2) \wedge b_2 \wedge hd(q) = d_2 \wedge X^{Q,B}(tl(q), b_1, d_1, \perp, d_2)) \\
Y_{s,3}^{Q,B}(q : \mathcal{Q}, b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D) &= \\
&(b_1 \wedge \neg b_2 \wedge X^{Q,B}(q, \perp, d_1, \top, d_1) \wedge hd(q) = d_1 \wedge X^{Q,B}(tl(q), \perp, d_1, \perp, d_2)) \\
&\vee (X^{Q,B}(q, b_1, d_1, b_2, d_2) \wedge b_2 \wedge hd(q) = d_2 \wedge X^{Q,B}(tl(q), b_1, d_1, \perp, d_2))
\end{aligned}$$

The solutions to  $X^{Q,B}$ ,  $Y_r^{B,Q}$ ,  $Y_s^{B,Q}$  and  $Y_r^{B,Q}$  are trivial. We substitute every solution in the first equation to obtain the following equation for  $X^{B,Q}$ :

$$\begin{aligned}
\nu X^{B,Q}(b_1 : \mathbb{B}, d_1 : D, b_2 : \mathbb{B}, d_2 : D, q : \mathcal{Q}) = & \\
& (\neg b_1 \implies (X^{B,Q}(b_1, d_1, b_2, d_2, q) \wedge |q| < 2 \\
& \quad \wedge \forall d \in D . X^{B,Q}(\top, d, b_2, d_2, [d] \# q))) \\
& \wedge ((b_1 \wedge \neg b_2) \implies (X^{B,Q}(b_1, d_1, b_2, d_2, q) \wedge X^{B,Q}(\perp, d_1, \top, d_1, q))) \\
& \wedge (b_2 \implies (X^{B,Q}(b_1, d_1, b_2, d_2, q) \wedge |q| > 0 \wedge d_2 = hd(q) \\
& \quad \wedge X^{B,Q}(b_1, d_1, \perp, d_2, tl(q)))) \\
& \wedge (|q| < 2 \implies \\
& \quad \forall d \in D . ((b_1 \wedge \neg b_2 \wedge X^{B,Q}(\perp, d_1, \top, d_1, q) \wedge X^{B,Q}(\top, d, \top, d_1, [d] \# q)) \\
& \quad \vee (X^{B,Q}(b_1, d_1, b_2, d_2, q) \wedge \neg b_1 \wedge X^{B,Q}(\top, d, b_2, d_2, [d] \# q)))) \\
& \wedge (|q| > 0 \implies \\
& \quad ((b_1 \wedge \neg b_2 \wedge X^{B,Q}(\perp, d_1, \top, d_1, q) \wedge hd(q) = d_1 \wedge X^{B,Q}(\perp, d_1, \perp, d_2, tl(q))) \\
& \quad \vee (X^{B,Q}(b_1, d_1, b_2, d_2, q) \wedge b_2 \wedge hd(q) = d_2 \wedge X^{B,Q}(b_1, d_1, \perp, d_2, tl(q))))))
\end{aligned}$$

To solve this equation we *instantiate* the boolean parameters  $b_1$  and  $b_2$ . Instantiation is a technique in which an equation  $\sigma X(d:D, e:E) = \phi$  with  $D = \{d_1, \dots, d_n\}$  is replaced by  $n$  equations  $(\sigma X_{d_1}(e:E) = \phi[d_1/d]) \cdots (\sigma X_{d_n}(e:E) = \phi[d_n/d])$  where occurrences of  $X(d_i, \dots)$  in the righthand sides are replaced by  $X_{d_i}(\dots)$ . Instantiation can be done on multiple parameters. The technique is described more formally and proven correct in [8]. We obtain the following four equations when instantiating  $b_1$  and  $b_2$ :

$$\begin{aligned}
\nu X_{\top, \top}(d_1 : \mathbb{B}, d_2 : D, q : \mathcal{Q}) = & \\
& X_{\top, \top}(d_1, d_2, q) \wedge |q| \geq 2 \wedge hd(q) = d_2 \wedge X_{\top, \perp}(d_1, d_2, tl(q)) \\
\nu X_{\top, \perp}(d_1 : \mathbb{B}, d_2 : D, q : \mathcal{Q}) = & \\
& X_{\top, \perp}(d_1, d_2, q) \wedge X_{\perp, \top}(d_1, d_1, q) \wedge (|q| < 2 \implies \forall d \in D . X_{\top, \top}(d, d_1, [d] \# q)) \wedge \\
& (|q| > 0 \implies hd(q) = d_1 \wedge X_{\perp, \perp}(d_1, d_2, tl(q))) \\
\nu X_{\perp, \top}(d_1 : \mathbb{B}, d_2 : D, q : \mathcal{Q}) = & \\
& X_{\perp, \top}(d_1, d_2, q) \wedge q = [d_2] \wedge (\forall d \in D . X_{\top, \top}(d, d_2, [d] \# q)) \wedge X_{\perp, \perp}(d_1, d_2, tl(q)) \\
\nu X_{\perp, \perp}(d_1 : \mathbb{B}, d_2 : D, q : \mathcal{Q}) = & \\
& X_{\perp, \perp}(d_1, d_2, q) \wedge |q| = 0 \wedge (\forall d \in D . X_{\top, \perp}(d, d_2, [d] \# q))
\end{aligned}$$

Note that in every equation for  $X_{x,y}$  we can safely omit the conjunct  $X_{x,y}(d_1, d_2, q)$ . By substituting the equations for  $X_{\perp, \top}$ ,  $X_{\perp, \perp}$  and  $X_{\top, \top}$  (in that order) in the equation for  $X_{\top, \perp}$ , we obtain for  $X_{\top, \perp}$ :

$$\nu X_{\top, \perp}(d_1 : D, d_2 : D, q : \mathcal{Q}) = q = [d_1] \wedge (\forall d \in D . X_{\top, \perp}(d, d_2, [d]))$$

By approximation we find that the solution to  $X_{\top, \perp}$  is  $q = [d_1]$ . Substituting this solution in the other equations gives us the solutions to all  $X_{x,y}$ :

$$\nu X_{\top, \top}(d_1 : D, d_2 : D, q : \mathcal{Q}) = q = [d_1, d_2]$$

$$\nu X_{\top, \perp}(d_1 : D, d_2 : D, q : \mathcal{Q}) = q = [d_1]$$

$$\nu X_{\perp, \top}(d_1 : D, d_2 : D, q : \mathcal{Q}) = q = [d_2]$$

$$\nu X_{\perp, \perp}(d_1 : D, d_2 : D, q : \mathcal{Q}) = q = []$$

Evaluating  $X^{B,Q}$  for the initial state  $(\perp, d, \perp, e, [])$  for any  $d, e \in D$ , amounts to evaluating  $X_{\perp, \perp}$  for  $(d, e, [])$  which yields *true*. Hence, processes  $B$  and  $Q$  are branching bisimilar.

## 5.2 Unbounded Queues

The capacity of a bounded queue is doubled by connecting a queue of the same size, which means that a composition of bounded queues is behaviorally different from the constituent queues. In this respect, a composition of queues with infinite capacity does not change the behavior, as this again yields an unbounded queue.

The processes  $S$  and  $T$  defined below model the composition of two unbounded queues and three unbounded queues, respectively. Remark that we obtained LPEs  $S$  and  $T$  as a result of an automated linearization of the parallel composition of two (resp. three) queues of infinite capacity. These original specifications have been omitted for brevity. Processes  $S$  and  $T$  can communicate with their environments via parameterized actions  $r(d)$  (read  $d$  from the environment) and  $w(d)$  (write  $d$  to the environment). The  $\tau$  actions represent the internal communication of data from one queue to the next.

$$\begin{aligned} S(s_0, s_1 : \mathcal{Q}) = & \\ & \sum_{v:D} s_1 \neq [] \implies r(v) \cdot S([v] \uplus s_0, s_1) \\ & + w(\text{hd}(s_1)) \cdot S(s_0, \text{tl}(s_1)) \\ & + s_0 \neq [] \implies \tau \cdot S(\text{tl}(s_0), [\text{hd}(s_0)] \uplus s_1) \end{aligned}$$

$$\begin{aligned} T(t_0, t_1, t_2 : \mathcal{Q}) = & \\ & \sum_{u:D} r(u) \cdot T([u] \uplus t_0, t_1, t_2) \\ & + t_2 \neq [] \implies w(\text{hd}(t_2)) \cdot T(t_0, t_1, \text{tl}(t_2)) \\ & + t_0 \neq [] \implies \tau \cdot T(\text{tl}(t_0), [\text{hd}(t_0)] \uplus t_1, t_2) \\ & + t_1 \neq [] \implies \tau \cdot T(t_0, \text{tl}(t_1), [\text{hd}(t_1)] \uplus t_2) \end{aligned}$$



By applying Algorithm 1 for processes  $S$  and  $T$ , we obtain the following PBES:

$$\begin{aligned}
& (\nu X^{S,T}(s_0, s_1, t_0, t_1, t_2 : \mathcal{Q}) = \\
& \quad (\forall v : D. Y_r^{S,T}(s_0, s_1, t_0, t_1, t_2, v)) \wedge (s_1 \neq [] \implies Y_w^{S,T}(s_0, s_1, t_0, t_1, t_2)) \\
& \quad \wedge (s_0 \neq [] \implies Y_\tau^{S,T}(s_0, s_1, t_0, t_1, t_2)) \wedge \\
& \quad (\forall u : D. Y_r^{T,S}(t_0, t_1, t_2, s_0, s_1, u)) \wedge (t_2 \neq [] \implies Y_w^{T,S}(t_0, t_1, t_2, s_0, s_1)) \\
& \quad \wedge ((t_1 \neq [] \vee t_0 \neq [])) \implies Y_\tau^{T,S}(t_0, t_1, t_2, s_0, s_1))) \\
& (\nu X^{T,S}(t_0, t_1, t_2, s_0, s_1 : \mathcal{Q}) = X^{S,T}(s_0, s_1, t_0, t_1, t_2)) \\
& (\mu Y_r^{S,T}(s_0, s_1, t_0, t_1, t_2 : \mathcal{Q}, v : D) = \\
& \quad (t_0 \neq [] \wedge Y_r^{S,T}(s_0, s_1, tl(t_0), [hd(t_0)] ++ t_1, t_2, v)) \vee \\
& \quad (t_1 \neq [] \wedge Y_r^{S,T}(s_0, s_1, t_0, tl(t_1), [hd(t_1)] ++ t_2, v)) \vee \\
& \quad (X^{S,T}(s_0, s_1, t_0, t_1, t_2) \wedge X^{S,T}([v] ++ s_0, s_1, [v] ++ t_0, t_1, t_2))) \\
& (\mu Y_w^{S,T}(s_0, s_1, t_0, t_1, t_2 : \mathcal{Q}) = \\
& \quad (t_0 \neq [] \wedge Y_w^{S,T}(s_0, s_1, tl(t_0), [hd(t_0)] ++ t_1, t_2)) \vee \\
& \quad (t_1 \neq [] \wedge Y_w^{S,T}(s_0, s_1, t_0, tl(t_1), [hd(t_1)] ++ t_2)) \vee \\
& \quad (X^{S,T}(s_0, s_1, t_0, t_1, t_2) \wedge t_2 \neq [] \wedge hd(t_2) = hd(s_1) \\
& \quad \wedge X^{S,T}(s_0, tl(s_1), t_0, t_1, tl(t_2)))) \\
& (\mu Y_\tau^{S,T}(s_0, s_1, t_0, t_1, t_2 : \mathcal{Q}) = \\
& \quad (t_0 \neq [] \wedge Y_\tau^{S,T}(s_0, s_1, tl(t_0), [hd(t_0)] ++ t_1, t_2)) \vee \\
& \quad (t_1 \neq [] \wedge Y_\tau^{S,T}(s_0, s_1, t_0, tl(t_1), [hd(t_1)] ++ t_2)) \vee \\
& \quad (X^{S,T}(s_0, s_1, t_0, t_1, t_2) \wedge (X^{S,T}(tl(s_0), [hd(s_0)] ++ s_1, t_0, t_1, t_2) \vee \\
& \quad (t_0 \neq [] \wedge X^{S,T}(tl(s_0), [hd(s_0)] ++ s_1, tl(t_0), [hd(t_0)] ++ t_1, t_2)) \vee \\
& \quad (t_1 \neq [] \wedge X^{S,T}(tl(s_0), [hd(s_0)] ++ s_1, t_0, tl(t_1), [hd(t_1)] ++ t_2)))))) \\
& (\mu Y_r^{T,S}(t_0, t_1, t_2, s_0, s_1 : \mathcal{Q}, u : D) = \\
& \quad (s_0 \neq [] \wedge Y_r^{T,S}(t_0, t_1, t_2, tl(s_0), [hd(s_0)] ++ s_1, u)) \vee \\
& \quad (X^{T,S}(t_0, t_1, t_2, s_0, s_1) \wedge X^{T,S}([u] ++ t_0, t_1, t_2, [u] ++ s_0, s_1))) \\
& (\mu Y_w^{T,S}(t_0, t_1, t_2, s_0, s_1 : \mathcal{Q}) = \\
& \quad (s_0 \neq [] \wedge Y_w^{T,S}(t_0, t_1, t_2, tl(s_0), [hd(s_0)] ++ s_1)) \vee \\
& \quad (X^{T,S}(t_0, t_1, t_2, s_0, s_1) \wedge s_1 \neq [] \wedge hd(s_1) = hd(t_2) \wedge \\
& \quad X^{T,S}(t_0, t_1, tl(t_2), s_0, tl(s_1)))) \\
& (\mu Y_\tau^{T,S}(t_0, t_1, t_2, s_0, s_1 : \mathcal{Q}) = \\
& \quad (s_0 \neq [] \wedge Y_\tau^{T,S}(t_0, t_1, t_2, tl(s_0), [hd(s_0)] ++ s_1)) \vee \\
& \quad (X^{T,S}(t_0, t_1, t_2, s_0, s_1) \wedge \\
& \quad (X^{T,S}(tl(t_0), [hd(t_0)] ++ t_1, t_2, s_0, s_1) \vee X^{T,S}(t_0, tl(t_1), [hd(t_1)] ++ t_2, s_0, s_1) \\
& \quad \vee (s_0 \neq [] \wedge (X^{T,S}(tl(t_0), [hd(t_0)] ++ t_1, t_2, tl(s_0), [hd(s_0)] ++ s_1) \\
& \quad \vee X^{T,S}(t_0, tl(t_1), [hd(t_1)] ++ t_2, tl(s_0), [hd(s_0)] ++ s_1))))))
\end{aligned}$$

Consider the equation for  $Y_w^{S,T}$ . It represents the case where process  $T$  has to simulate a  $w(hd(s_1))$  action of process  $S$  by possibly executing a finite number of  $\tau$ -steps before executing action  $w(hd(t_2))$ . Inspired by the scenario that captures the minimal amount of  $\tau$ -steps that are needed (two steps when  $t_1 = [] \wedge t_2 = []$ , one when  $t_1 \neq [] \wedge t_2 = []$  and none otherwise), we strengthen the equation for  $Y_w^{S,T}$  as follows:

$$\begin{aligned} \mu Y_w^{S,T}(s_0, s_1, t_0, t_1, t_2 : \mathcal{Q}) = & \quad (3) \\ & (t_0 \neq [] \wedge \underline{t_1 = [] \wedge t_2 = []} \wedge Y_w^{S,T}(s_0, s_1, tl(t_0), [hd(t_0)] \# t_1, t_2)) \vee \\ & (t_1 \neq [] \wedge \underline{t_2 = []} \wedge Y_w^{S,T}(s_0, s_1, t_0, tl(t_1), [hd(t_1)] \# t_2)) \vee \\ & (t_2 \neq [] \wedge hd(t_2) = hd(s_1) \wedge X^{S,T}(s_0, s_1, t_0, t_1, t_2) \\ & \wedge X^{S,T}(s_0, tl(s_1), t_0, t_1, tl(t_2))) \end{aligned}$$

The solution to this equation is at most as large as the solution to the original equation. Therefore, if the solution to the strengthened PBES yields *true* on the initial state, then the solution to the original PBES would have done so as well, thereby justifying our modification. We approximate the solution to equation (3) as follows:

$$\begin{aligned} Y_{w,0}^{S,T}(s_0, s_1, t_0, t_1, t_2 : \mathcal{Q}) &= \perp \\ Y_{w,1}^{S,T}(s_0, s_1, t_0, t_1, t_2 : \mathcal{Q}) &= \\ & t_2 \neq [] \wedge hd(t_2) = hd(s_1) \wedge X^{S,T}(s_0, s_1, t_0, t_1, t_2) \\ & \wedge X^{S,T}(s_0, tl(s_1), t_0, t_1, tl(t_2)) \\ Y_{w,2}^{S,T}(s_0, s_1, t_0, t_1, t_2 : \mathcal{Q}) &= \\ & (t_1 \neq [] \wedge t_2 = [] \wedge hd(t_1) = hd(s_1) \wedge X^{S,T}(s_0, s_1, t_0, tl(t_1), [hd(t_1)]) \\ & \wedge X^{S,T}(s_0, tl(s_1), t_0, tl(t_1), [])) \vee \\ & (t_2 \neq [] \wedge hd(t_2) = hd(s_1) \wedge X^{S,T}(s_0, s_1, t_0, t_1, t_2) \\ & \wedge X^{S,T}(s_0, tl(s_1), t_0, t_1, tl(t_2))) \\ Y_{w,3}^{S,T}(s_0, s_1, t_0, t_1, t_2 : \mathcal{Q}) &= \\ & (t_0 \neq [] \wedge t_1 = [] \wedge t_2 = [] \wedge hd(t_0) = hd(s_1) \\ & \wedge X^{S,T}(s_0, s_1, tl(t_0), [], [hd(t_0)]) \wedge X(s_0, tl(s_1), tl(t_0), [], [])) \vee \\ & (t_1 \neq [] \wedge t_2 = [] \wedge hd(t_1) = hd(s_1) \wedge X^{S,T}(s_0, s_1, t_0, tl(t_1), [hd(t_1)]) \\ & \wedge X^{S,T}(s_0, tl(s_1), t_0, tl(t_1), [])) \vee \\ & (t_2 \neq [] \wedge hd(t_2) = hd(s_1) \wedge X^{S,T}(s_0, s_1, t_0, t_1, t_2) \\ & \wedge X^{S,T}(s_0, tl(s_1), t_0, t_1, tl(t_2))) \\ Y_{w,4}^{S,T}(s_0, s_1, t_0, t_1, t_2 : \mathcal{Q}) &= Y_{w,3}^{S,T}(s_0, s_1, t_0, t_1, t_2) \end{aligned}$$

Because  $Y_{w,4}^{S,T} = Y_{w,3}^{S,T}$ , the solution to equation (3) is  $Y_{w,3}^{S,T}$ . In a similar way, we obtain a solution for  $Y_w^{T,S}$  by strengthening the first disjunct. Regarding the equations

for the  $Y_\tau$ s and  $Y_r$ s, we note that the mimicking of a  $\tau$  step of one process by the other can be postponed. This means that we can strengthen each of the equations for the  $Y_\tau$ s and  $Y_r$ s by removing all but the last disjunct.

For every predicate variable except  $X^{S,T}$ , we have now obtained an equation in which that variable does not occur in the right-hand side. These solutions can be substituted in the equation for  $X^{S,T}$  without affecting its solution, yielding the following closed equation for  $X^{S,T}$ :

$$\begin{aligned}
\nu X^{S,T}(s_0, s_1, t_0, t_1, t_2 : \mathcal{Q}) = & \\
& X^{S,T}(s_0, s_1, t_0, t_1, t_2) \wedge (\forall v : D . X([v] \# s_0, s_1, [v] \# t_0, t_1, t_2)) \\
& \wedge (s_1 \neq [] \implies \\
& \quad ((t_0 \neq [] \wedge t_1 = [] \wedge t_2 = [] \wedge hd(t_0) = hd(s_1) \wedge \\
& \quad \quad X^{S,T}(s_0, s_1, tl(t_0), [], [hd(t_0)]) \wedge X(s_0, tl(s_1), tl(t_0), [], [])) \\
& \quad \vee (t_1 \neq [] \wedge t_2 = [] \wedge hd(t_1) = hd(s_1) \wedge \\
& \quad \quad X^{S,T}(s_0, s_1, t_0, tl(t_1), [hd(t_1)]) \wedge X^{S,T}(s_0, tl(s_1), t_0, tl(t_1), [])) \\
& \quad \vee (t_2 \neq [] \wedge hd(t_2) = hd(s_1) \wedge X^{S,T}(s_0, s_1, t_0, t_1, t_2) \wedge \\
& \quad \quad X^{S,T}(s_0, tl(s_1), t_0, t_1, tl(t_2)))))) \\
& \wedge (s_0 \neq [] \implies (X(s_0, s_1, t_0, t_1, t_2) \wedge \\
& \quad (X(tl(s_0), [hd(s_0)] \# s_1, t_0, t_1, t_2) \\
& \quad \vee (t_0 \neq [] \wedge X(tl(s_0), [hd(s_0)] \# s_1, tl(t_0), [hd(t_0)] \# t_1, t_2)) \\
& \quad \vee (t_1 \neq [] \wedge X(tl(s_0), [hd(s_0)] \# s_1, t_0, tl(t_1), [hd(t_1)] \# t_2)))))) \\
& \wedge (t_2 \neq [] \implies \\
& \quad ((s_0 \neq [] \wedge s_1 = [] \wedge hd(s_0) = hd(t_2) \wedge \\
& \quad \quad X^{S,T}(tl(s_0), [hd(s_0)], t_0, t_1, t_2) \wedge X(tl(s_0), [], t_0, t_1, t_2)) \\
& \quad \vee (s_1 \neq [] \wedge hd(s_1) = hd(t_2) \wedge X^{S,T}(s_0, s_1, t_0, t_1, t_2) \wedge \\
& \quad \quad X^{S,T}(s_0, tl(s_1), t_0, t_1, tl(t_2)))))) \\
& \wedge ((t_0 \neq [] \vee t_1 \neq []) \implies (X(s_0, s_1, t_0, t_1, t_2) \wedge \\
& \quad (X(s_0, s_1, tl(t_0), [hd(t_0)] \# t_1, t_2) \vee X(s_0, s_1, t_0, tl(t_1), [hd(t_1)] \# t_2) \\
& \quad \vee (s_0 \neq [] \wedge (X(tl(s_0), [hd(s_0)] \# s_1, tl(t_0), [hd(t_0)] \# t_1, t_2) \vee \\
& \quad \quad X(tl(s_0), [hd(s_0)] \# s_1, t_0, tl(t_1), [hd(t_1)] \# t_2))))))
\end{aligned}$$

The formula  $s_0 \# s_1 = t_0 \# t_1 \# t_2$  can be shown to be an invariant for equation  $X^{S,T}$  (for a definition of invariant, see [17]). This implies that without restricting the solution for equation  $X^{S,T}$  for those values of  $s_0, s_1, t_0, t_1, t_2$  that satisfy the invariant, we can add the invariant to  $X^{S,T}$ :

$$\begin{aligned}
\nu X^{S,T}(s_0, s_1, t_0, t_1, t_2 : \mathcal{Q}) = & \\
& s_0 \# s_1 = t_0 \# t_1 \# t_2 \wedge X^{S,T}(s_0, s_1, t_0, t_1, t_2) \wedge \dots
\end{aligned}$$

The addition of the invariant  $s_0 \dot{+} s_1 = t_0 \dot{+} t_1 \dot{+} t_2$  accelerates and simplifies the approximation of  $X^{S,T}$ , which now stabilises at the third approximation:

$$\begin{aligned}
X_0^{S,T}(s_0, s_1, t_0, t_1, t_2 : Q) &= \top \\
X_1^{S,T}(s_0, s_1, t_0, t_1, t_2 : Q) &= \\
& s_0 \dot{+} s_1 = t_0 \dot{+} t_1 \dot{+} t_2 \\
& \wedge (s_1 \neq [] \implies \\
& \quad ((t_0 \neq [] \wedge t_1 = [] \wedge t_2 = [] \wedge hd(t_0) = hd(s_1)) \\
& \quad \vee (t_1 \neq [] \wedge t_2 = [] \wedge hd(t_1) = hd(s_1)) \vee (t_2 \neq [] \wedge hd(t_2) = hd(s_1))) \\
& \wedge (t_2 \neq [] \implies \\
& \quad ((s_0 \neq [] \wedge s_1 = [] \wedge hd(s_0) = hd(t_2)) \vee (s_1 \neq [] \wedge hd(s_1) = hd(t_2))) \\
& = s_0 \dot{+} s_1 = t_0 \dot{+} t_1 \dot{+} t_2 \\
X_2^{S,T}(s_0, s_1, t_0, t_1, t_2 : Q) &= \\
& s_0 \dot{+} s_1 = t_0 \dot{+} t_1 \dot{+} t_2 \wedge \forall v : D . ([v] \dot{+} s_0) \dot{+} s_1 = ([v] \dot{+} t_0) \dot{+} t_1 \dot{+} t_2 \\
& \wedge (s_1 \neq [] \implies \\
& \quad ((t_0 \neq [] \wedge t_1 = [] \wedge t_2 = [] \wedge s_0 \dot{+} s_1 = t_0 \wedge s_0 \dot{+} tl(s_1) = tl(t_0)) \\
& \quad \vee (t_1 \neq [] \wedge t_2 = [] \wedge s_0 \dot{+} s_1 = t_0 \dot{+} t_1 \wedge s_0 \dot{+} tl(s_1) = t_0 \dot{+} tl(t_1)) \\
& \quad \vee (t_2 \neq [] \wedge s_0 \dot{+} s_1 = t_0 \dot{+} t_1 \dot{+} t_2 \wedge s_0 \dot{+} tl(s_1) = t_0 \dot{+} t_1 \dot{+} tl(t_2))) \\
& \wedge (s_0 \neq [] \implies s_0 \dot{+} s_1 = t_0 \dot{+} t_1 \dot{+} t_2) \\
& \wedge (t_2 \neq [] \implies \\
& \quad ((s_0 \neq [] \wedge s_1 = [] \wedge s_0 = t_0 \dot{+} t_1 \dot{+} t_2 \wedge tl(s_0) = t_0 \dot{+} t_1 \dot{+} tl(t_2)) \\
& \quad \vee (s_1 \neq [] \wedge s_0 \dot{+} s_1 = t_0 \dot{+} t_1 \dot{+} t_2 \wedge s_0 \dot{+} tl(s_1) = t_0 \dot{+} t_1 \dot{+} tl(t_2))) \\
& \wedge ((t_0 \neq [] \vee t_1 \neq [])) \implies s_0 \dot{+} s_1 = t_0 \dot{+} t_1 \dot{+} t_2 \\
& = s_0 \dot{+} s_1 = t_0 \dot{+} t_1 \dot{+} t_2
\end{aligned}$$

Under assumption that the invariant holds, the solution to  $X^{S,T}$  is  $s_0 \dot{+} s_1 = t_0 \dot{+} t_1 \dot{+} t_2$ <sup>3</sup>. Evaluating the solution to  $X^{S,T}$  for the initial values of the parameters of  $S$  and  $T$ , we obtain  $[] \dot{+} [] = [] \dot{+} [] \dot{+} []$ , which clearly holds. This means that  $S([], [])$  and  $T([], [], [])$  are branching bisimilar. In fact, all processes  $S(s_0, s_1)$  and  $T(t_0, t_1, t_2)$  satisfying the condition  $s_0 \dot{+} s_1 = t_0 \dot{+} t_1 \dot{+} t_2$  are branching bisimilar.

## 6 Transformation for Other Equivalences

In this section, we demonstrate how we can adapt the algorithm presented in Section 4 to other variants of bisimulation. The strong case is simple and somehow known in [19] modulo different formalisms. For completeness, we include it as Algorithm 2. The cases for weak bisimulation and (branching) simulation equivalence are novel. They are presented as Algorithm 3 and Algorithm 4 respectively. The correctness proofs are similar to the one for branching bisimulation.

<sup>3</sup> Note that the fact that the solution and the invariant match is coincidental. For example, it is clear that the trivial invariant *true* ( $\top$ ) does not exhibit this phenomenon.

**Algorithm 2** Generation of a PBES for Strong Bisimulation*sbisim* =  $\nu E$ , **where**

$$E := \{ X^{M,S}(d : D^M, d' : D^S) = \text{match}^{M,S}(d, d') \wedge \text{match}^{S,M}(d', d) , \\ X^{S,M}(d' : D^S, d : D^M) = X^{M,S}(d, d') \}$$

Where we use the following abbreviations, for all  $a \in \text{Act} \wedge (p, q) \in \{(M, S), (S, M)\}$ :

$$\text{match}^{p,q}(d : D^p, d' : D^q) = \bigwedge_{a \in \text{Act}} \forall e : E_a^p. (h_a^p(d, e) \implies \text{step}_a^{p,q}(d, d', e)); \\ \text{step}_a^{p,q}(d : D^p, d' : D^q, e : E_a^p) = \\ \exists e' : E_a^q. h_a^q(d', e') \wedge (f_a^p(d, e) = f_a^q(d', e')) \wedge X^{p,q}(g_a^p(d, e), g_a^q(d', e'));$$

**Algorithm 3** Generation of a PBES for Weak Bisimulation*wbisim* =  $\nu E_2 \mu E_1$ , **where**

$$E_2 := \{ X^{M,S}(d : D^M, d' : D^S) = \text{match}^{M,S}(d, d') \wedge \text{match}^{S,M}(d', d) , \\ X^{S,M}(d' : D^S, d : D^M) = X^{M,S}(d, d') \} \\ E_1 := \{ Y_{1,a}^{p,q}(d : D^p, d' : D^q, e : E_a^p) = \text{close}_{1,a}^{p,q}(d, d', e), \\ Y_{2,a}^{p,q}(d : D^p, d' : D^q) = \text{close}_{2,a}^{p,q}(d, d'), \\ \quad \mid a \in \text{Act} \wedge (p, q) \in \{(M, S), (S, M)\} \}$$

Where we use the following abbreviations, for all  $a \in \text{Act} \wedge (p, q) \in \{(M, S), (S, M)\}$ :

$$\text{match}^{p,q}(d : D^p, d' : D^q) = \bigwedge_{a \in \text{Act}} \forall e : E_a^p. (h_a^p(d, e) \implies Y_{1,a}^{p,q}(d, d', e)); \\ \text{close}_{1,a}^{p,q}(d : D^p, d' : D^q, e : E_a^p) = \exists e' : E_a^q. (E_a^q. (h_a^q(d', e') \wedge Y_{1,a}^{p,q}(d, g_a^q(d', e'), e)) \\ \quad \vee \text{step}_a^{p,q}(d, d', e)); \\ \text{step}_a^{p,q}(d : D^p, d' : D^q, e : E_a^p) = (a = \tau \wedge \text{close}_{2,a}^{p,q}(g_a^p(d, e), d')) \vee \\ \exists e' : E_a^q. h_a^q(d', e') \wedge (f_a^p(d, e) = f_a^q(d', e')) \wedge \text{close}_{2,a}^{p,q}(g_a^p(d, e), g_a^q(d', e')) ; \\ \text{close}_{2,a}^{p,q}(d : D^p, d' : D^q) = X^{p,q}(d, d') \vee \exists e' : E_a^q. h_a^q(d', e') \wedge Y_{2,a}^{p,q}(d, g_a^q(d', e'));$$

**Algorithm 4** Generation of a PBES for (Branching) Simulation Equivalence*brsim*( $m, n$ ) =  $\nu E_2 \mu E_1$ , **where**

$$E_2 := \{ X(d : D^M, d' : D^S) = X^{M,S}(d, d') \wedge X^{S,M}(d', d), \\ X^{M,S}(d : D^M, d' : D^S) = \text{match}^{M,S}(d, d'), \\ X^{S,M}(d' : D^S, d : D^M) = \text{match}^{S,M}(d', d) \} \\ E_1 := \{ Y_a^{p,q}(m, n, e) = \text{close}_a^{p,q}(d, d', e) \mid a \in \text{Act} \}$$

Where we use the following abbreviations, for all  $a \in \text{Act} \wedge (p, q) \in \{(M, S), (S, M)\}$ :

$$\text{match}^{p,q}(d : D^p, d' : D^q) = \bigwedge_{a \in \text{Act}} \forall e : E_a^p. (h_a^p(d, e) \implies Y_a^{p,q}(d, d', e)); \\ \text{close}_a^{p,q}(d : D^p, d' : D^q, e : E_a^p) = \exists e' : E_a^q. (E_a^q. (h_a^q(d', e') \wedge Y_a^{p,q}(d, g_a^q(d', e'), e)) \\ \quad \vee (X^{p,q}(d, d') \wedge \text{step}_a^{p,q}(d, d', e))); \\ \text{step}_a^{p,q}(d : D^p, d' : D^q, e : E_a^p) = (a = \tau \wedge X^{p,q}(g_a^p(d, e), d')) \vee \\ \exists e' : E_a^q. h_a^q(d', e') \wedge (f_a^p(d, e) = f_a^q(d', e')) \wedge X^{p,q}(g_a^p(d, e), g_a^q(d', e'));$$

## 7 Conclusion

We have shown how to transform the strong, weak and branching (bi)simulation equivalence checking problems for infinite systems to solving Parameterized Boolean Equation Systems. We demonstrated our method on two small examples, showing that the concatenation of two one-place buffers behave as a queue of size 2, and that the concatenation of two unbounded queues is branching bisimilar to the concatenation of three unbounded queues. The latter example could not be solved directly with the cones and foci method (without introducing a third process), because these systems are not functionally branching bisimilar, and moreover, both systems perform  $\tau$ -steps.

Our solution is a symbolic verification algorithm. Compared to the previously known algorithms, it has the advantage that the solution of the PBES indicates exactly which states of the implementation and specification are bisimilar. This provides some positive feedback in case the initial states of the two systems are not bisimilar. Note that we have introduced a *generic* scheme that can be applied to other weak equivalences and preorders in branching time spectrum [10], and also to other formalisms of concurrency.

We conjecture that for infinite systems, it is essential that the PBES has alternation depth two, as opposed to the finite case. We leave it for future work to apply our method to various equivalences for mobile processes, in particular  $\pi$ -calculus [25], such as weak early, late and open bisimulation. Orthogonal to this, we shall continue our work on improving tool support for solving PBESs, and the application of our techniques to larger specifications of infinite systems.

*Acknowledgments.* We are grateful to Wan Fokkink and Jan Friso Groote for stimulating discussions.

## References

1. H. R. Andersen. Model checking and boolean graphs. *Theoretical Computer Science*, 126(1):3-30, 1994.
2. R. Alur and D.L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183-235, 1994.
3. H. R. Andersen and B. Vergauwen. Efficient checking of behavioural relations and modal assertions using fixed-point inversion. In Proc. CAV 1995, LNCS 939, pp. 142-154, Springer, 1995.
4. T. Basten. Branching bisimilarity is an equivalence indeed! *Information Processing Letters*, 58:141-147, 1996.
5. T. Bolognesi and E. Brinksma. Introduction to the ISO specification language LOTOS. *Computer Networks*, 14: 25-59, 1987.
6. K.M. Chandy and J. Misra. *Parallel Program Design: A Foundation*. Addison-Wesley, 1988.
7. R. Cleaveland and B. Steffen. Computing behavioural relations, logically. In Proc. ICALP 1991, LNCS 510, pp. 127-138, Springer, 1991.
8. A. van Dam, S.C.W. Ploeger and T.A.C. Willemsse. Solving Parameterised Boolean Equation Systems by Explicit Instantiation. In preparation.
9. W. Fokkink, J. Pang and J. van de Pol. Cones and foci: A mechanical framework for protocol verification. *Formal Methods in System Design*, 29(1):1-31, 2006.
10. R. van Glabbeek. The Linear Time - Branching Time Spectrum II. In Proc. CONCUR 1993, LNCS 715, pp. 66-81, Springer, 1993.

11. R.J. van Glabbeek and W.P. Weijland. Branching time and abstraction in bisimulation semantics. *Journal of the ACM*, 43:555-600, 1996.
12. J.F. Groote and R. Mateescu. Verification of temporal properties of processes in a setting with data. In Proc. AMAST 1998, LNCS 1548, pp. 74-90, Springer, 1998.
13. J.F. Groote and J. van de Pol. A bounded retransmission protocol for large data packets. In Proc. AMAST 1996, LNCS 1101, pp. 536-550, Springer, 1996.
14. J.F. Groote and M. Reniers. Algebraic process verification. In J.A. Bergstra, A. Ponse, and S.A. Smolka, eds, *Handbook of Process Algebra*, pp. 1151-1208. Elsevier, 2001.
15. J.F. Groote and F.W. Vaandrager. An efficient algorithm for branching bisimulation and stuttering equivalence. In Proc. ICALP'90, LNCS 443, pp. 626-638. Springer, 1990.
16. J.F. Groote and T.A.C. Willemse. Model-checking processes with data. *Science of Computer Program*, 56(3): 251-273, 2005.
17. J.F. Groote and T.A.C. Willemse. Parameterised boolean equation systems. *Theoretical Computer Science*, 343(3): 332-369, 2005.
18. H. Kwak, J. Choi, I. Lee and A. Philippou. Symbolic weak bisimulation for value-passing calculi. Technical Report, MS-CIS-98-22, Department of Computer and Information Science, University of Pennsylvania, 1998.
19. H. Lin. Symbolic transition graph with assignment. In Proc. CONCUR 1996, LNCS 1119, pp. 50-65, Springer, 1996.
20. N. Lynch and M. Tuttle. An introduction to input/output automata. *CWI Quarterly*, 2(3):219-246, 1989.
21. A. Mader. Verification of modal properties using boolean equation systems. PhD Thesis, VERSAL 8, Bertz Verlag, Berlin, 1997.
22. R. Mateescu. A generic on-the-fly solver for alternation-free boolean equation systems. In Proc. TACAS 2003, LNCS 2619, pp. 81-96. Springer, 2003.
23. R. Milner. *A Calculus of Communicating Systems*. Springer, 1980.
24. R. Milner. *Communication and Concurrency*. Prentice Hall, 1989.
25. R. Milner, J. Parrow and D. Walker. A calculus of mobile processes (Part I/II). *Information and Computation*, 100(1): 1-77, 1992.
26. R. Paige and R. Tarjan. Three partition refinement algorithms. *SIAM Journal of Computing*, 16(6): 973-989, 1987.
27. A. Tarski. A lattice-theoretical fixpoint theorem and its applications. *Pacific Journal of Mathematics*, 5(2): 285-309, 1955.
28. D. Zhang and R. Cleaveland. Fast generic model-checking for data-based systems. In Proc. FORTE 2005, LNCS 3731, pp. 83-97, Springer, 2005.