An Efficient Simulation Algorithm on Kripke Structures

FRANCESCO RANZATO

Dipartimento di Matematica, University of Padova, Italy

Abstract

A number of algorithms for computing the simulation preorder (and equivalence) on Kripke structures are available. Let Σ denote the state space, $\rightarrow$ the transition relation and P_{sim} the partition of Σ induced by simulation equivalence. While some algorithms are designed to reach the best space bounds, whose dominating additive term is $|P_{\mathrm{sim}}|^2$, other algorithms are devised to attain the best time complexity $O(|P_{\mathrm{sim}}||{\rightarrow}|)$. We present a novel simulation algorithm which is both space and time efficient: it runs in $O(|P_{\mathrm{sim}}|^2 \log |P_{\mathrm{sim}}| + |\Sigma| \log |\Sigma|)$ space and $O(|P_{\mathrm{sim}}||{\rightarrow}| \log |\Sigma|)$ time. Our simulation algorithm thus reaches the best space bounds while closely approaching the best time complexity.

1 Introduction

The simulation preorder is a fundamental behavioral relation widely used in process algebra for establishing system correctness and in model checking as a suitable abstraction for reducing the size of state spaces [6]. The problem of efficiently computing the simulation preorder (and consequently simulation equivalence) on finite Kripke structures has been thoroughly investigated and generated a number of simulation algorithms [2, 3, 4, 7, 9, 11, 12, 14, 22, 23]. Both time and space complexities play an important role in simulation algorithms, since in several applications, especially in model checking, memory requirements may become a serious bottleneck as the input transition system grows.

State of the Art. Consider a finite Kripke structure where Σ denotes the state space, $\rightarrow$ the transition relation and P_{sim} the partition of Σ induced by simulation equivalence. The best simulation algorithms are those by, in chronological order, Gentilini, Piazza and Policriti (GPP) [10, 11] (subsequently corrected in [12]), Ranzato and Tapparo (RT) [20, 22], Markovski (Mar) [17], Cécé (Space-Céc and Time-Céc) [5]. The simulation algorithms GPP and RT are designed for Kripke structures, while Space-Céc, Time-Céc and Mar are for more general labeled transition systems. Their space and time complexities are summarized in the following table.

Algorithm	**Space complexity**	**Time complexity**
Space-Céc [5]	$O(\lvert P_{\mathrm{sim}}\rvert^2 + \lvert{\rightarrow}\rvert \log \lvert{\rightarrow}\rvert)$	$O(\lvert P_{\mathrm{sim}}\rvert^2 \lvert{\rightarrow}\rvert)$
Time-Céc [5]	$O(\lvert P_{\mathrm{sim}}\rvert\lvert\Sigma\rvert \log \lvert\Sigma\rvert + \lvert{\rightarrow}\rvert \log \lvert{\rightarrow}\rvert)$	$O(\lvert P_{\mathrm{sim}}\rvert\lvert{\rightarrow}\rvert)$
GPP [11]	$O(\lvert P_{\mathrm{sim}}\rvert^2 \log \lvert P_{\mathrm{sim}}\rvert + \lvert\Sigma\rvert \log \lvert\Sigma\rvert)$	$O(\lvert P_{\mathrm{sim}}\rvert^2 \lvert{\rightarrow}\rvert)$
Mar [17]	$O((\lvert\Sigma\rvert + \lvert P_{\mathrm{sim}}\rvert^2) \log \lvert P_{\mathrm{sim}}\rvert)$	$O(\lvert{\rightarrow}\rvert + \lvert P_{\mathrm{sim}}\rvert\lvert\Sigma\rvert + \lvert P_{\mathrm{sim}}\rvert^3)$
RT [22]	$O(\lvert P_{\mathrm{sim}}\rvert\lvert\Sigma\rvert \log \lvert\Sigma\rvert)$	$O(\lvert P_{\mathrm{sim}}\rvert\lvert{\rightarrow}\rvert)$
ESim (this paper)	$O(\lvert P_{\mathrm{sim}}\rvert^2 \log \lvert P_{\mathrm{sim}}\rvert + \lvert\Sigma\rvert \log \lvert\Sigma\rvert)$	$O(\lvert P_{\mathrm{sim}}\rvert\lvert{\rightarrow}\rvert \log \lvert\Sigma\rvert)$

We remark that all the above space bounds are bit space complexities, i.e., the word size is a single bit. Let us also remark that all the articles [10, 11, 12] state that the bit space complexity of GPP is in $O(|P_{\mathrm{sim}}|^2 + |\Sigma| \log |P_{\mathrm{sim}}|)$. However, as observed also in [5], this is not precise. In fact, the algorithm GPP [11, Section 4, p. 98] assumes that the states belonging to some block are stored as a doubly linked list, and this entails a bit space complexity in $O(|\Sigma| \log |\Sigma|)$. Furthermore, GPP uses Henzinger, Henzinger and Kopke [14] simulation algorithm (HKK) as a subroutine, whose bit space complexity is in $O(|\Sigma|^2 \log |\Sigma|)$, which is called on a Kripke structure where states are blocks of the current partition. The bit space complexity of GPP must therefore include an additive term $|P_{\mathrm{sim}}|^2 \log |P_{\mathrm{sim}}|$ and therefore results to be $O(|P_{\mathrm{sim}}|^2 \log |P_{\mathrm{sim}}| + |\Sigma| \log |\Sigma|)$. It is worth observing that a space complexity in $O(|P_{\mathrm{sim}}|^2 + |\Sigma| \log |P_{\mathrm{sim}}|)$ can be considered optimal for a simulation algorithm, since this is of the same order as the size of the output, which needs $|P_{\mathrm{sim}}|^2$ space for storing the simulation preorder as a partial order on simulation equivalence classes and $|\Sigma| \log |P_{\mathrm{sim}}|$ space for storing the simulation equivalence class for any state. Hence, the bit space complexities of GPP and Space-Céc can be considered quasi-optimal. As far as time complexity is concerned, the algorithms RT and Time-Céc both feature the best time bound $O(|P_{\mathrm{sim}}||{\rightarrow}|)$.

Contributions. We present here a novel space and time Efficient Simulation algorithm, called ESim, which features a bit space complexity in $O(|P_{\mathrm{sim}}|^2 \log |P_{\mathrm{sim}}| + |\Sigma| \log |\Sigma|)$ and a time complexity in $O(|P_{\mathrm{sim}}||{\rightarrow}| \log |\Sigma|)$. Thus, ESim reaches the best space bound of GPP and significantly improves the GPP time bound $O(|P_{\mathrm{sim}}|^2 |{\rightarrow}|)$ by replacing a multiplicative factor $|P_{\mathrm{sim}}|$ with $\log |\Sigma|$. Furthermore, ESim significantly improves the RT space bound $O(|P_{\mathrm{sim}}||\Sigma| \log |\Sigma|)$ and closely approaches the best time bound $O(|P_{\mathrm{sim}}||{\rightarrow}|)$ of RT and Time-Céc.

ESim is a partition refinement algorithm, meaning that it maintains and iteratively refines a so-called partition-relation pair $\langle P, \trianglelefteq \rangle$, where P is a partition of Σ that overapproximates the final simulation partition P_{sim}, while $\trianglelefteq$ is a binary relation over P which overapproximates the final simulation preorder. ESim relies on the following three main points, which in particular allow to attain the above complexity bounds.

(1) Two distinct notions of partition and relation stability for a partition-relation pair are introduced. Accordingly, at a logical level, ESim is designed as a partition refinement algorithm which iteratively performs two clearly distinct refinement steps: the refinement of the current partition P which splits some blocks of P and the refinement of the relation $\trianglelefteq$ which removes some pairs of blocks from $\trianglelefteq$.

(2) ESim exploits a logical characterization of partition refiners, i.e. blocks of P that allow to split the current partition P, which admits an efficient implementation.

(3) ESim only relies on data structures, like lists and matrices, that are indexed on and contain blocks of the current partition P. The hard task here is to devise efficient ways to keep updated these partition-based data structures along the iterations of ESim. We show that this can be done efficiently, in particular by resorting to Hopcroft's "process the smaller half" principle [16] when updating a crucial data structure after a partition split.

This is the full version of the conference paper [19].

2 Background

Notation. If $R \subseteq \Sigma \times \Sigma$ is any relation and $X \subseteq \Sigma$ then $R(X) \triangleq \{x' \in \Sigma \mid \exists x \in X.\, (x, x') \in R\}$. Recall that R is a preorder relation when it is reflexive and transitive. If f is a function defined on $\wp(\Sigma)$ and $x \in \Sigma$ then we often write $f(x)$ to mean $f(\{x\})$. $\mathrm{Part}(\Sigma)$ denotes the set of partitions of Σ. If $P \in \mathrm{Part}(\Sigma)$, $s \in \Sigma$ and $S \subseteq \Sigma$ then $P(s)$ denotes the block of P that contains s while $P(S) = \cup_{s\in S} P(s)$. $\mathrm{Part}(\Sigma)$ is endowed with the standard partial order $\preceq$: $P_1 \preceq P_2$, i.e. P_2 is coarser than P_1, iff for any $s \in \Sigma$, $P_1(s) \subseteq P_2(s)$. If $P_1 \preceq P_2$ and $B \in P_1$ then $P_2(B)$ is a block of P_2 which is also denoted by $\mathrm{parent}_{P_2}(B)$. For a given nonempty subset $S \subseteq \Sigma$ called splitter, we denote by $\mathit{Split}(P, S)$ the partition obtained from P by replacing each block $B \in P$ with $B \cap S$ and $B \smallsetminus S$, where we also allow no splitting, namely $\mathit{Split}(P, S) = P$ (this happens exactly when $P(S) = S$).

Simulation Preorder and Equivalence. A transition system $(\Sigma, \to)$ consists of a set Σ of states and of a transition relation $\to \subseteq \Sigma \times \Sigma$. Given a set AP of atoms (of some specification language), a Kripke structure (KS) $\mathcal{K} = (\Sigma, \to, \ell)$ over AP consists of a transition system $(\Sigma, \to)$ together with a state labeling function $\ell : \Sigma \to \wp(AP)$. The state partition induced by ℓ is denoted by $P_\ell \triangleq \{\{s' \in \Sigma \mid \ell(s) = \ell(s')\} \mid s \in \Sigma\}$. The predecessor/successor transformers $\mathrm{pre}, \mathrm{post} : \wp(\Sigma) \to \wp(\Sigma)$ are defined as usual: $\mathrm{pre}(T) \triangleq \{s \in \Sigma \mid \exists t \in T.\ s{\to}t\}$ and $\mathrm{post}(S) \triangleq \{t \in \Sigma \mid \exists s \in S.\ s{\to}t\}$. If $S_1, S_2 \subseteq \Sigma$ then $S_1{\to}^{\exists} S_2$ iff there exist $s_1 \in S_1$ and $s_2 \in S_2$ such that $s_1{\to}s_2$.

A relation $R \subseteq \Sigma \times \Sigma$ is a simulation on a Kripke structure $(\Sigma, \to, \ell)$ if for any $s, s' \in \Sigma$, if $s' \in R(s)$ then:

(A) $\ell(s) = \ell(s')$;

(B) for any $t \in \Sigma$ such that $s{\to}t$, there exists $t' \in \Sigma$ such that $s'{\to}t'$ and $t' \in R(t)$.

Given $s, t \in \Sigma$, t simulates s, denoted by $s \leq t$, if there exists a simulation relation R such that $t \in R(s)$. It turns out that the largest simulation on a given KS exists, is a preorder relation called simulation preorder and is denoted by R_{sim}. Thus, for any $s, t \in \Sigma$, we have that $s \leq t$ iff $(s, t) \in R_{\mathrm{sim}}$. The simulation partition $P_{\mathrm{sim}} \in \mathrm{Part}(\Sigma)$ is the symmetric reduction of R_{sim}, namely, for any $s, t \in \Sigma$, $P_{\mathrm{sim}}(s) = P_{\mathrm{sim}}(t)$ iff $s \leq t$ and $t \leq s$.

3 Logical Simulation Algorithm

3.1 Partition-Relation Pairs

A partition-relation pair $\mathcal{P} = \langle P, \trianglelefteq \rangle$, PR for short, is a state partition $P \in \mathrm{Part}(\Sigma)$ together with a binary relation $\trianglelefteq \subseteq P \times P$ between blocks of P. We write $B \vartriangleleft C$ when $B \trianglelefteq C$ and $B \neq C$ and $(B', C') \trianglelefteq (B, C)$ when $B' \trianglelefteq B$ and $C' \trianglelefteq C$. When $\trianglelefteq$ is a preorder/partial order then $\mathcal{P}$ is called, respectively, a preorder/partial order PR.

PRs allow to represent symbolically, i.e. through state partitions, a relation between states. A relation $R \subseteq \Sigma \times \Sigma$ induces a PR $\mathrm{PR}(R) = \langle P, \trianglelefteq \rangle$ defined as follows:

- for any s, $P(s) \triangleq \{t \in \Sigma \mid R(s) = R(t)\}$;
- for any s, t, $P(s) \trianglelefteq P(t)$ iff $t \in R(s)$.

It is easy to note that if R is a preorder then $\mathrm{PR}(R)$ is a partial order PR. On the other hand, a PR $\mathcal{P} = \langle P, \trianglelefteq \rangle$ induces the following relation $\mathrm{Rel}(\mathcal{P}) \subseteq \Sigma \times \Sigma$:

$$(s, t) \in \mathrm{Rel}(\mathcal{P}) \ \Leftrightarrow\ P(s) \trianglelefteq P(t).$$

Here, if $\mathcal{P}$ is a preorder PR then $\mathrm{Rel}(\mathcal{P})$ is clearly a preorder.

A PR $\mathcal{P} = \langle P, \trianglelefteq \rangle$ is defined to be a simulation PR on a KS $\mathcal{K}$ when $\mathrm{Rel}(\mathcal{P})$ is a simulation on $\mathcal{K}$, namely when $\mathcal{P}$ represents a simulation relation between states. Hence, if $\mathcal{P}$ is a simulation PR and $P(s) = P(t)$ then s and t are simulation equivalent, while if $P(s) \trianglelefteq P(t)$ then t simulates s.

Given a PR $\mathcal{P} = \langle P, \trianglelefteq \rangle$, the map $\mu_{\mathcal{P}} : \wp(\Sigma) \to \wp(\Sigma)$ is defined as follows:

$$\text{for any } X \in \wp(\Sigma),\ \mu_{\mathcal{P}}(X) \triangleq \mathrm{Rel}(\mathcal{P})(X) = \cup\{C \in P \mid \exists s \in X.\, P(s) \trianglelefteq C\}.$$

Note that, for any $s \in \Sigma$, $\mu_{\mathcal{P}}(s) = \mu_{\mathcal{P}}(P(s)) = \cup\{C \in P \mid P(s) \trianglelefteq C\}$. For preorder PRs, this map allows us to characterize the property of being a simulation PR as follows.

Theorem 3.1. *Let $\mathcal{P} = \langle P, \trianglelefteq \rangle$ be a preorder PR. Then, $\mathcal{P}$ is a simulation iff*

(i) *if $B \trianglelefteq C$, $b \in B$ and $c \in C$ then $\ell(b) = \ell(c)$;*

(ii) *if $B \to^{\exists} C$ and $B \trianglelefteq D$ then $D \to^{\exists} \mu_{\mathcal{P}}(C)$;*

(iii) *for any $C \in P$, $P = \mathit{Split}(P, \mathrm{pre}(\mu_{\mathcal{P}}(C)))$.*

Proof. ($\Rightarrow$) Condition (i) clearly holds. Assume that $B \to^{\exists} C$ and $B \trianglelefteq D$. Hence, there exist $b \in B$ and $c \in C$ such that $b \to c$. Consider any state $d \in D$. Since $\mathcal{P}$ is a simulation and $P(b) \trianglelefteq P(d)$, there exist some state e such that $d \to e$ and $C = P(c) \trianglelefteq P(e)$. Hence, $D \to^{\exists} \mu_{\mathcal{P}}(C)$. Finally, if $C \in P$ and $x \in \mathrm{pre}(\mu_{\mathcal{P}}(C))$ then there exists some block $D \trianglerighteq C$ and state $d \in D$ such that $x \to d$. If $y \in P(x)$ then since $P(x) = P(y)$, by reflexivity of $\trianglelefteq$, we have that $P(x) \trianglelefteq P(y)$, so that, since $\mathcal{P}$ is a simulation, there exists some state e such that $y \to e$ and $P(d) \trianglelefteq P(e)$. Since $\trianglelefteq$ is transitive, we have that $C \trianglelefteq P(e)$. Hence, $y \in \mathrm{pre}(\mu_{\mathcal{P}}(C))$. We have thus shown that $P(x) \subseteq \mathrm{pre}(\mu_{\mathcal{P}}(C))$, so that $P = \mathit{Split}(P, \mathrm{pre}(\mu_{\mathcal{P}}(C)))$.
($\Leftarrow$) Let us show that $\mathrm{Rel}(\mathcal{P})$ is a simulation, i.e., if $P(s) \trianglelefteq P(s')$ then: (a) $\ell(s) = \ell(s')$; (b) if $s \to t$ then there exists t' such that $s' \to t'$ and $P(t) \trianglelefteq P(t')$. Condition (a) holds by hypothesis (i). If $s \to t$ then $P(s) \to^{\exists} P(t)$ so that, by condition (ii), we have that $P(s') \to^{\exists} \mu_{\mathcal{P}}(P(t))$, namely there exists $s'' \in P(s')$ such that $s'' \in \mathrm{pre}(\mu_{\mathcal{P}}(P(t)))$. By condition (iii), $P(s'') \subseteq \mathrm{pre}(\mu_{\mathcal{P}}(P(t)))$, i.e., $s' \in \mathrm{pre}(\mu_{\mathcal{P}}(P(t)))$. Hence, there exists t' such that $s' \to t'$ and $P(t) \trianglelefteq P(t')$. □

3.2 Partition and Relation Refiners

By Theorem 3.1, assuming that condition (i) holds, there are two possible reasons for a PR $\mathcal{P} = \langle P, \trianglelefteq \rangle$ for not being a simulation:

(1) There exist $B, C, D \in P$ such that $B \to^{\exists} C$, $B \trianglelefteq D$, but $D \not\to^{\exists} \mu_{\mathcal{P}}(C)$; in this case we say that the block C is a *relation refiner* for $\mathcal{P}$.

(2) There exist $B, C \in P$ such that $B \cap \mathrm{pre}(\mu_{\mathcal{P}}(C)) \neq \varnothing$ and $B \smallsetminus \mathrm{pre}(\mu_{\mathcal{P}}(C)) \neq \varnothing$; in this case we say that the block C is a *partition refiner* for $\mathcal{P}$.

We therefore define:

$\mathrm{RRefiner}(\mathcal{P}) \triangleq \{C \in P \mid C$ is a relation refiner for $\mathcal{P}\}$;

$\mathrm{PRefiner}(\mathcal{P}) \triangleq \{C \in P \mid C$ is a partition refiner for $\mathcal{P}\}$.

Accordingly, $\mathcal{P}$ is defined to be relation or partition *stable* when, respectively, $\mathrm{RRefiner}(\mathcal{P}) = \varnothing$ or $\mathrm{PRefiner}(\mathcal{P}) = \varnothing$. Then, Theorem 3.1 can be read as follows: $\mathcal{P}$ is a simulation iff $\mathcal{P}$ satisfies condition (i) and is both relation and partition stable.

If $C \in \mathrm{PRefiner}(\mathcal{P})$ then P is first refined to $P' \triangleq \mathit{Split}(P, \mathrm{pre}(\mu_{\mathcal{P}}(C)))$, i.e. P is split w.r.t. the splitter $S = \mathrm{pre}(\mu_{\mathcal{P}}(C))$. Accordingly, the relation $\trianglelefteq$ on P is transformed into the following relation $\trianglelefteq'$ defined on P':

$$\trianglelefteq' \;\triangleq\; \{(D, E) \in P' \times P' \mid \mathrm{parent}_P(D) \trianglelefteq \mathrm{parent}_P(E)\} \qquad (\dagger)$$

Hence, two blocks D and E of the refined partition P' are related by $\trianglelefteq'$ if their parent blocks $\mathrm{parent}_P(D)$ and $\mathrm{parent}_P(E)$ in P were related by $\trianglelefteq$. Hence, if $\mathcal{P}' = \langle P', \trianglelefteq' \rangle$ then for all $D \in P'$, we have that $\mu_{\mathcal{P}'}(D) = \mu_{\mathcal{P}}(\mathrm{parent}_P(D))$. We will show that this refinement of $\langle P, \trianglelefteq \rangle$ is correct because if $B \in P$ is split into $B \smallsetminus S$ and $B \cap S$ then all the states in $B \smallsetminus S$ are not simulation equivalent to all the states in $B \cap S$. Note that if $B \in P$ has been split into $B \cap S$ and $B \smallsetminus S$ then both $B \cap S \trianglelefteq' B \smallsetminus S$ and $B \smallsetminus S \trianglelefteq' B \cap S$ hold, and consequently $\mathcal{P}'$ becomes relation unstable.

On the other hand, if $\mathcal{P}$ is partition stable and $C \in \mathrm{RRefiner}(\mathcal{P})$ then we will show that $\trianglelefteq$ can be safely refined to the following relation $\trianglelefteq'$:

$$\begin{aligned} \trianglelefteq' &\triangleq \trianglelefteq \smallsetminus \{(B, D) \in P \times P \mid B \to^{\exists} C,\ B \trianglelefteq D,\ D \not\to^{\exists} \mu_{\mathcal{P}}(C)\} \\ &= \{(B, D) \in P \times P \mid B \trianglelefteq D,\ \big(B \to^{\exists} C \Rightarrow D \to^{\exists} \mu_{\mathcal{P}}(C)\big)\} \end{aligned} \tag{‡}$$

because if $(B, D) \in \trianglelefteq \smallsetminus \trianglelefteq'$ then all the states in D cannot simulate all the states in B.

$\mathrm{ESim}(\textbf{PR}\ \langle P, \trianglelefteq \rangle)$ {
  $\mathit{Initialize}()$; $\mathit{PStabilize}()$; **bool** $\mathrm{PStable} := \mathit{RStabilize}()$; **bool** $\mathrm{RStable} :=$ **tt**;
  while $\neg(\mathrm{PStable}\ \&\ \mathrm{RStable})$ **do**
    if $\neg\,\mathrm{PStable}$ **then** $\{\mathrm{RStable} := \mathit{PStabilize}();\ \mathrm{PStable} :=$ **tt**;}
    if $\neg\,\mathrm{RStable}$ **then** $\{\mathrm{PStable} := \mathit{RStabilize}();\ \mathrm{RStable} :=$ **tt**;}
}

bool $\mathit{PStabilize}()$ {
  $P_{\mathrm{old}} := P$;
  while $\exists C \in \mathrm{PRefiner}(\mathcal{P})$ **do**
    $S := \mathrm{pre}(\mu_{\mathcal{P}}(C))$; $P := \mathit{Split}(S)$;
    forall $(D, E) \in P \times P$ **do** $D \trianglelefteq E\ :=\ \mathrm{parent}_P(D) \trianglelefteq \mathrm{parent}_P(E)$;
  return $(P = P_{\mathrm{old}})$;
}

bool $\mathit{RStabilize}()$ {
  // Precondition: $\mathrm{PStable} =$ **tt**
  $\trianglelefteq_{\mathrm{old}} := \trianglelefteq$; $\mathrm{Delete} := \varnothing$;
  while $\exists C \in \mathrm{RRefiner}(\mathcal{P})$ **do**
    $\mathrm{Delete}\ :=\ \mathrm{Delete} \cup \{(B, D) \in P \times P \mid B \trianglelefteq D,\ B \to^{\exists} C,\ D \not\to^{\exists} \mu_{\mathcal{P}}(C)\}$;
  $\trianglelefteq := \trianglelefteq \smallsetminus \mathrm{Delete}$;
  return $(\trianglelefteq = \trianglelefteq_{\mathrm{old}})$;
}

Figure 1: Logical Simulation Algorithm.

The above facts lead us to design a basic simulation algorithm ESim described in Figure 1. ESim maintains a PR $\mathcal{P} = \langle P, \trianglelefteq \rangle$, which initially is $\langle P_\ell, \mathrm{id} \rangle$ and is iteratively refined as follows:

$\mathit{PStabilize}()$: If $\langle P, \trianglelefteq \rangle$ is not partition stable then the partition P is split for $\mathrm{pre}(\mu_{\mathcal{P}}(C))$ as long as a partition refiner C for $\mathcal{P}$ exists, and when this happens the relation $\trianglelefteq$ is transformed to $\trianglelefteq'$ as defined by (†); at the end of this process, we obtain a PR $\mathcal{P}' = \langle P', \trianglelefteq' \rangle$ which is partition stable and if P has been actually refined, i.e. $P' \prec P$ then the current PR $\mathcal{P}'$ becomes relation unstable.

$\mathit{RStabilize}()$: If $\langle P, \trianglelefteq \rangle$ is not relation stable then the relation $\trianglelefteq$ is refined to $\trianglelefteq'$ as described by (‡) as long as a relation refiner for $\mathcal{P}$ exists; hence, at the end of this refinement process $\langle P, \trianglelefteq' \rangle$ becomes relation stable but possibly partition unstable.

Moreover, the following properties of the current PR of ESim hold.

Lemma 3.2. *In any run of* ESim, *the following two conditions hold:*

(i) *If $\mathit{PStabilize}()$ is called on a partial order PR $\langle P, \trianglelefteq \rangle$ then at the exit we obtain a PR $\langle P', \trianglelefteq' \rangle$ which is a preorder.*

(ii) *If $\mathit{RStabilize}()$ is called on a preorder PR $\langle P, \trianglelefteq \rangle$ then at the exit we obtain a PR $\langle P, \trianglelefteq' \rangle$ which is a partial order.*

Proof. Let us first consider $\mathit{PStabilize}()$. Consider an input partial order PR $\mathcal{P} = \langle P, \trianglelefteq \rangle$, a splitter S such that $P' = \mathit{Split}(P, S)$ and let $\trianglelefteq'$ be defined as in equation (†). Let us show that $\langle P', \trianglelefteq' \rangle$ is a preorder PR.

(Reflexivity): If $B \in P'$ then, as $\trianglelefteq$ is reflexive, $P(B) \trianglelefteq P(B)$ and thus $B \trianglelefteq' B$.

(Transitivity): Assume that $B, C, D \in P'$ and $B \trianglelefteq' C$ and $C \trianglelefteq' D$. Then, $P(B) \trianglelefteq P(C)$ and $P(C) \trianglelefteq P(D)$, so that by transitivity of $\trianglelefteq$, $P(B) \trianglelefteq P(D)$. Hence, $B \trianglelefteq' D$.

Let us then take into account $\mathit{RStabilize}()$, consider an input preorder PR $\mathcal{P} = \langle P, \trianglelefteq \rangle$ and let $\langle P, \trianglelefteq' \rangle$ be the output PR of $\mathit{RStabilize}()$.

(Reflexivity): If $B \in P$ then, by reflexivity of $\trianglelefteq$, $B \trianglelefteq B$. If $B \to^{\exists} C$, for some $C \in P$, then since $C \trianglelefteq C$ by reflexivity of $\trianglelefteq$, we have that $B \to^{\exists} \mu_{\mathcal{P}}(C)$. Hence, $B \trianglelefteq' B$.

(Transitivity): Assume that $B \trianglelefteq' C$ and $C \trianglelefteq' D$. Then, $B \trianglelefteq C$ and $C \trianglelefteq D$, so that by transitivity of $\trianglelefteq$, $B \trianglelefteq D$. If $B \to^{\exists} E$ then, since $B \trianglelefteq' C$, $C \to^{\exists} \mu_{\mathcal{P}}(E)$. Hence, there exists $F \in P$ such that $E \trianglelefteq F$ and $C \to^{\exists} F$. Since $C \trianglelefteq' D$, we have that $D \to^{\exists} \mu_{\mathcal{P}}(F)$. Since $\trianglelefteq$ is transitive and $E \trianglelefteq F$, $\mu_{\mathcal{P}}(F) \subseteq \mu_{\mathcal{P}}(E)$. Thus, we have shown that $B \to^{\exists} E$ implies $D \to^{\exists} \mu_{\mathcal{P}}(E)$, namely $B \trianglelefteq' D$.

(Antisymmetry): We observe that after calling $\mathit{PStabilize}()$ on a partial order PR, antisymmetry can be lost because for any block B which is split into $B_1 = B \cap S$ and $B_2 = B \smallsetminus S$, where $S = \mathrm{pre}(\mu_{\mathcal{P}}(C))$, we have that $B_1 \trianglelefteq B_2$ and $B_2 \trianglelefteq B_1$. In this case, $\mathit{RStabilize}()$ removes the pair $(B \cap S, B \smallsetminus S)$ from the relation $\trianglelefteq$: in fact, while $B \cap S \subseteq \mathrm{pre}(\mu_{\mathcal{P}}(C))$ and therefore $B \cap S \to^{\exists} E$, for some block $E \subseteq \mu_{\mathcal{P}}(C)$, we have that $(B \smallsetminus S) \cap \mathrm{pre}(\mu_{\mathcal{P}}(C)) = \varnothing$, so that, since $\mu_{\mathcal{P}}(E) \subseteq \mu_{\mathcal{P}}(C)$, $(B \smallsetminus S) \cap \mathrm{pre}(\mu_{\mathcal{P}}(E)) = \varnothing$, i.e., $B \smallsetminus S \not\to^{\exists} \mu_{\mathcal{P}}(E)$, and therefore $B \cap S \not\trianglelefteq' B \smallsetminus S$. Hence, $\mathit{RStabilize}()$ outputs a relation $\trianglelefteq'$ which is antisymmetric. □

The main loop of ESim terminates when the current PR $\langle P, \trianglelefteq \rangle$ becomes both partition and relation stable. By the above Lemma 3.2, the output PR $\mathcal{P}$ of ESim is a partial order, and hence a preorder, so that Theorem 3.1 can be applied to $\mathcal{P}$ which then results to be a simulation PR. It turns out that this algorithm is correct, meaning that the output PR $\mathcal{P}$ actually represents the simulation preorder.

Theorem 3.3 (**Correctness**). *Let Σ be finite.* ESim *is correct, i.e.,* ESim *terminates on any input and if $\langle P, \trianglelefteq \rangle$ is the output PR of* ESim *on input $\langle P_\ell, \mathrm{id} \rangle$ then for any $s, t \in \Sigma$, $s \leq t \;\Leftrightarrow\; P(s) \trianglelefteq P(t)$.*

Proof. Let us first note that ESim always terminates. In fact, if $\langle P, \trianglelefteq \rangle$ is the current PR at the beginning of some iteration of the while-loop of ESim and $\langle P', \trianglelefteq' \rangle$ is the current PR at the beginning of the next iteration then, since $\langle P', \trianglelefteq' \rangle$ is either partition or relation unstable, we have that either $P' \lhd P$ or $P' = P$ and $\trianglelefteq' \subsetneq \trianglelefteq$. Since the state space Σ is finite, at some iteration it must happen that $P' = P$ and $\trianglelefteq' = \trianglelefteq$ so that PStable $\&$ RStable $=$ **tt**.

When ESim terminates, we have that $\mathrm{RRefiner}(\langle P, \trianglelefteq \rangle) = \varnothing = \mathrm{PRefiner}(\langle P, \trianglelefteq \rangle)$. Also, let us observe that condition (i) of Theorem 3.1 always holds for the current PR $\langle P, \trianglelefteq \rangle$ because the input PR

$\langle P_\ell, \mathrm{id}\rangle$ initially satisfies condition (i) and this condition is clearly preserved at any iteration of ESim. Furthermore, at the beginning, we have that $\langle P, \trianglelefteq\rangle = \langle P_\ell, \mathrm{id}\rangle$ and this is trivially a partial order. Thus, we can apply Lemma 3.2 for any call to $\mathit{PStabilize}()$ and $\mathit{RStabilize}()$, so that we obtain that the output PR $\langle P, \trianglelefteq\rangle$ is a preorder. Hence, Theorem 3.1 can be applied to the output preorder PR $\langle P, \trianglelefteq\rangle$, which is then a simulation. Thus, $\mathrm{Rel}(\langle P, \trianglelefteq\rangle) \subseteq R_{\mathrm{sim}}$.

Conversely, let us show that if $\mathcal{P}$ is the output PR of ESim then $R_{\mathrm{sim}} \subseteq \mathrm{Rel}(\mathcal{P})$. This is shown as follows: if $\mathcal{P}$ is a preorder PR such that $R_{\mathrm{sim}} \subseteq \mathrm{Rel}(\mathcal{P})$ and $\mathit{RStabilize}()$ or $\mathit{PStabilize}()$ are called on $\mathcal{P}$ then at the exit we obtain a PR $\mathcal{P}'$ such that $R_{\mathrm{sim}} \subseteq \mathrm{Rel}(\mathcal{P}')$.

Let us first take into account $\mathit{RStabilize}()$, consider an input preorder PR $\mathcal{P} = \langle P, \trianglelefteq\rangle$ such that $R_{\mathrm{sim}} \subseteq \mathrm{Rel}(\mathcal{P})$, and let $\mathcal{P}' = \langle P, \trianglelefteq'\rangle$ be the output PR of $\mathit{RStabilize}()$. We show that $R_{\mathrm{sim}} \subseteq \mathrm{Rel}(\mathcal{P}')$, that is, for any $s, t \in \Sigma$, if $s \leq t$ then $P(s) \trianglelefteq' P(t)$. By hypothesis, from $s \leq t$ we obtain $P(s) \trianglelefteq P(t)$. Assume that $P(s) \to^\exists C$, for some $C \in P$. Hence, $P(s) \to^\exists \mu_{\mathcal{P}}(C)$. Since the PR $\mathcal{P}$ is partition stable, we have that $P(s) \subseteq \mathrm{pre}(\mu_{\mathcal{P}}(C))$. Thus, there exists some $D \in P$ and $d \in D$ such that $C \trianglelefteq D$ and $s \to d$. Therefore, since t simulates s, there exists some state e such that $t \to e$ and $d \leq e$. By hypothesis, from $d \leq e$ we obtain $D = P(d) \trianglelefteq P(e)$. Hence, from $C \trianglelefteq D$ and $D \trianglelefteq P(e)$, since $\trianglelefteq$ is transitive, we obtain $C \trianglelefteq P(e)$. Thus, $t \to^\exists \mu_{\mathcal{P}}(C)$ and in turn $P(t) \to^\exists \mu_{\mathcal{P}}(C)$. We can thus conclude that $P(s) \trianglelefteq' P(t)$.

Let us now consider $\mathit{PStabilize}()$. Consider an input preorder PR $\mathcal{P} = \langle P, \trianglelefteq\rangle$ (which, by Lemma 3.2, actually is a partial order PR) such that $R_{\mathrm{sim}} \subseteq \mathrm{Rel}(\mathcal{P})$. Consider a splitter S such that $P' = \mathit{Split}(P, S)$ and let $\trianglelefteq'$ be defined as in equation (†). Let $\mathcal{P}' = \langle P', \trianglelefteq'\rangle$ and let us check that $R_{\mathrm{sim}} \subseteq \mathrm{Rel}(\mathcal{P}')$, i.e., if $s \leq t$ then $P'(s) \trianglelefteq' P'(t)$. By hypothesis, if $s \leq t$ then $P(s) \trianglelefteq P(t)$. Moreover, by definition of $\trianglelefteq'$ and since $P' \preceq P$, $P(s) \trianglelefteq P(t)$ iff $P'(s) \trianglelefteq' P'(t)$.

To sum up, we have shown that for the output PR $\langle P, \trianglelefteq\rangle$, $R_{\mathrm{sim}} = \mathrm{Rel}(\langle P, \trianglelefteq\rangle)$, so that $s \leq t$ iff $P(s) \trianglelefteq P(t)$. □

4 Efficient Implementation

4.1 Data Structures

ESim is implemented by relying on the following data structures.

States: A state s is represented by a record that contains the list $\mathrm{post}(s)$ of its successors, a pointer s.block to the block $P(s)$ that contains s and a boolean flag used for marking purposes. The whole state space Σ is represented as a doubly linked list of states. $\{\mathrm{post}(s)\}_{s\in\Sigma}$ therefore represents the input transition system.

Partition: The states of any block B of the current partition P are consecutive in the list Σ, so that B is represented by two pointers begin and end: B.begin is the first state of B in Σ and B.end is the successor of the last state of B in Σ, i.e., $B = [B.\mathrm{begin}, B.\mathrm{end}[$. Moreover, B stores a boolean flag B.intersection and a block pointer B.brother whose meanings are as follows: after a call to $\mathit{Split}(P, S)$ for splitting P w.r.t. a set of states S, if $B_1 = B \cap S$ and $B_2 = B \smallsetminus S$, for some $B \in P$ that has been split by S then B_1.intersection = **tt** and B_2.intersection = **ff**, while B_1.brother points to B_2 and B_2.brother points to B_1. If instead B has not been split by S then B.intersection = **null** and B.brother = **null**. Also, any block B stores in $\mathit{Rem}(B)$ a list of blocks of P, which is used by $\mathit{RStabilize}()$, and in B.preE the list of blocks $C \in P$ such that $C \to^\exists B$. Finally, any block B stores in B.size the size of B, in B.count an integer counter bounded by $|P|$ which is used by $\mathit{PStabilize}()$ and a pair of boolean flags used for marking purposes. The current partition P is stored as a doubly linked list of blocks.

Relation: The current relation $\trianglelefteq$ on P is stored as a resizable $|P| \times |P|$ boolean matrix. Recall [8, Section 17.4] that insert operations in a resizable array (whose capacity is doubled as needed) take amortized constant time and that a resizable matrix (or table) can be implemented as a resizable array of resizable

```
Initialize() {
    // Initialize BCount
    forall B ∈ P do
        forall C ∈ P do  BCount(B, C) := 0;
    forall B ∈ P do
        forall x ∈ B do
            forall y ∈ post(x) do
                if (BCount(B, y.block) = 0) then BCount(B, y.block) := 1;
    // Initialize preE
    updatePreE(); // In Figure 5
    // Initialize Count
    forall B ∈ P do
        forall C ∈ P do  Count(B, C) := 0;
    forall D ∈ P do
        forall B ∈ D.preE do
            forall C ∈ P such that C ⊴ D do Count(B, C)++;
    // Initialize Rem
    forall C ∈ P do
        forall B ∈ P do
            forall D ∈ B.preE do
                if (Count(D, C) = 0) then Rem(C).append(D);
}
```

Figure 2: Initialization of data structures.

arrays. The boolean matrix $\trianglelefteq$ is resized by adding a new entry to $\trianglelefteq$, namely a new row and a new column, for any block B that is split into two new blocks $B \smallsetminus S$ and $B \cap S$. The old entry B becomes the entry for the new block $B \smallsetminus S$ while the new entry is used for the new block $B \cap S$.

Auxiliary Data Structures: We store and maintain a resizable boolean matrix BCount and a resizable integer matrix Count, both indexed over P, whose meanings are as follows:

$$\text{BCount}(B, C) \triangleq \begin{cases} 1 & \text{if } B{\to}^{\exists}C \\ 0 & \text{if } B \not\to^{\exists} C \end{cases}$$

$$\text{Count}(B, C) \triangleq \textstyle\sum_{E \trianglerighteq C} \text{BCount}(B, E)$$

Hence, Count(B, C) stores the number of blocks E such that $C \trianglelefteq E$ and $B{\to}^{\exists}E$. The table Count allows to implement the test $B \not\to^{\exists} \mathrm{pre}(\mu_{\mathcal{P}}(C))$ in constant time as Count$(B, C) = 0$.

The data structures BCount, preE, Count and Rem are initialized by a function *Initialize()* at line 2 of ESim, which is described in Figure 2.

4.2 Partition Stability

Our implementation of ESim will exploit the following logical characterization of partition refiners.

Theorem 4.1. *Let $\langle P, \trianglelefteq\rangle$ be a partial order PR. Then,* $\mathrm{PRefiner}(\langle P, \trianglelefteq\rangle) \neq \varnothing$ *iff there exist $B, C \in P$ such that the following three conditions hold:*

(i) $B{\to}^{\exists}C$;

```
list⟨State⟩ preμ(Block C) {
    list⟨State⟩ S := ∅;
    forall x ∈ Σ do
        forall y ∈ post(x) do
            if (C ⊴ y.block & unmarked(x)) then {S.append(x); mark(x);}
    forall x ∈ S do unmark(x);
    return S;
}
list⟨Block⟩ Split(list⟨State⟩ S) {
    list⟨Block⟩ split;
    forall B ∈ P do B.intersection := null;
    forall x ∈ S do
        if (x.block.intersection = null) then
            x.block.intersection := ff;
            Block B := new Block; x.block.brother := B;
            B.brother := x.block; B.intersection := tt;
            split.append(x.block);
        move x in list Σ from x.block at the end of B;
        if (x.block = ∅) then // x.block ⊆ S
            x.block.begin := B.begin; x.block.end := B.end;
            x.block.brother := null; x.block.intersection := null;
            split.remove(x.block); delete B;
    return split;
}
```

Figure 3: Split algorithm.

(ii) *for any* $C' \in P$*, if* $C \lhd C'$ *then* $B \not\to^{\exists} C'$*;*

(iii) $B \not\subseteq \mathrm{pre}(C)$.

Proof. Let $\mathcal{P} = \langle P, \unlhd \rangle$.
($\Leftarrow$) From condition (i) we have that $B \cap \mathrm{pre}(\mu_{\mathcal{P}}(C)) \neq \varnothing$. From conditions (ii) and (iii), $B \not\subseteq \mathrm{pre}(\mu_{\mathcal{P}}(C))$. Thus, $C \in \mathrm{PRefiner}(\mathcal{P})$.
($\Rightarrow$) Assume that $\mathrm{PRefiner}(\mathcal{P}) \neq \varnothing$. Since $\langle P, \unlhd \rangle$ is a partial order, we consider a partition refiner $C \in \max(\mathrm{PRefiner}(\mathcal{P}))$ which is maximal w.r.t. the partial order $\unlhd$. Since C is a partition refiner, there exists some $B \in P$ such that $B \cap \mathrm{pre}(\mu_{\mathcal{P}}(C)) \neq \varnothing$ and $B \not\subseteq \mathrm{pre}(\mu_{\mathcal{P}}(C))$. If $C' \in P$ is such that $C \lhd C'$ then C' cannot be a partition refiner because C is a maximal partition refiner. Hence, if $B \to^{\exists} C'$ then $B \subseteq \mathrm{pre}(\mu_{\mathcal{P}}(C'))$, because C' is not a partition refiner, so that, since $\mathrm{pre}(\mu_{\mathcal{P}}(C')) \subseteq \mathrm{pre}(\mu_{\mathcal{P}}(C))$, $B \subseteq \mathrm{pre}(\mu_{\mathcal{P}}(C))$, which is a contradiction. Hence, for any $C' \in P$ if $C \lhd C'$ then $B \not\to^{\exists} C'$. Therefore, from $B \cap \mathrm{pre}(\mu_{\mathcal{P}}(C)) \neq \varnothing$ we obtain that $B \to^{\exists} C$. Moreover, from $B \not\subseteq \mathrm{pre}(\mu_{\mathcal{P}}(C))$ we obtain that $B \not\subseteq \mathrm{pre}(C)$. ☐

Notice that this characterization of partition refiners requires that the current PR is a partial order relation and, by Lemma 3.2, for any call to $\mathit{PStabilize}()$, this is actually guaranteed by the ESim algorithm.

The algorithm in Figure 4 is an implementation of the $\mathit{PStabilize}()$ function that relies on Theorem 4.1 and on the above data structures. The function $\mathit{FindPRefiner}()$ implements the conditions of Theorem 4.1: it returns a partition refiner for the current PR $\mathcal{P} = \langle P, \unlhd \rangle$ when this exists, otherwise it returns a null pointer. Given a block $B \in P$, the function $\mathit{Post}(B)$ returns a list of blocks $C \in P$ that satisfy conditions (i) and (iii) of Theorem 4.1, i.e., those blocks C such that $B \to^{\exists} C$ and $B \not\subseteq \mathrm{pre}(C)$. This is accomplished through the counter C.count that at the exit of the for-loop at lines 18-23 in Figure 4 stores

```
1  bool PStabilize() {
2    list⟨Block⟩ split := ∅;
3    while (C := FindPRefiner()) ≠ null) do
4      list⟨State⟩ S := preμ(C);  split := Split(S);
5      updateRel(split);  updateBCount(split);  updatePreE();
6      updateCount(split);  updateRem(split);
7    return (split = ∅);
8  }

9  Block FindPRefiner() {
10   forall B ∈ P do
11     list⟨Block⟩ p := Post(B);
12     forall C ∈ p do
13       if (Count(B, C) = 1) then return C;
14   return null;
15 }

16 list⟨Block⟩ Post(Block B) {
17   list⟨Block⟩ p := ∅;
18   forall b ∈ B, do
19     forall c ∈ post(b) do
20       Block  C := c.block;
21       if unmarked1(C) then  {mark1(C); C.count = 0; p.append(C);}
22       if unmarked2(C) then  {mark2(C); C.count++;}
23     forall C ∈ p do  unmark2(C);
24   forall C ∈ p do
25     unmark1(C);
26     if (C.count = B.size) then p.remove(C);}
27   return p;
28 }
```

Figure 4: $\mathit{PStabilize}()$ Algorithm.

the number of states in B having (at least) an outgoing transition to C, i.e., C.count $= |B \cap \mathrm{pre}(C)|$. Hence, we have that:

$$B{\to}^{\exists}C \text{ and } B \not\subseteq \mathrm{pre}(C) \;\Leftrightarrow\; 1 \leq C.\text{count} < B.\text{size}.$$

Then, for any candidate partition refiner $C \in \mathit{Post}(B)$, it remains to check condition (ii) of Theorem 4.1. This condition is checked in $\mathit{FindPRefiner}()$ by testing whether Count$(B, C) = 1$: this is correct because Count$(B, C) \geq 1$ holds since $C \in \mathit{Post}(B)$ and therefore $B{\to}^{\exists}C$, so that

$$\text{Count}(B, C) = 1 \;\text{ iff }\; \forall C' \in P. C \lhd C' \Rightarrow B \not\to^{\exists} C'.$$

Hence, if Count$(B, C) = 1$ holds at line 13 of $\mathit{FindPRefiner}()$, by Theorem 4.1, C is a partition refiner. Once a partition refiner C has been returned by $\mathit{Post}(B)$, $\mathit{PStabilize}()$ splits the current partition P w.r.t. the splitter $S = \mathrm{pre}(\mu_{\mathcal{P}}(C))$ by calling the function $\mathit{Split}(S)$, updates the relation $\trianglelefteq$ as defined by equation (†) in Section 3 by calling $\mathit{updateRel}()$, updates the data structures BCount, preE, Count and Rem, and then check again whether a partition refiner exists. At the exit of the main while-loop of $\mathit{PStabilize}()$, the current PR $\langle P, \trianglelefteq \rangle$ is partition stable.

$\mathit{PStabilize}()$ calls the functions pre$\mu()$ and $\mathit{Split}()$ in Figure 3. Recall that the states of a block B of P are consecutive in the list of states Σ, so that B is represented as $B = [B.\text{begin}, B.\text{end}[$. The implementation of $\mathit{Split}(S)$ is quite standard (see e.g. [13, 22]): this is based on a linear scan of the states in S and for each state in S performs some constant time operations. Hence, $\mathit{Split}(S)$ takes $O(|S|)$ time. Also, $\mathit{Split}(S)$ returns the list *split* of blocks $B \smallsetminus S$ such that $\varnothing \subsetneq B \smallsetminus S \subsetneq B$ (i.e., B.intersection = **ff**).

Let us remark that a call $Split(S)$ may affect the ordering of the states in the list Σ because states are moved from old blocks to newly generated blocks.

We will show that the overall time complexity of $PStabilize()$ along a whole run of ESim is in $O(|P_{\mathrm{sim}}||{\rightarrow}|)$.

```
updateRel(list⟨Block⟩ split) {
  forall B ∈ split do addNewEntry(B) in matrix ⊴;
  forall B ∈ P do
    forall C ∈ split do
      if (B.intersection = tt) then  B ⊴ C := B.brother ⊴ C.brother;
      else B ⊴ C := B ⊴ C.brother;
  forall C ∈ P do
    forall B ∈ split do
      if (C.intersection = ff) then  B ⊴ C := B.brother ⊴ C;
}
updateBCount(list⟨Block⟩ split) {
  forall B ∈ split do addNewEntry(B) in matrix Count;
  forall B ∈ P do
    forall x ∈ B do
      forall y ∈ post(x) do  BCount(B, y.block) := 0;
  forall B ∈ P do
    forall x ∈ B do
      forall y ∈ post(x) do
        if (BCount(B, y.block) = 0) then BCount(B, y.block) := 1;
}
updatePreE() {
  forall B ∈ P do B.preE := ∅;
  forall B ∈ P do
    forall x ∈ B do
      forall y ∈ post(x) do  {unmark(B);  y.block.preE.append(B);}
  forall C ∈ P do
    forall B ∈ C.preE do
      if unmarked(B) then mark(B);
      else C.preE.remove(B);
    forall B ∈ C.preE do unmark(B);
}
updateRem(list⟨Block⟩ split) {
  forall B ∈ split do  Rem(B) := Rem(B.brother);
}
```

Figure 5: Update functions.

4.3 Updating Data Structures

In the function $PStabilize()$, after calling $Split(S)$, firstly we need to update the boolean matrix that stores the relation $\trianglelefteq$ in accordance with definition (†) in Section 3. After that, since both P and $\trianglelefteq$ are changed we need to update the data structures BCount, preE, Count and Rem. The implementations of the functions *updateRel*(), *updateBCount*(), *updatePreE*() and *updateRem*() are quite straightforward and are described in Figure 5.

The function *updateCount*() is in Figure 6 and deserves special care in order to design a time efficient implementation. The core of the *updateCount*() algorithm follows Hopcroft's "process the smaller half" principle [16] for updating the integer matrix Count. Let P' be the partition which is obtained by splitting the partition P w.r.t. the splitter S. Let B be a block of P that has been split into $B \cap S$ and $B \smallsetminus S$. Thus, we need to update Count($B \cap S, C$) and Count($B \smallsetminus S, C$) for any $C \in P'$ by knowing Count($B, \mathrm{parent}_P(C)$). Let us first observe that after lines 3-10 of $updateCount()$, we have that for any $B, C \in P'$, Count(B, C) $=$ Count($\mathrm{parent}_P(B), \mathrm{parent}_P(C)$). Let X be the block in $\{B \cap S, B \smallsetminus S\}$ with the smaller size, and let Z be the other block, so that $|X| \leq |B|/2$ and $|X| + |Z| = |B|$. Let C be any block in P'. We set Count(X, C) to 0, while Count(Z, C) is left unchanged, namely Count(Z, C) $=$ Count(B, C). We can correctly update both Count(Z, C) and Count(X, C) by just scanning all the outgoing transitions from X. In fact, if $x \in X$, $x \to y$ and the block $P(y)$ is scanned for the first time then for all $C \trianglelefteq P(y)$, Count(X, C) is incremented by 1, while if $Z \not\to^{\exists} P(y)$, i.e. BCount($Z, P(y)$) $= 0$, then Count(Z, C) is decremented by 1. The correctness of this procedure goes as follows:

(1) At the end, Count(X, C) is clearly correct because its value has been re-computed from scratch.

(2) At the end, Count(Z, C) is correct because Count(Z, C) initially stores the value Count(B, C), and if there exists some block D such that $C \trianglelefteq D$, $B \to^{\exists} D$ whereas $Z \not\to^{\exists} D$ — this is correctly implemented at line 28 as BCount(Z, D) $= 0$, since the date structure BCount is up to date — then necessarily $X \to^{\exists} D$, because B has been split into X and Z, so that $D = P(y)$ for some $y \in \mathrm{post}(X)$, namely D has been taken into account by some increment Count(X, C)++ and consequently Count(Z, C) is decremented by 1 at line 28.

Moreover, if some block $D \in P' \smallsetminus \{B \cap S, B \smallsetminus S\}$ is such that both $D \to^{\exists} X$ and $D \to^{\exists} Z$ hold then for all the blocks $C \in P$ such that $C \trianglelefteq X$ (or, equivalently, $C \trianglelefteq Z$), we need to increment Count(D, C) by 1. This is done at lines 30-32 by relying on the updated date structures preE and BCount.

Let us observe that the time complexity of a single call of *updateCount*($split$) is

$$|P|\big(|split| + \sum_{X \in split} \big(|\{(x,y) \mid x \in X, y \in \Sigma, x \to y\}| + |\{(X,D) \mid D \in P, X \to^{\exists} D\}|\big)\big).$$

Hence, let us calculate the overall time complexity of *updateCount*(). If X and X' are two blocks that are scanned in two different calls of *updateCount* and $X' \subseteq X$ then $|X'| \leq |X|/2$. Consequently, any transition $x \to y$ at line 23 and $D \to^{\exists} X$ at line 30 can be scanned in some call of *updateCount*() at most $\log_2 |\Sigma|$ times. Thus, the overall time complexity of *updateCount*() is in $O(|P_{\mathrm{sim}}||{\to}| \log |\Sigma|)$.

4.4 Relation Stability

The logical procedure $RStabilize()$ in Figure 1 is implemented by the algorithm in Figure 7. Let $\mathcal{P}^{\mathrm{in}} = \langle P, \trianglelefteq^{\mathrm{in}} \rangle$ be the current PR when calling $RStabilize()$. For each relation refiner $C \in P$, the function $RStabilize()$ must iteratively refine the initial relation $\trianglelefteq^{\mathrm{in}}$ in accordance with equation (‡) in Section 3. Hence, if $B \to^{\exists} C$, $B \trianglelefteq D$ and $D \not\to^{\exists} \mu_{\mathcal{P}^{\mathrm{in}}}(C)$, the entry $B \trianglelefteq D$ of the boolean matrix that represents the relation $\trianglelefteq$ must be set to **ff**. Thus, the idea is to store and incrementally maintain for each block $C \in P$ a list $Rem(C)$ of blocks $D \in P$ such that:

(A) If C is a relation refiner for $\mathcal{P}^{\mathrm{in}}$ then $Rem(C) \neq \varnothing$;

(B) If $D \in Rem(C)$ then necessarily $D \not\to^{\exists} \mu^{\mathrm{in}}_{\mathcal{P}}(C)$.

It turns out that C is a relation refiner for $\mathcal{P}^{\mathrm{in}}$ iff there exist blocks B and D such that $B \to^{\exists} C$, $D \in Rem(C)$ and $B \trianglelefteq D$. Hence, the set of blocks $Rem(C)$ is reminiscent of the set of states $remove(s)$ used in Henzinger et al.'s [14] simulation algorithm, since each pair (B, D) which must be removed from

```
// Precondition: BCount and preE are updated with the current PR
updateCount(list⟨Block⟩ split) {
  forall B ∈ split do addNewEntry(B) in matrix Count;
  forall B ∈ P do
    forall C ∈ split do
      if (B.intersection = tt) then Count(B, C) := Count(B.brother, C.brother);
      else Count(B, C) := Count(B, C.brother);
  forall C ∈ P do
    forall B ∈ split do
      if (C.intersection = ff) then Count(B, C) := Count(B.brother, C);
  forall C ∈ P do unmark(C);
  forall B ∈ split do
    // Update Count(B, ·) and Count(B.brother, ·)
    Block X, Z;
    if (B.size ≤ B.brother.size) then
      {X := B; Z := B.brother;}
    else
      {X := B.brother; Z := B;}
    forall C ∈ P do
      Count(X, C) := 0;
      // Count(Z, C) := Count(B, C);
    forall x ∈ X do
      forall y ∈ post(x) do
        if unmarked(y.block) then
          mark(y.block);
          forall C ∈ P such that C ⊴ y.block do
            Count(X,C)++;
            if (BCount(Z, y.block) = 0) then Count(Z,C)−−;
    // For all D ∉ {B, B.brother}, updateCount(D, ·)
    forall D ∈ X.preE do
      if (D ≠ X & D ≠ Z & BCount(D, Z) = 1) then
        forall C ∈ P such that C ⊴ X do Count(D, C)++;
}
```

Figure 6: *updateCount*() function.

the relation $\trianglelefteq$ is such that $D \in Rem(C)$, for some block C.

Initially, namely at the first call of $RStabilize()$ by ESim, $Rem(C)$ is set by the function *Initialize*() to $\{D \in P \mid D {\to}^{\exists} \Sigma,\ D {\not\to}^{\exists} \mu_{\mathcal{P}}(C)\}$. Hence, $RStabilize()$ scans all the blocks in the current partition P and selects those blocks C such that $Rem(C) \neq \varnothing$, which are therefore candidate to be relation refiners. Then, by scanning all the blocks $B \in C$.preE and $D \in Rem(C)$, if $B \trianglelefteq D$ holds then the entry $B \trianglelefteq D$ must be set to **ff**. However, the removal of the pair (B, D) from the current relation $\trianglelefteq$ may affect the function $\mu_{\mathcal{P}}$. This is avoided by making a copy $oldRem(C)$ of all the $Rem(C)$'s at the beginning of $RStabilize()$ and then using this copy. During the main for-loop of $RStabilize()$, $Rem(C)$ must satisfy the following invariant property:

$$\text{(Inv)}:\ \forall C \in P.\, Rem(C) = \{D \in P \mid D {\to}^{\exists} \mu_{\mathcal{P}}^{\mathrm{in}}(C),\ D {\not\to}^{\exists} \mu_{\mathcal{P}}(C)\}.$$

This means that at the beginning of $RStabilize()$, any $Rem(C)$ is set to empty, and after the removal of a pair (B, D) from $\trianglelefteq$, since $\mu_{\mathcal{P}}(B)$ has changed, we need: (i) to update the matrix Count, for all the entries (F, B) where $F {\to}^{\exists} D$, and (ii) to check if there is some block F such that $F {\not\to}^{\exists} \mu_{\mathcal{P}}(B)$, because any such

```
1  bool RStabilize() {
2    // μ_P^in := μ_P;
3    forall C ∈ P do {oldRem(C) := Rem(C); Rem(C) = ∅;}
4    bool Removed := ff;
5    forall C ∈ P such that oldRem(C) ≠ ∅ do
6      // Invariant (Inv): ∀C ∈ P. Rem(C) = {D ∈ P | D →∃ μ_P^in(C), D ↛∃ μ_P(C)}
7      forall B ∈ C.preE do
8        forall D ∈ oldRem(C) do
9          if (B ⊴ D) then
10           B ⊴ D := ff; Removed := tt;
11           // update Count and Rem
12           forall F ∈ D.preE do
13             Count(F, B) := Count(F, B)−1;
14             if (Count(F, B) = 0 & Rem(B) = ∅) then // F →∃ μ_P^in(B) & F ↛∃ μ_P(B)
15               Rem(B).append(F);
16 }
```

Figure 7: $RStabilize()$ algorithm.

F must be added to $Rem(B)$ in order to maintain the invariant property (Inv).

4.5 Complexity

The time complexity of the algorithm ESim relies on the following key properties:

(1) The overall number of partition refiners found by ESim is in $O(|P_{\mathrm{sim}}|)$. Moreover, the overall number of newly generated blocks by the splitting operations performed by calling $Split(S)$ at line 4 of $PStabilize()$ is in $O(|P_{\mathrm{sim}}|)$. In fact, let $\{P_i\}_{i\in[0,n]}$ be the sequence of different partitions computed by ESim where P_0 is the initial partition P_ℓ, P_n is the final partition P_{sim} and for all $i \in [1, n]$, P_i is the partition after the i-th call to $Split(S)$, so that $P_i \prec P_{i-1}$. The number of new blocks which are produced by a call $Split(S)$ that refines P_i to P_{i+1} is $2(|P_{i+1}| - |P_i|)$. Thus, the overall number of newly generated blocks is $\sum_{i=1}^{n} 2(|P_i|-|P_{i-1}|) = 2(|P_{\mathrm{sim}}|-|P_\ell|) \in O(|P_{\mathrm{sim}}|)$.

(2) The invariant (Inv) of the sets $Rem(C)$ guarantees the following property: if C_1 and C_2 are two blocks that are selected by the for-loop at line 5 of $RStabilize()$ in two different calls of $RStabilize()$, and $C_2 \subseteq C_1$ (possibly $C_1 = C_2$) then $(\cup Rem(C_1)) \cap (\cup Rem(C_2)) = \varnothing$.

Theorem 4.2. ESim *runs in* $O(|P_{\mathrm{sim}}|^2 \log |P_{\mathrm{sim}}| + |\Sigma| \log |\Sigma|)$*-space and* $O(|P_{\mathrm{sim}}||{\rightarrow}| \log |\Sigma|)$*-time.*

Proof. ***Space Complexity.*** The input transition system is represented by the post relation, so that the size of post is not taken into account in the space complexity of ESim. The doubly linked list of states take $O(|\Sigma| \log |\Sigma|)$ while the pointers s.block take $O(|\Sigma| \log |P_{\mathrm{sim}}|)$. The partition P and the pointers stored in each block of P overall take $O(|P_{\mathrm{sim}}| \log |\Sigma|)$. The binary relation $\trianglelefteq$ takes $O(|P_{\mathrm{sim}}|^2)$. The auxiliary data structures Rem, preE and BCount overall take $O(|P_{\mathrm{sim}}|^2)$, while the integer matrix Count takes $O(|P_{\mathrm{sim}}|^2 \log |P_{\mathrm{sim}}|)$. Hence, the overall bit space complexity for storing the above data structures is $O(|P_{\mathrm{sim}}|^2 \log |P_{\mathrm{sim}}| + |\Sigma| \log |\Sigma|)$.

Time Complexity. The time complexity bound of ESim is shown by the following points.

(A) The initialization function *Initialize* takes $|P|^2 + |{\rightarrow}| + |P||\{(B, D) \mid B, D \in P,\ B \rightarrow^{\exists} D\}|$ time. Observe that $|P| \leq |P_{\mathrm{sim}}| \leq |{\rightarrow}|$ so that the time complexity of *Initialize* is in $O(|P_{\mathrm{sim}}||{\rightarrow}|)$.

(B) A call to $\mathrm{pre}\mu(C)$ takes $O(|{\rightarrow}|)$ time. A call to $Split(S)$ takes $|S|$ time. Since S is returned by $\mathrm{pre}\mu(C)$, $|S| \leq |{\rightarrow}|$ holds so that the time complexity of a call to $Split(S)$ is in $O(|{\rightarrow}|)$. A call to *Post*(B) takes $|\{(b, c) \mid b \in B, c \in \Sigma, b{\rightarrow}c\}|$ time, so that a call to *FindPRefiner* takes $O(|{\rightarrow}|)$ time. Moreover, let us observe that *FindPRefiner* returns **null** just once, because when *FindPRefiner* returns **null** the current PR of ESim is both partition and relation stable and therefore ESim terminates and outputs that PR. Consequently, since, by point (1) above, the overall number of partition refiners is in $O(|P_{\mathrm{sim}}|)$, the overall number of function calls for *FindPRefiner* is in $O(|P_{\mathrm{sim}}|)$ and, in turn, the overall time complexity of *FindPRefiner* is in $O(|P_{\mathrm{sim}}||{\rightarrow}|)$ time. Also, the overall time complexity of $\mathrm{pre}\mu(C)$ and $Split(S)$ is in $O(|P_{\mathrm{sim}}||{\rightarrow}|)$.

(C) Let us observe that the calls *updateRel*$(split)$ and *updateRem*$(split)$ take $O(|P||split|)$ time, while *updatePreE*$()$ and *updateBCount*$(split)$ take $O(|{\rightarrow}|)$ time. Since the overall number of calls for these functions is in $O(|P_{\mathrm{sim}}|)$ and since $\sum_{i \in \text{Iterations}} |split_i|$ is in $O(|P_{\mathrm{sim}}|)$, it turns out that their overall time complexity is in $O(|P_{\mathrm{sim}}|(|P_{\mathrm{sim}}| + |{\rightarrow}|))$, so that, since $|P_{\mathrm{sim}}| \leq |{\rightarrow}|$, it is in $O(|P_{\mathrm{sim}}||{\rightarrow}|)$. Moreover, as already shown in Section 4.3, the overall time complexity of *updateCount*$(split)$ is in $O(|P_{\mathrm{sim}}||{\rightarrow}| \log |\Sigma|)$.

(D) Hence, by points (B) and (C), the overall time complexity of $PStabilize()$ is in $O(|P_{\mathrm{sim}}||{\rightarrow}| \log |\Sigma|)$.

(E) Let $C \in P_{\mathrm{in}}$ be some block of the initial partition and let $\langle C_i \rangle_{i \in I_C}$, for some set of indices I_C, be a sequence of blocks selected by the for-loop at line 5 of $RStabilize()$ such that: (a) for any $i \in I_C$, $C_i \subseteq C$ and (b) for any i, C_{i+1} has been selected after C_i and C_{i+1} is contained in C_i. Observe that C is the parent block in P_{in} of all the C_i's. Then, by the property (2) above, it turns out that the corresponding sets in $\{\cup Rem(C_i)\}_{i \in I_C}$ are pairwise disjoint so that $\sum_{i \in I_C} |\,Rem(C_i)| \leq |P_{\mathrm{sim}}|$. This property guarantees that if $D \in oldRem(C_i)$ at line 8 then for all the blocks $D' \subseteq D$ and for any $j \in I_C$ such that $i < j$, $D' \notin oldRem(C_j)$. Moreover, if the test $B \trianglelefteq D$ at line 9 is true for some iteration k, so that $B \trianglelefteq D$ is set to **ff**, then for all the blocks D' and B' such that $D' \subseteq D$ and $B' \subseteq B$ the test $D' \trianglelefteq B'$ will be always false for all the iterations which follow k. From these observations, we derive that the overall time complexity of the code of the for-loop at lines 7-10 is $\sum_C \sum_{i \in I_C} \sum_{B \rightarrow^{\exists} C} |\,Rem(C_i)| \leq |P_{\mathrm{sim}}||\{(B, C) \mid B, C \in P_{\mathrm{sim}}, B{\rightarrow}^{\exists}C\}| \leq |P_{\mathrm{sim}}||{\rightarrow}|$. Moreover, the overall time complexity of the code of the for-loop at lines 12-15 is $\sum_B \sum_D \sum_{F \rightarrow^{\exists} D} 1 \leq |P_{\mathrm{sim}}||\{(F, D) \mid F, D \in P_{\mathrm{sim}}, F{\rightarrow}^{\exists}D\}| \leq |P_{\mathrm{sim}}||{\rightarrow}|$. We also observe that the overall time complexity of the for-loop at line 3 of $RStabilize()$ is in $O(|P_{\mathrm{sim}}|^2)$. Thus, the overall time complexity of $RStabilize()$ is in $O(|P_{\mathrm{sim}}|(|P_{\mathrm{sim}}| + |{\rightarrow}|))$, so that, since $|P_{\mathrm{sim}}| \leq |{\rightarrow}|$, it is in $O(|P_{\mathrm{sim}}||{\rightarrow}|)$.

Summing up, by points (A), (D) and (E), we have shown that the overall time complexity of ESim is in $O(|P_{\mathrm{sim}}||{\rightarrow}| \log |\Sigma|)$. ☐

5 Conclusion and Further Work

We have introduced a new algorithm, called ESim, for efficiently computing the simulation preorder which: (i) reaches the space bound of the simulation algorithm GPP [10, 11] — which has the best space complexity — while significantly improving its time bound; (ii) significantly improves the space bound of the simulation algorithm RT [20, 22] — which has the best time complexity — while closely approching its time bound. Moreover, the space complexity of ESim is quasi-optimal, meaning that it differs only for logarithmic factors from the size of the output.

We see a couple of interesting avenues for further work. A first natural question arises: can the time complexity of ESim be further improved and reaches the time complexity of RT? This would require to eliminate the multiplicative factor $\log |\Sigma|$ from the time complexity of ESim and, presently, this seems to us quite hard to achieve. More in general, it would be interesting to investigate whether some lower space and time bounds can be stated for the simulation preorder problem. Secondly, ESim is designed for Kripke structures. While an adaptation of a simulation algorithm from Kripke structures to labeled transition systems (LTSs) can be conceptually simple, unfortunately such a shift may lead to some loss in both space and time complexities, as argued in [5]. We mention the works [1, 15] and [17] that provide simulation algorithms for LTSs by adapting, respectively, RT and GPP. It is thus worth investigating whether and how ESim can be efficiently adapted to work with LTSs.

Acknowledgements. We acknowledge the contribution of Francesco Tapparo to a preliminary stage of this research which was informally presented in [21]. This work was partially supported by Microsoft Research SEIF 2013 Award and by the University of Padova under the project BECOM.

References

[1] P.A. Abdulla, A, Bouajjani, L. Holík, L. Kaati and T. Vojnar. Computing simulations over tree automata. In *Proc. 14th Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'08)*, LNCS 4963, pp. 93–108, 2008.

[2] B. Bloom. *Ready simulation, bisimulation, and the semantics of CCS-like languages*. Ph.D. thesis, Massachusetts Institute of Technology, 1989.

[3] B. Bloom and R. Paige. Transformational design and implementation of a new efficient solution to the ready simulation problem. *Sci. Comp. Program.*, 24(3):189-220, 1995.

[4] D. Bustan and O. Grumberg. Simulation-based minimization. *ACM Trans. Comput. Log.*, 4(2):181-204, 2003.

[5] G. Cécé. Three simulation algorithms for labelled transition systems. Preprint cs.arXiv:1301.1638, arXiv.org, 2013.

[6] E.M. Clarke, O. Grumberg and D.A. Peled. *Model Checking*. The MIT Press, 1999.

[7] R. Cleaveland, J. Parrow and B. Steffen. The concurrency workbench: A semantics based tool for the verification of concurrent systems. *ACM Trans. Program. Lang. Systems*, 15(1):36-72, 1993.

[8] T.H. Cormen, C.E. Leiserson, R.L. Rivest and C. Stein. *Introduction to Algorithms*. The MIT Press and McGraw-Hill, 2nd ed., 2001.

[9] S. Crafa, F. Ranzato and F. Tapparo. Saving space in a time efficient simulation algorithm. *Fundam. Inform.*, 108(1-2):23-42, 2011.

[10] R. Gentilini, C. Piazza and A. Policriti. Simulation as coarsest partition problem. In *Proc. Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'02)*, LNCS 2280, pp. 415-430, 2002.

[11] R. Gentilini, C. Piazza and A. Policriti. From bisimulation to simulation: coarsest partition problems. *J. Automated Reasoning*, 31(1):73-103, 2003.

[12] R. van Glabbeek and B. Ploeger. Correcting a space-efficient simulation algorithm. In *Proc. 20th Int. Conf. on Computer Aided Verification (CAV'08)*, LNCS 5123, pp. 517-529, 2008.

[13] J.F. Groote and F. Vaandrager. An efficient algorithm for branching bisimulation and stuttering equivalence. In *Proc. 17th ICALP*, LNCS 443, pp. 626-638, 1990.

[14] M.R. Henzinger, T.A. Henzinger and P.W. Kopke. Computing simulations on finite and infinite graphs. In *Proc. 36th IEEE FOCS*, 453-462, 1995.

[15] L. Holík and J. Šimáček. Optimizing an LTS-simulation algorithm. *Computing and Informatics*, 29(6+):1337-1348, 2010.

[16] J.E. Hopcroft. A $n \log n$ algorithm for minimizing states in a finite automaton. In Z. Kohavi and A. Paz eds., *Theory of Machines and Computations*, pp. 189-176, Academic Press, 1971.

[17] J. Markovski. Saving time in a space-efficient simulation algorithm. In *Proc. 11th Int. Conf. on Quality Software*, pp. 244-251, IEEE, 2011.

[18] R. Paige and R.E. Tarjan. Three partition refinement algorithms. *SIAM J. Comput.*, 16(6):973-989, 1987

[19] F. Ranzato. A more efficient simulation algorithm on Kripke structures. In *Proceedings of the 38th International Symposium on Mathematical Foundations of Computer Science (MFCS'13)*, LNCS 8087, pp. 753-764, Springer, 2013.

[20] F. Ranzato and F. Tapparo. A new efficient simulation equivalence algorithm. In *Proc. 22nd Annual IEEE Symp. on Logic in Computer Science (LICS'07)*, pp. 171-180, 2007.

[21] F. Ranzato and F. Tapparo. A time and space efficient simulation algorithm. Short talk at *24th Annual IEEE Symposium on Logic in Computer Science (LICS'09)*, 2009.

[22] F. Ranzato and F. Tapparo. An efficient simulation algorithm based on abstract interpretation. *Inf. Comput.*, 208(1):1-22, 2010.

[23] L. Tan and R. Cleaveland. Simulation revisited. In *Proc. 7th Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'01)*, LNCS 2031, pp. 480-495, 2001.