Partition Refinement for Bisimilarity in CCP
Andrés Aristizábal, Filippo Bonchi, Luis Pino, Frank Valencia

To cite this version:

HAL Id: hal-00641408
https://hal.archives-ouvertes.fr/hal-00641408v3
Submitted on 5 Dec 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Partition Refinement for Bisimilarity in CCP*  

Andrés Aristizábal †  
CNRS/DGA  
andresaristi@lix.polytechnique.fr  

Filippo Bonchi †  
CNRS  
filippo.bonchi@ens-lyon.fr  

Luis Fernando Pino †  
INRIA/DGA  
luis.pino@lix.polytechnique.fr  

Frank D. Valencia †  
CNRS  
frank.valencia@lix.polytechnique.fr  

ABSTRACT  
Saraswat’s concurrent constraint programming (ccp) is a mature formalism for modeling processes (or programs) that interact by telling and asking constraints in a global medium, called the store. Bisimilarity is a standard behavioural equivalence in concurrency theory, but a well-behaved notion of bisimilarity for ccp has been proposed only recently. When the state space of a system is finite, the ordinary notion of bisimilarity can be computed via the well-known partition refinement algorithm, but unfortunately, this algorithm does not work for ccp bisimilarity.

In this paper, we propose a variation of the partition refinement algorithm for verifying ccp bisimilarity. To the best of our knowledge this is the first work providing for the automatic verification of program equivalence for ccp.

Keywords  
Concurrent Constraint Programming, Bisimilarity, Partition Refinement.

1. INTRODUCTION  
Bisimilarity is the main representative of the so called behavioral equivalences, i.e., equivalence relations that determine when two processes (e.g., the specification and the implementation) behave in the same way. Many efficient algorithms and tools for bisimilarity checking have been developed [13][15][9]. Among these, the partition refinement algorithm [10] is the best known: first it generates the state space of a labeled transition system (LTS), i.e., the set of states reachable through the transitions; then, it creates a partition equating all states and afterwards, iteratively, refines these partitions by splitting non equivalent states. At the end, the resulting partition equates all and only bisimilar states.

Concurrent Constraint Programming (ccp) [13] is a formalism that combines the traditional algebraic and operational view of process calculi with a declarative one based upon first-order logic. In ccp, processes (agents or programs) interact by adding (or telling) and asking information (namely, constraints) in a medium (store).

Problem. The ccp formalism has been widely investigated and tested in terms of theoretical studies and the implementation of several ccp programming languages. From the applied computing point of view, however, ccp lacks algorithms and tools to automatically verify program equivalence. In this paper, we will give the first step towards automatic verification of ccp program equivalences by providing an algorithm to automatically verify a ccp process (or program) equivalence from the literature. Namely, saturated barbed bisimilarity.

Saturated barbed bisimilarity ($\sim_{sb}$) for ccp was introduced in [1]. Two configurations are equivalent according to $\sim_{sb}$ if (i) they have the same store, (ii) their transitions go into equivalent states and (iii) they are still equivalent when adding an arbitrary constraint to the store. In [1], a weak variant of $\sim_{sb}$ is shown to be fully abstract w.r.t. the standard observational equivalence of $\sim_{ob}$.

Unfortunately, the standard partition refinement algorithm does not work for $\sim_{sb}$ because condition (iii) requires to check all possible constraints that might be added to the store. In this paper we introduce a modified partition refinement algorithm for $\sim_{sb}$.

We closely follow the approach in [3] that studies the notion of saturated bisimilarity from a more general perspective and proposes an abstract checking procedure.

We first define a derivation relation $\vdash_D$ amongst the transitions of ccp processes: $\gamma \vdash_D \gamma'$ which intuitively means that the latter transition is a logical consequence of the former.

Then we introduce the notion of redundant transition. Intuitively, a transition $\gamma \rightarrow_{D} \gamma_2$ is redundant if there exists another transition $\gamma \rightarrow_{D} \gamma_1$ that logically implies it, that is $\gamma \vdash_D \gamma_1 \vdash_D \gamma_2$. Now, if we consider the LTS having only non-redundant transitions, the ordinary notion of bisimilarity coincides with $\sim_{sb}$. Thus, in principle, we could remove all the redundant transitions and then check bisimilarity with the standard partition refinement algorithm. But how can we decide which transitions are redundant, if redundancy itself depends on $\sim_{sb}$?

Our solution consists in computing $\sim_{sb}$ and redundancy at the same time. In the first step, the algorithm considers all the states as equivalent and all the transitions (potentially redundant) as redundant. At any iteration, states are discerned according to the current estimation of non-redundant transitions and then non-redundant transitions are updated according to the new computed partition.

A distinctive aspect of our algorithm is that in the initial partition, we insert not only the reachable states, but also extra ones which are needed to check for redundancy. We prove that these additional states are finitely many and thus the termination of the algorithm is guaranteed whenever the original LTS is finite (as it is the case

*This work has been partially supported by the project ANR-09-BLAN-0169-01 PANDA, and by the French Defence procurement agency (DGA) with two PhD grants.
†Comète, LIX, Laboratoire de l’Ecole Polytechnique associé à l’INRIA
‡ENS Lyon, Université de Lyon, LIP (UMR 5668 CNRS ENS Lyon UCBL INRIA), 46 Allée d’Italie, 69364 Lyon, France
of the standard partition refinement). Unfortunately, the number of these states might be exponential wrt the size of the original LTS, consequently the worst-case running time is exponential.

**Contributions.** We provide an algorithm that allows us to verify saturated barbed bisimilarity for ccp. To the best of our knowledge, this is the first algorithm for the automatic verification of a ccp program equivalence. This is done in Sections 3 and 4 by building upon the results of [5]. In Section 4.1 and 5.2 we also show the termination and the complexity of the algorithm. We have implemented the algorithm in C++ and the code is available at [http://www.lix.polytechnique.fr/~andresaristi/strong/](http://www.lix.polytechnique.fr/~andresaristi/strong/).

## 2. BACKGROUND

We now introduce the original standard partition refinement [10] and concurrent constraint programming (ccp).

### Partition Refinement

In this section we recall the partition refinement algorithm introduced in [10] for checking bisimilarity over the states of a labeled transition system (LTS). Recall that an LTS can be intuitively seen as a graph where nodes represent states (of computation) and arcs represent transitions between states. A transition $P \xrightarrow{a} Q$ between $P$ and $Q$ labelled with $a$ can be typically thought of as an evolution from $P$ to $Q$ provided that a condition $a$ is met.

Let us now introduce some notation. Given a set $S$, a partition of $S$ is a set of blocks, i.e., subsets of $S$, that are all disjoint and whose union is $S$. We write $\{B_1\} \ldots \{B_n\}$ to denote a partition consisting of blocks $B_1, \ldots, B_n$. A partition represents an equivalence relation where equivalent elements belong to the same block. We write $P\mathcal{P}Q$ to mean that $P$ and $Q$ are equivalent in the partition $P$.

The partition refinement algorithm (see Alg. 1) checks the bisimilarity of a set of initial states $IS$ as follows. First, it computes $IS^*$, that is the set of all states that are reachable from $IS$. Then it creates the partition $P^0$ where all the elements of $IS^*$ belong to the same block (i.e., they are all equivalent). After the initialization, it iteratively refines the partitions by employing the function $F$, defined as follows: for all partitions $P$, $P \mathcal{R}(P)$ if

- if $P \xrightarrow{a} P'$ then exists $Q'$ s.t. $Q \xrightarrow{a} Q'$ and $P \mathcal{P} Q'$.

The algorithm terminates whenever two consecutive partitions are equivalent. In such partition two states belong to the same block iff they are bisimilar.

Note that any iteration splits blocks and never fuses them. For this reason if $IS^*$ is finite, the algorithm terminates in at most $|IS^*|$ iterations.

**Proposition 1.** If $IS^*$ is finite, then the algorithm terminates and the resulting partition equates all and only the bisimilar states.

---

**Algorithm 1** Partition-Refinement ($IS$)

**Initialization**

1. $IS^*$ is the set of all processes reachable from $IS$.
2. $P^0 := \{IS^*\}$.

**Iteration** $P^{n+1} := F(P^n)$.

**Termination** If $P^n = P^{n+1}$ then return $P^n$.

### CCP

We now recall the concurrent constraint programming process calculus (ccp) [13] [14]. In particular its notion of saturated bisimilarity ($\sim_{sb}$) [1] is defined as follows: for all partitions $P$, $P \mathcal{R}(P)$ if for each $x \in V$. Broadly speaking $P$ has the properties of the existential quantification of $x$, i.e., $P \xrightarrow{a} P'$ if $P \mathcal{P} Q'$ and $P \mathcal{P} Q$. The worst-case running time is exponential wrt the size of the original LTS, hence the worst-case running time is exponential.

---

**Frame**: A ccp program $P$ consists of variables $V$ and a collection of guarded commands $\mathcal{C}$, a ccp program equivalence.

Let us now introduce some notation. Given a set $S$, we write $\{a\}_{S}$ as follows. First, it computes $IS^*$, that is the set of all states that are reachable from $IS$. Then it creates the partition $P^0$ where all the elements of $IS^*$ belong to the same block (i.e., they are all equivalent). After the initialization, it iteratively refines the partitions by employing the function $F$, defined as follows: for all partitions $P$, $P \mathcal{R}(P)$ if

- if $P \xrightarrow{a} P'$ then exists $Q'$ s.t. $Q \xrightarrow{a} Q'$ and $P \mathcal{P} Q'$.

The algorithm terminates whenever two consecutive partitions are equivalent. In such partition two states belong to the same block iff they are bisimilar.

Note that any iteration splits blocks and never fuses them. For this reason if $IS^*$ is finite, the algorithm terminates in at most $|IS^*|$ iterations.

**Proposition 1.** If $IS^*$ is finite, then the algorithm terminates and the resulting partition equates all and only the bisimilar states.

**Algorithm 1** Partition-Refinement ($IS$)

**Initialization**

1. $IS^*$ is the set of all processes reachable from $IS$.
2. $P^0 := \{IS^*\}$.

**Iteration** $P^{n+1} := F(P^n)$.

**Termination** If $P^n = P^{n+1}$ then return $P^n$.

### CCP

We now recall the concurrent constraint programming process calculus (ccp) [13] [14]. In particular its notion of saturated bisimilarity ($\sim_{sb}$) [1] is defined as follows: for all partitions $P$, $P \mathcal{R}(P)$ if for each $x \in V$. Broadly speaking $P$ has the properties of the existential quantification of $x$, i.e., $P \xrightarrow{a} P'$ if $P \mathcal{P} Q'$ and $P \mathcal{P} Q$. The worst-case running time is exponential wrt the size of the original LTS, hence the worst-case running time is exponential.

---

**Frame**: A ccp program $P$ consists of variables $V$ and a collection of guarded commands $\mathcal{C}$, a ccp program equivalence.

Let us now introduce some notation. Given a set $S$, we write $\{a\}_{S}$ as follows. First, it computes $IS^*$, that is the set of all states that are reachable from $IS$. Then it creates the partition $P^0$ where all the elements of $IS^*$ belong to the same block (i.e., they are all equivalent). After the initialization, it iteratively refines the partitions by employing the function $F$, defined as follows: for all partitions $P$, $P \mathcal{R}(P)$ if

- if $P \xrightarrow{a} P'$ then exists $Q'$ s.t. $Q \xrightarrow{a} Q'$ and $P \mathcal{P} Q'$.

The algorithm terminates whenever two consecutive partitions are equivalent. In such partition two states belong to the same block iff they are bisimilar.

Note that any iteration splits blocks and never fuses them. For this reason if $IS^*$ is finite, the algorithm terminates in at most $|IS^*|$ iterations.

**Proposition 1.** If $IS^*$ is finite, then the algorithm terminates and the resulting partition equates all and only the bisimilar states.
with identifier \( p \) and actual parameters \( z \). We presuppose that for each procedure call \( p(z_1, \ldots, z_m) \) there exists a unique procedure definition possibly recursive, of the form \( p(x_1, \ldots, x_m) \equiv P \) where \( \forall e \in \{ x_1, \ldots, x_m \} \).

**Reduction Semantics.** The operational semantics is given by transitions between configurations. A configuration is a pair \( \langle P, d \rangle \) representing a state of a system: \( d \) is a constraint representing the global store, and \( P \) is a process, i.e., a term of the syntax. We use \( \text{Conf} \) with typical elements \( \gamma, \gamma' \) to denote the set of configurations. The operational model of ccp is given by the transition relation \( \rightarrow \subseteq \text{Conf} \times \text{Conf} \) defined in Tab. 1. Except for R5, these standard rules are self-explanatory. We include R5 for completeness of the presentation but it is not necessary to understand our work in the next section. For the sake of space we refer the interested reader to [11] for a detailed explanation of the rules.

**Barbed Semantics.** The authors in [11] introduced a barbed semantics for ccp. Barbed equivalences have been introduced in [11] for CCS, and become the standard behavioural equivalences for formalisms equipped with unlabeled reduction semantics. Intuitively, barbs are basic observations (predicates) on the states of a system.

In the case of ccp, barbs are taken from the underlying set \( \text{Con}_0 \) of the constraint system. A configuration \( \gamma = \langle P, d \rangle \) is said to satisfy the barb \( c(\gamma) \) iff \( c \in d \).

**Definition 2.** A barbed bisimulation is a symmetric relation \( \mathcal{R} \) on configurations s.t. whenever \( (\gamma_1, \gamma_2) \in \mathcal{R} \):

(i) if \( \gamma_1 \downarrow \) then \( \gamma_2 \downarrow \),

(ii) if \( \gamma_1 \rightarrow \gamma'_1 \) then there exists \( \gamma'_2 \) s.t. \( \gamma_2 \rightarrow \gamma'_2 \) and \( (\gamma'_1, \gamma'_2) \in \mathcal{R} \).

\( \gamma_1 \) and \( \gamma_2 \) are **barbed bisimilar** \( (\gamma_1 \sim_b \gamma_2) \), if there exists a barbed bisimulation \( \mathcal{R} \) s.t. \( (\gamma_1, \gamma_2) \in \mathcal{R} \).

One can verify that \( \sim_b \) is an equivalence. However, it is not a congruence; i.e., it is not preserved under arbitrary contexts (the interested reader can check Ex. 7 in [11]). An elegant solution to modify bisimilarity for obtaining a congruence consists in **saturated barbed bisimulation** [4][3][2] (pioneered by [2]]. The basic idea is simple: saturated bisimilarations are closed w.r.t. all the possible contexts of the language. In the case of ccp, it is enough to require that bisimulations are **upward closed** as in condition **(iii)** below.

**Definition 3.** A saturated barbed bisimulation is a symmetric relation \( \mathcal{R} \) on configurations s.t. whenever \( (\gamma_1, \gamma_2) \in \mathcal{R} \) with \( \gamma_1 = \langle P, d \rangle \) and \( \gamma_2 = \langle Q, e \rangle \):

(i) if \( \gamma_1 \downarrow \) then \( \gamma_2 \downarrow \),

(ii) if \( \gamma_1 \rightarrow \gamma'_1 \) then there exists \( \gamma'_2 \) s.t. \( \gamma_2 \rightarrow \gamma'_2 \) and \( (\gamma'_1, \gamma'_2) \in \mathcal{R} \).

(iii) for every \( a \in \text{Con}_0 \), \( ((P, d \uplus a), (Q, e \uplus a)) \in \mathcal{R} \).

\( \gamma_1 \) and \( \gamma_2 \) are **saturated barbed bisimilar** \( (\gamma_1 \sim_{sb} \gamma_2) \) if there exists a saturated barbed bisimulation \( \mathcal{R} \) s.t. \( (\gamma_1, \gamma_2) \in \mathcal{R} \).

**Example 2.** Take \( T = \text{tell}(true) \), \( P = \text{ask}(x < 7) \rightarrow T \) and \( Q = \text{ask}(x < 5) \rightarrow T \). You can see that \( (P, true) \not\sim_{sb} (Q, true) \), since \( (P, x < 7) \rightarrow , \) while \( (Q, x < 7) \not\rightarrow . \) Consider now the configuration \( (P, Q, true) \) and observe that \( (P, true) \sim_{sb} (P, true) \). Indeed, for all constraints \( e, s.t. x < 7 \subseteq e \), both the configurations evolve into \( (T, e) \), while for all \( e, s.t. x < 7 \nsubseteq e \), both configurations cannot proceed. Since \( x < 7 \subseteq x < 5 \), the behaviour of \( Q \) is somehow absorbed by the behaviour of \( P \).

**Example 3.** Since \( \sim_{sb} \) is upward closed, \( (P + Q, z < 5) \sim_{sb} (P, z < 5) \) follows immediately by the previous example. Now take \( R = \text{ask}(z < 5) \rightarrow (P + Q) \) and \( S = \text{ask}(z < 7) \rightarrow P \). By analogous arguments of the previous example, one can show that \( (R + S, true) \sim_{sb} (S, true) \).

**Example 4.** Take \( T' = \text{tell}(y = 1) \), \( Q' = \text{ask}(x < 5) \rightarrow T' \) and \( R' = \text{ask}(z < 5) \rightarrow P + Q' \). Observe that \( (P + Q', z < 5) \not\sim_{sb} (P, z < 5) \) and that \( (R' + S, true) \not\sim_{sb} (S, true) \). Since \( (P + Q', x < 5) \) and \( (R' + S, true) \) can reach a store containing the constraint \( y = 1 \).

In [11], a weak variant of \( \sim_{sb} \) is introduced and it is shown that it is **fully abstract** w.r.t. the standard observational equivalence of [14]. In this paper, we will show an algorithm for checking \( \sim_{sb} \) and we leave, as future work, to extend it for the weak semantics.

Nevertheless, the equivalence \( \sim_{sb} \) would seem hard to (automatically) check because of the upward-closure (namely, the quantification over all possible \( a \in \text{Con}_0 \) in condition (iii) of Def. 3). The work in [11] deals with this issue by refining the notion of transition by adding to it a label that carries additional information about the constraints that cause the reduction.

**Labeled Semantics.** As explained in [11], in a transition of the form \( \langle P, d \rangle \xrightarrow{(\alpha, e)} \langle P', d' \rangle \) the label \( \alpha \) represents a minimal information (from the environment) that needs to be added to the store \( d \) to evolve from \( \langle P, d \rangle \) into \( \langle P', d' \rangle \), i.e., \( \langle P, d \uplus \alpha \rangle \rightarrow \langle P', d' \rangle \).

The labeled transition relation \( \rightarrow \subseteq \text{Conf} \times \text{Con}_0 \times \text{Conf} \) is defined by the rules in Tab. 2. The rule LR2, for example, says that \( \langle \text{ask} (c) \rightarrow P, d \rangle \) can evolve to \( \langle P, d \uplus c \rangle \) if the environment provides a minimal constraint \( c \) that added to the store \( d \) entails \( c \), i.e., \( c \in \min \{ a \in \text{Con}_0 | c \subseteq d \uplus a \} \). Note that assuming that \( \text{Con}_0 \subseteq \text{Conf} \times \text{Con}_0 \times \text{Conf} \) is well-founded (Sec. 2) is necessary to guarantee that \( a \) exists whenever \( a \in \text{Con}_0 \subseteq \text{Con}_0 \subseteq \) is not empty. The other rules, except LR4, are easily seen to realize the above intuition. An explanation of LR5 is not needed to understand the present work. For the sake of space, we refer the reader to [11] for a more detailed explanation of these labeled rules. Fig. 3 illustrates the LTSs of our running example.

**Syntactic Bisimilarity.** When defining bisimilarity over a LTS, bars are not usually needed because they can be somehow inferred from the labels of the transitions. For instance, in CCS, \( P \downarrow_c \) iff

\[
\begin{align*}
\text{R1} & \quad \langle \text{tell}(c), d \rangle \rightarrow (0, d \uplus c) \\
\text{R2} & \quad \langle \text{ask} (c) \rightarrow P, d \rangle \rightarrow (P, d) \\
\text{R3} & \quad (P, d) \rightarrow (P', d') \\
\text{R4} & \quad (P, d) \rightarrow (P', d') \\
\text{R5} & \quad (P, e \uplus z_d, d) \rightarrow (P', e' \uplus z_d, d) \\
\text{R6} & \quad (P[\vec{z}], d) \rightarrow \gamma' \quad \text{for } (p[\vec{z}]) \simeq \gamma
\end{align*}
\]

Table 1: Reduction semantics for ccp (the symmetric rules for R3 and R4 are omitted)
P \xrightarrow{a} s. However this is not the case of ccp: barbs cannot be removed from the definition of bisimilarity because they cannot be inferred from the transitions.

Taking into account the barbs, the obvious adaptation of labeled bisimilarity for ccp is the following:

**Definition 4.** A syntactic bisimulation is a symmetric relation $R$ on configurations s.t. whenever $(\gamma_1, \gamma_2) \in R$:

(i) if $\gamma_1 \xrightarrow{a} \gamma_1'$ then $\gamma_2 \xrightarrow{a} \gamma_2'$

(ii) if $\gamma_1 \xleftarrow{a} \gamma_1'$ then $\exists \gamma_2'$ s.t. $\gamma_2 \xrightarrow{a} \gamma_2'$ and $(\gamma_1', \gamma_2') \in R$.

$\gamma_1$ and $\gamma_2$ are syntactically bisimilar, $(\gamma_1 \sim \gamma_2)$ if there exists a syntactic bisimulation $R$ s.t. $(\gamma_1, \gamma_2) \in R$.

Unfortunately as shown in $\sim_{sb}$ is over-discriminating. As an example, consider the configurations $(P + Q, z < 5)$ and $(P, z < 5)$, whose LTS is shown in Fig. 1. They are not equivalent according to $\sim_{sb}$. Indeed $(P + Q, z < 5) \xrightarrow{\alpha} \alpha \beta \beta$ while $(P, z < 5) \xrightarrow{\alpha} \gamma \beta$. However they are equivalent according to $\sim_{ab}$ (Ex. 3).

**3. IRREDUNDANT BISIMILARITY**

Syntactic bisimilarity is over-discriminating because of some redundant transitions. For instance, consider the transitions:

(a) $(P + Q, z < 5) \xrightarrow{z < 5} (T, z < 5 \cup x < 7)$

(b) $(P + Q, z < 5) \xrightarrow{\alpha} (T, z < 5 \cup x < 5)$

Transition (a) means that for all constraints $e$ s.t. $x < 7 \subseteq e$, $(P + Q, z < 5) \xrightarrow{\alpha} (T, z < 5 \cup x < 7)$; while transition (b) means that the reduction (c) is possible for all $e$ s.t. $x < 5 \subseteq e$. Since $x < 7 \subseteq x < 5$, transition (b) is “redundant”, in the sense that its meaning is “logically derived” by transition (a).

The following notion captures the above intuition:

**Definition 5.** We say that $(P, c) \xrightarrow{a} (P', c')$ derives $(P, c) \xrightarrow{b} (P', c')$, written $(P, c) \xrightarrow{\beta} (P', c')$, if there exists $e$ s.t. the following conditions hold:

(i) $\beta = a \cup e$

(ii) $c' = c' \cup e$

(iii) $\alpha \neq \beta$

One can verify in the above example that (a) $\xrightarrow{\beta}$ (b). Notice that in order to check if $(P + Q, z < 5) \sim_{ab} (P, z < 5)$, we could first remove the redundant transition (b) and then check $\sim_{ab}$.

More generally, a naive approach to compute $\sim_{ab}$ would be to first remove all those transitions that can be derived by others, and then apply the partition refinement algorithm. However, this approach would fail since it would distinguish $(R + S, true)$ and $(S, true)$ that, instead, are in $\sim_{ab}$ (Ex. 3). Indeed, $(R + S, true)$ can perform:

(e) $(R + S, true) \xrightarrow{\alpha} (P, z < 7)$

(f) $(R + S, true) \xrightarrow{\beta} (P + Q, z < 5)$

while $(S, true) \xrightarrow{\alpha} (P + Q, z < 5)$. Note that transition (e) cannot be derived by other transitions, since $(e) \| (f)$. Indeed, $P$ is syntactically different from $P + Q$, even if they have the same behaviour when inserted in the store $z < 5$, i.e., $(P, z < 5) \sim_{ab} (P + Q, z < 5)$ (Ex. 3). The transition (f) is also “redundant”, since its behaviour “does not add anything” to the behaviour of (e).

**Definition 6.** Let $R$ be a relation and $\gamma \xrightarrow{\gamma_1}$ and $\gamma \xrightarrow{\gamma_2}$ be two transitions. We say that the former dominates the latter one in $R$ (written $\gamma \triangleright \gamma_1$ or $\gamma \xrightarrow{\triangleright} \gamma_2$) if

(i) $\gamma \xrightarrow{\gamma_1} \gamma_1 \triangleright \gamma_2$

(ii) $\gamma \xrightarrow{\triangleright} \gamma_2$s

A transition is redundant w.r.t. $R$ if it is dominated in $R$ by another transition. Otherwise, it is irredudant.

Note that the transition $\gamma \xrightarrow{\gamma_1}$ might not be generated by the rules in Tab. 2 but simply derived by $\gamma \xrightarrow{\gamma_1}$ through $\triangleright$. For
instance, transition (e) dominates (f) in $\sim_{sb}$, because (e)$\vdash_{D} (R + S, true)$ \iff (P, z < 5) and (P, z < 5)$\sim_{sb}(P + Q, z < 5)$.

Therefore, we could compute $\sim_{sb}$ by removing all those transitions that are redundant wrt $\sim_{sb}$. This, however, would lead us to a circular situation: How to decide which transitions are redundant when redundancy itself depends on $\sim_{sb}$.

Our solution relies on the following definition that allows to compute bisimilarity and redundancy at the same time.

**Definition 7.** An irredundant bisimulation is a symmetric relation $R$ on configurations s.t.
whenever $(\gamma_{1}, \gamma_{2}) \in R$:

(i) if $\gamma_{1} \vdash_{D}$ then $\gamma_{2} \vdash_{D}$,
(ii) if $\gamma_{1} \vdash_{D}$ is irredundant in $R$ then $\exists \gamma_{2}'$ s.t.
$\gamma_{2} \vdash_{D} \gamma_{2}'$ and $(\gamma_{1}', \gamma_{2}) \in R$.

$\gamma_{1}$ and $\gamma_{2}$ are irredundant bisimilar ($\gamma_{1} \sim_{IR} \gamma_{2}$), if there exists an irredundant bisimulation $R$ s.t. $(\gamma_{1}, \gamma_{2}) \in R$.

**Theorem 1.** $\sim_{L} = \sim_{sb}$.

**Proof.** See [2]. $\square$

4. PARTITION REFINEMENT FOR CCP

Recall that we mentioned in Sec. 2 that checking $\sim_{sb}$ seems hard because of the quantification over all possible constraints. However, by using Theo. 1, we shall introduce an algorithm for checking $\sim_{sb}$ by employing the notion of irredundant bisimulation.

The first novelty w.r.t. the standard partition refinement (Alg. 1) consists in using *barbs*. Since configurations satisfying different barbs are surely different, we can safely start with a partition that equates all and only those states satisfying the same barbs. Note that two configurations satisfy the same barbs iff they have the same store. Thus, we take as initial partition $P^{0} = \{I S_{S_{0}}\} \ldots \{I S_{S_{d}}\}$, where $I S_{S_{d}}$ is the subset of the configurations of $I S^{*}$ with store $d_{1}$.

Another difference is that instead of using the function $IR$ of Alg. 1 we refine the partitions by employing the function $IR$ defined as follows: for all partitions $P$, $\gamma_{1} IR(P) \gamma_{2}$ iff

- if $\gamma_{1} \vdash_{D} \gamma_{1}'$ is irredundant in $P$, then there exists $\gamma_{2}'$ s.t.
$\gamma_{2} \vdash_{D} \gamma_{2}'$ and $\gamma_{1}' P^{*} \gamma_{2}'$.

It is now important to observe that in the computation of $IR(P^{n})$, there might be involved also states that are not reachable from the initial states $I S$. For instance, consider the LTSs of $(S, true)$ and $(R + S, true)$ in Fig. 1. The state $(T, z < 5)$ is not reachable but is needed to check if $(R + S, true)$ \iff (P, z < 5) is redundant (look at the example after Def. 5).

For this reason, we have also to change the initialization step of our algorithm, by including in the set $I S^{*}$ all the states that are needed to check redundancy. This is done, by using the following closure rules:

- $(IS) \gamma_{1} \in I S^{*} \Rightarrow \gamma_{1} \in I S^{*}$
- $(IS) \gamma_{2} \in I S^{*} \Rightarrow \gamma_{1} \vdash_{D} \gamma_{2}$ and $\gamma_{2} \in I S^{*}$

**Algorithm 2 CCP-Partition-Refinement (IR)**

1. Compute $I S^{*}$ with the rules (IS), (RS) and (RD),
2. $P^{0} := \{I S_{S_{0}}\} \ldots \{I S_{S_{d}}\}$.

**Iteration** $P^{n+1} := IR(P^{n})$. $P^{n+1}$ is finite.

**Termination** If $P^{n+1} = P^{n}$ then return $P^{n}$.

Fig. 2 shows the partitions computed by the algorithm with initial states $(R + S, true)$, $(S, true)$ and $(R + S, true)$ be-
long to the same block, while $(R' + S, true)$ belong to a different one (meaning that the former two are saturated bisimilar, while $(R' + S, true)$ is different). In the initial partition all states with the same store are equated. In $P^{1}$, the blocks are split by considering the outgoing transitions: all the final states are distinguished (since they cannot perform any transitions) and $(T', z < 5 \cup x < 5)$ is distinguished from $(T', z < 5 \cup x < 5)$. All the other blocks are not divided, since all the transitions with label $x < 5$ are redundant in $P^{1}$ (since $(P, z < 5)P^{0} (P + Q', z < 5), (P, z < 5)P^{0} \vdash_{D} (P + Q', z < 5)$ and $(T', z < 5 \cup x < 5)P^{0} (T', z < 5 \cup x < 5)$). Then, in $P^{2}$, $(P + Q', z < 5)$ is distinguished from $(P, z < 5)$ since the transition $(P + Q', z < 5) \iff (P, z < 5)$ is not redundant anymore in $P^{1}$ (since $(T', z < 5 \cup x < 5)$ and $(T', z < 5 \cup x < 5)$ belong to different blocks in $P^{0}$). Then in $P^{3}$, $(R' + S, true)$ is distinguished from $(S, true)$ since the transition $(R' + S, true) \iff (P, z < 5)$ is not redundant in $P^{2}$ (since $(P + Q', z < 5)P^{2} (P, z < 5)$). Finally, the algorithm computes $P^{*}$ that is equal to $P^{3}$ and return it.

It is interesting to observe that the transition $(R' + S, true) \iff (P, z < 5)$ is redundant in all the partitions computed by the algorithm (and thus in $\sim_{sb}$), while the transition $(R' + S, true) \iff (P, z < 5)$ is considered redundant in $P^{0}$ and $P^{1}$ and not redundant in $P^{2}$ and $P^{3}$.

4.1 Termination

Note that any iteration splits blocks and never fuse them. For this reason if $I S^{*}$ is finite, the algorithm terminates in at most $|I S^{*}|$ iterations. The proof of the next proposition assumes that $\vdash_{D}$ is decidable. However, as we shall prove in the next section, the decidability of $\vdash_{D}$ follows from our assumption about the decidability of the ordering relation $\sqsubseteq$ of the underlying constraint system and Theo. 3.
Proposition 2. If $IS^*$ is finite, then the algorithm terminates and the resulting partition coincides with $\sim_{sb}$.

Proof. See [2].

We now prove that if the set $\text{Config}(IS)$ of all configurations reachable from $IS$ (through the LTS generated by the rules in Tab. 2) is finite, then $IS^*$ is finite.

This condition can be easily guaranteed by imposing some syntactic restrictions on ccp terms, like for instance, by excluding either the procedure call or the hiding operator.

Theorem 2. If $\text{Config}(IS)$ is finite, then $IS^*$ is finite.

Proof. See [2].

4.2 Complexity of the Implementation

Here we give asymptotic bounds for the execution time of Alg. 2) and the decision procedure for $\vdash$ (Def. 5) needed in the redundancy checks.

Recall that we assume $\Box$ to be decidable. Notice that requirement of having some $e$ that satisfies both conditions (i) and (ii) in Def. 5 suggests that deciding whether two given transitions belong to $\vdash$ may be costly. The following theorem, however, provides a simpler characterization of $\vdash$ allowing us to reduce the decision problem of $\vdash$ to that of $\Box$.

Theorem 3. $\langle P, c \rangle \vdash \langle P', c' \rangle$ iff the following conditions hold:

(a) $\alpha \subseteq \beta$

(b) $c'' = c' \cup \beta$

Proof. See [2].

Henceforth we shall assume that given a constraint system $C$, the function $f_C$ represents the time complexity of deciding (whether two given constraints are in) $\Box$. The following is a useful corollary of the above theorem.

Corollary 1. Given two transitions $t$ and $t'$, deciding whether $t \vdash t'$ takes $O(f_C)$ time.

Remark 2. We introduced $\vdash$ as in Def. 5 as natural adaptation of the corresponding notion in [5]. The simpler characterization given by the above theorem is due to particular properties of ccp transitions, in particular monotonicity of the store, and hence it may not hold in a more general scenario.

Complexity. The size of the set $IS^*$ is central to the complexity of Alg. 2 and depends on topology of the underlying transition graph. For tree-like topologies, a typical representation of many arguments that the size of $IS^*$ is asymptotic upper bounds in analysis of algorithms—see [6].

Our implementation of Alg. 2 is a variant of the original partition refinement algorithm in [10] with two main differences: The computation of $IS^*$ according to rules (IS), (RS) and (RD) (line 2, Alg. 2) and the decision procedure for $\vdash$ (Def. 5) needed in the redundancy checks.

Let $m$ be the number of transitions between those states. Then $n \times 2^{O(m)} \times f_c$ is an upper bound for the running time of Alg. 2.

Proof. See [2].

5. CONCLUDING REMARKS

In this paper we provided an algorithm for verifying (strong) bisimilarity for ccp by building upon the work in [5]. Weak bisimilarity is the variant obtained by ignoring, as much as possible, silent transitions (transitions labelled with true in the ccp case). Neither [5] nor the present work deal with this weak variant. We therefore plan to provide an algorithm for this central equivalence in future work.

6. REFERENCES


