BRICS

Basic Research in Computer Science

BRICS RS-00-16 J. Srba: Complexity of Weak Bisimilarity and Regularity for BPA and BPP

Complexity of Weak Bisimilarity and Regularity for BPA and BPP

Jiří Srba

BRICS Report Series RS-00-16

ISSN 0909-0878 June 2000

See back inner page for a list of recent BRICS Report Series publications. Copies may be obtained by contacting:

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK–8000 Aarhus C
Denmark
Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

`http://www.brics.dk`
`ftp://ftp.brics.dk`
This document in subdirectory `RS/00/16/`

Complexity of Weak Bisimilarity and Regularity for BPA and BPP

Jiří Srba

BRICS[⋆]
Department of Computer Science
University of Aarhus
Ny Munkegade bld. 540
DK-8000 Aarhus C, Denmark
srba@brics.dk

Abstract. It is an open problem whether weak bisimilarity is decidable for Basic Process Algebra (BPA) and Basic Parallel Processes (BPP). A *PSPACE* lower bound for BPA and *NP* lower bound for BPP have been demonstrated by Stribrna. Mayr achieved recently a result, saying that weak bisimilarity for BPP is Π_2^P-hard. We improve this lower bound to *PSPACE*, moreover for the restricted class of *normed* BPP.
Weak regularity (finiteness) of BPA and BPP is not known to be decidable either. In the case of BPP there is a Π_2^P-hardness result by Mayr, which we improve to *PSPACE*. No lower bound has previously been established for BPA. We demonstrate *DP*-hardness, which in particular implies both *NP* and *co-NP*-hardness.
In each of the bisimulation/regularity problems we consider also the classes of normed processes.

Keywords: BPA, BPP, weak bisimulation, weak regularity, complexity

1 Introduction

An intensive study of a variety of process algebras based on the interleaving model of CCS (see [Mil89]) has taken place in the last couple of years. Lots of activity has been focused on the analysis of infinite state systems. The two central questions are decidability and complexity of certain behavioural equivalences (for a survey see [Mol96]) and verification of system properties expressed in suitable logics (for a survey see [BE97]).

[⋆] Basic Research in Computer Science,
Centre of the Danish National Research Foundation.

In this paper we address the first question with a special focus on the bisimulation equivalence. *Strong bisimulation equivalence* is known to be decidable for the classes of Basic Process Algebra (BPA) [CHS95] and Basic Parallel Processes (BPP) [CHM93]. If we restrict ourself to *normed* processes, there are even polynomial time algorithms for bisimilarity of BPA and BPP [HJM96a,HJM96b].

However, we draw our attention towards the notion of *weak bisimilarity*, which is a more general equivalence than strong bisimilarity, in the sense that it allows to abstract from internal behaviour of processes by introducing a *silent action* τ, which is not observable [Mil89].

Decidability of weak bisimulation equivalence and weak regularity (finiteness) for BPA and BPP are well known open problems. There are partial results, e.g. by Hirshfeld [Hir96], showing decidability of weak bisimilarity for restricted classes of so called *totally normed* BPA and BPP. Stribrna proved in [Str98] *NP*-hardness for these restricted classes. Also, some results are known about weak bisimilarity of BPA/BPP with finite state systems [JKM98,KM99]. In spite of the fact that weak bisimilarity and regularity are not known to be decidable, only a few lower bounds have been found.

For weak bisimilarity in the BPA class, *PSPACE*-hardness was proved by Stribrna [Str98], using a reduction from *totality problem for finite nondeterministic automata*. No lower bound has previously been established for weak regularity in this class.

In the class of BPP, weak bisimilarity appeared to be *NP*-hard [Str98]. This result was recently improved by Mayr [May00a] to Π_2^P (in polynomial hierarchy). In the same paper, Π_2^P-hardness for weak regularity is proved.

Our contribution. We show *PSPACE*-hardness of weak bisimilarity for BPP, thus improving the Π_2^P-hardness result by Mayr, and moreover we prove our result for the restricted class of *normed* BPP. This result can be transformed to weak regularity for BPP, thus achieving *PSPACE* lower bound (again even for normed processes).

For the class of BPA we prove *DP*-hardness of weak regularity, which in particular means both *NP* and *co-NP*-hardness. Moreover *NP*-hardness can be transformed to the normed case.

All these results hold also for PA (Process Algebra [BW90]), which is a natural "union" of BPA and BPP, where we are allowed to use both sequential and parallel composition.

2 Basic definitions

Let $\mathcal{A}ct$ and $\mathcal{C}onst$ be countable sets of *actions* and *process constants* such that $\mathcal{A}ct \cap \mathcal{C}onst = \emptyset$. Moreover suppose that $\mathcal{A}ct$ contains a distinguishable *silent action* τ. Let $Op \subseteq \{.\ , ||\}$. We define the class of *process expressions over Op* as

$$E_{Op} ::= \epsilon \mid X \mid E \otimes E$$

where ϵ is the *empty process*, X ranges over $\mathcal{C}onst$ and $\otimes$ ranges over Op. The operator '.' is a *sequential composition*, and '$||$' stands for a *parallel composition*. In what follows we will not distinguish between process expressions related by a *structural congruence*, which is the smallest congruence over process expressions such that the following lows hold:

- '.' is associative
- '$||$' is associative and commutative
- 'ϵ' is a unit for '.' and '$||$'.

In this paper we consider the class of PA (Process Algebra [BW90]) expressions $E_{\{.,\ ||\}}$ and its natural subclasses; BPA (Basic Process Algebra, also known as context-free processes) expressions $E_{\{.\}}$ with only sequential composition; and BPP (Basic Parallel Processes) expressions $E_{\{||\}}$ with only parallel composition.
A *PA (resp. BPA or BPP) process rewrite system* (PRS) [May00b] is a finite set Δ of *rules* of the form $X \xrightarrow{a} E$, where $X \in \mathcal{C}onst$, $a \in \mathcal{A}ct$ and $E \in E_{\{.,\ ||\}}$ (resp. $E \in E_{\{.\}}$ or $E \in E_{\{||\}}$). Let us denote the set of actions and process constants that appear in Δ as $\mathcal{A}ct(\Delta)$ resp. $\mathcal{C}onst(\Delta)$ (note that these sets are finite). A process rewrite system Δ determines a *transition system* [Plo81,Mol96] where the states are process expressions over $\mathcal{C}onst(\Delta)$, and $\mathcal{A}ct(\Delta)$ is the set of labels. The *transition relation* is the least relation satisfying the following SOS rules (recall that '$||$' is commutative).

$$\frac{(X \xrightarrow{a} E) \in \Delta}{X \xrightarrow{a} E} \qquad \frac{E \xrightarrow{a} E'}{E.F \xrightarrow{a} E'.F} \qquad \frac{E \xrightarrow{a} E'}{E||F \xrightarrow{a} E'||F}$$

As usual we extend the transition relation to the elements of $\mathcal{A}ct^*$. We also write $E \longrightarrow^* E'$, whenever $E \xrightarrow{w} E'$ for some $w \in \mathcal{A}ct^*$. A state E' is *reachable from a state* E iff $E \longrightarrow^* E'$.
A *weak transition relation* is defined as follows.

$$\overset{a}{\Longrightarrow} \overset{\text{def}}{=} \begin{cases} \xrightarrow{\tau^*} \circ \xrightarrow{a} \circ \xrightarrow{\tau^*} & \text{if } a \neq \tau \\ \qquad \xrightarrow{\tau^*} & \text{if } a = \tau \end{cases}$$

We define a *process* as a pair (P, Δ), where P is a process expression and Δ is a process rewrite system. *States* of (P, Δ) are the states of the corresponding transition system. We say that a state E is *reachable* iff $P \longrightarrow^* E$. Whenever (P, Δ) has only finitely many reachable states, we call it a *finite-state process*.
Important subclasses of process algebras can be obtained by an extra restriction on the involved processes - *normedness*. A process expression E is *normed* iff there is $w \in \mathcal{A}ct^*$ such that $E \xrightarrow{w} \epsilon$. A process (P, Δ) is normed if all its process constants $\mathcal{C}onst(\Delta)$ are normed. We say that (P, Δ) is *totally normed* iff it is normed and moreover there is no transition $X \overset{\tau}{\Longrightarrow} \epsilon$ for any $X \in \mathcal{C}onst(\Delta)$.
Now we will introduce the concept of *weak bisimilarity* [Par81,Mil89]. A binary relation R over process expressions is a *weak bisimulation* iff whenever $(E, F) \in R$ then for each $a \in \mathcal{A}ct$:

- if $E \overset{a}{\Longrightarrow} E'$ then $F \overset{a}{\Longrightarrow} F'$ and $(E', F') \in R$
- if $F \overset{a}{\Longrightarrow} F'$ then $E \overset{a}{\Longrightarrow} E'$ and $(E', F') \in R$.

Processes (P_1, Δ_1) and (P_2, Δ_2) are *weakly bisimilar*, and we write $(P_1, \Delta_1) \approx (P_2, \Delta_2)$, iff there is a weak bisimulation R such that $(P_1, P_2) \in R$. Note that without loss of generality we can suppose that $\Delta_1 = \Delta_2$ since we can always consider a disjoint union of Δ_1 and Δ_2 as a new Δ.
Bisimulation equivalence has an elegant characterisation in terms of *bisimulation games* [Tho93,Sti95]. A bisimulation game on a pair of processes (P_1, Δ) and (P_2, Δ) is a two-player game of an 'attacker' and a 'defender'. The attacker chooses one of the processes and makes an $\overset{a}{\Longrightarrow}$-move for some $a \in \mathcal{A}ct(\Delta)$. The defender must respond by making an $\overset{a}{\Longrightarrow}$-move in the other process under the same action a. Now the game repeats, starting from the new processes. If one player cannot move, the other player wins. If the game is infinite,

the defender wins. The processes (P_1, Δ) and (P_2, Δ) are weakly bisimilar iff the defender has a winning strategy (and non-bisimilar iff the attacker has a winning strategy).

3 Hardness of Weak Bisimilarity and Regularity for BPP

Problem:	Weak bisimilarity of (normed) BPP
Instance:	Two (normed) BPP processes (P_1, Δ) and (P_2, Δ).
Question:	$(P_1, \Delta) \approx (P_2, \Delta)$?

In what follows we show that weak bisimilarity of normed BPP is *PSPACE*-hard. We prove it by reduction from QSAT[1], which is known to be *PSPACE*-complete [Pap94].

Problem:	QSAT
Instance:	A natural number n and a Boolean formula ϕ in conjunctive normal form with Boolean variables $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$.
Question:	Is $\forall x_1 \exists y_1 \forall x_2 \exists y_2 \ldots \forall x_n \exists y_n . \phi$ true?

Literal is a variable or the negation of a variable. Let

$$C \equiv \forall x_1 \exists y_1 \forall x_2 \exists y_2 \ldots \forall x_n \exists y_n . C_1 \wedge C_2 \wedge \ldots \wedge C_k$$

be an instance of QSAT, where each *clause* C_j, $1 \leq j \leq k$, is a disjunction of literals. We define the following BPP processes (P_1, Δ) and (P_2, Δ), where

$$\mathcal{C}onst(\Delta) = \{Q_1, \ldots, Q_k, X_1, \ldots, X_n, Y_1, \ldots, Y_n\}$$

and

$$\mathcal{A}ct(\Delta) = \{q_1, \ldots, q_k, x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n, y\}.$$

For each i, $1 \leq i \leq n$, let

[1] This problem is known also as QBF, for *Quantified Boolean formula.*

α_i be a parallel composition of process constants from $\{Q_1, \ldots, Q_k\}$ such that Q_j appears in α_i iff the literal x_i occurs in C_j (i.e. if x_i is set to true then C_j is satisfied),

$\overline{\alpha_i}$ be a parallel composition of process constants from $\{Q_1, \ldots, Q_k\}$ such that Q_j appears in $\overline{\alpha_i}$ iff the literal $\neg x_i$ occurs in C_j (i.e. if x_i is set to false then C_j is satisfied),

β_i be a parallel composition of process constants from $\{Q_1, \ldots, Q_k\}$ such that Q_j appears in β_i iff the literal y_i occurs in C_j,

$\overline{\beta_i}$ be a parallel composition of process constants from $\{Q_1, \ldots, Q_k\}$ such that Q_j appears in $\overline{\beta_i}$ iff the literal $\neg y_i$ occurs in C_j.

The set of transition rules Δ is given by

$$\begin{array}{lll}
X_i \xrightarrow{x_i} Y_i||\alpha_i & X_i \xrightarrow{\overline{x}_i} Y_i||\overline{\alpha_i} & \text{for } 1 \leq i \leq n \\
\\
Y_i \xrightarrow{y} X_{i+1}||\beta_i & Y_i \xrightarrow{y} X_{i+1}||\overline{\beta_i} & \text{for } 1 \leq i \leq n-1 \\
Y_n \xrightarrow{y} \beta_n & Y_n \xrightarrow{y} \overline{\beta_n} & \\
\\
X_i \xrightarrow{q_j} X_i & Y_i \xrightarrow{q_j} Y_i & \text{for } 1 \leq i \leq n \text{ and } 1 \leq j \leq k \\
\\
Q_j \xrightarrow{q_j} Q_j & Q_j \xrightarrow{\tau} \epsilon & \text{for } 1 \leq j \leq k.
\end{array}$$

Finally, let

$$P_1 \stackrel{\text{def}}{=} X_1||Q_1||Q_2||\ldots||Q_k \qquad \text{and} \qquad P_2 \stackrel{\text{def}}{=} X_1.$$

We can see the processes P_1 and P_2 using Petri net notation in Figure 1. This figure is only illustrative, and some transitions, namely $X_i \xrightarrow{q_j} X_i$ and $Y_i \xrightarrow{q_j} Y_i$ for $1 \leq i \leq n$, $1 \leq j \leq k$ are missing. The curly lines stand for the corresponding sets of arrows for α_i, $\overline{\alpha_i}$, β_i resp. $\overline{\beta_i}$. The intuition is that the attacker will be forced to play only in the process P_1 and if C is true then the defender will have the possibility to add all the process constants $\{Q_1, \ldots, Q_k\}$.

Let γ be a parallel composition of elements from $\mathcal{C}onst(\Delta)$. We define the set of process constants that occur in γ as $\mathsf{set}(\gamma) \stackrel{\text{def}}{=} \{X \in \mathcal{C}onst(\Delta) \mid X \text{ occurs in } \gamma\}$ and we also define $\mathsf{set}_Q(\gamma) \stackrel{\text{def}}{=} \mathsf{set}(\gamma) \cap \{Q_1, \ldots, Q_k\}$. The following proposition is an immediate consequence of the definition of Δ.

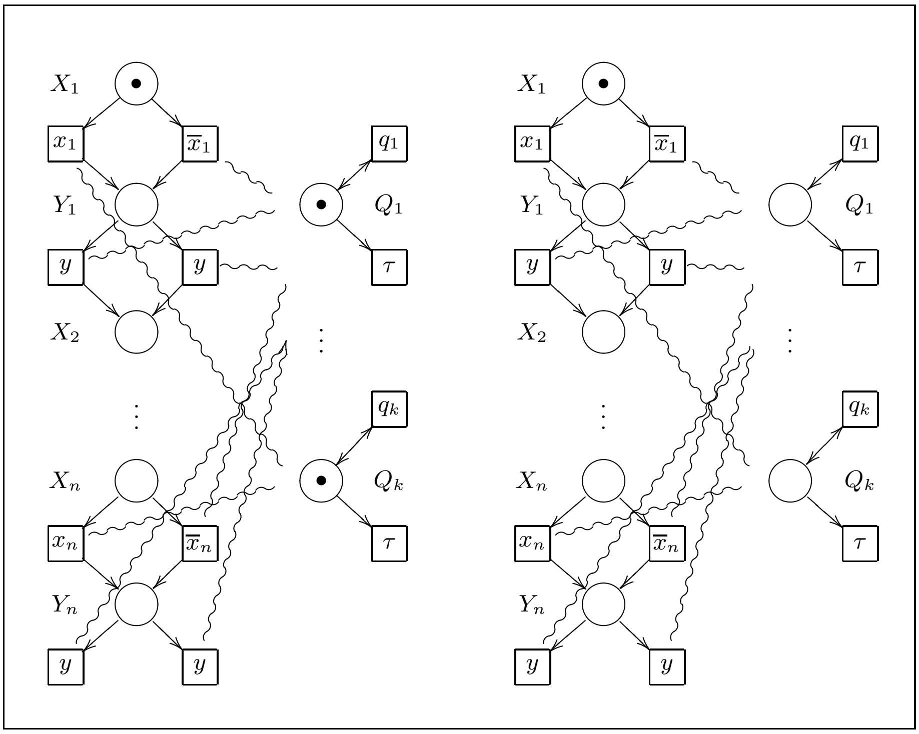

Fig. 1. The processes (P_1, Δ) and (P_2, Δ) as Petri nets.

Proposition 1. *Let γ resp. γ' be a parallel composition of some process constants from $\{Q_1, \ldots, Q_k\}$. If $\mathsf{set}_Q(\gamma) = \mathsf{set}_Q(\gamma')$ then $(\gamma, \Delta) \approx (\gamma', \Delta)$.*

We want to show that C is true if and only if $(P_1, \Delta) \approx (P_2, \Delta)$.

Lemma 1. *If $(P_1, \Delta) \approx (P_2, \Delta)$ then C is true.*

Proof. We show that $(P_1, \Delta) \not\approx (P_2, \Delta)$, supposing that C is false. If C is false then $C' \overset{\text{def}}{=} \exists x_1 \forall y_1 \exists x_2 \forall y_2 \ldots \exists x_n \forall y_n . \neg(C_1 \wedge C_2 \wedge \ldots \wedge C_k)$ is true and from this we claim that the attacker has a winning strategy in the bisimulation game for (P_1, Δ) and (P_2, Δ). The attacker plays only in the process P_1 (without using τ actions) performing the following sequence of actions

$$\widetilde{x}_1, y, \widetilde{x}_2, y, \ldots, \widetilde{x}_n, y$$

where $\widetilde{x}_i$, $1 \leq i \leq n$, corresponds to either x_i or $\overline{x}_i$, depending on the truth values for which the formula C' is true. It does not matter, how the choice of the rule for the action y is solved. The defender can only respond by performing the same actions $\widetilde{x}_1, y, \widetilde{x}_2, y, \ldots, \widetilde{x}_n, y$ (eventually using some τ actions). The actions $\widetilde{x}_1, \ldots, \widetilde{x}_n$ are forced. For the action y there are always two possibilities, corresponding to assigning a truth value for some y_i, $1 \leq i \leq n$. Finally the processes P_1 and P_2 are in states P_1' and P_2', respectively, such that $\mathsf{set}(P_1') = \{Q_1, \ldots, Q_k\}$ and $\mathsf{set}(P_2') \subseteq \{Q_1, \ldots, Q_k\}$. Since we assume that C' is true, there must be a clause C_j, $1 \leq j \leq k$, which is not satisfied. Hence $Q_j \notin \mathsf{set}(P_2')$ and P_2' cannot perform q_j. However, q_j is enabled in P_1' and thus the attacker has a winning strategy. This implies that $(P_1, \Delta) \not\approx (P_2, \Delta)$. □

For the proof of the opposite direction let us first observe the following property of (P_1, Δ) and (P_2, Δ) above. Let δ be some state such that $\mathsf{set}(\delta) \cap \{Q_1, \ldots, Q_k\} = \emptyset$ and let γ and γ' be a parallel composition of some process constants from $\{Q_1, \ldots, Q_k\}$ satisfying the condition that $\mathsf{set}_Q(\gamma) \supseteq \mathsf{set}_Q(\gamma')$. Let us consider the processes $\delta || \gamma$ and $\delta || \gamma'$. Whenever the attacker chooses any move in the second one, the defender has an answer, which makes these two processes weakly bisimilar (exploiting τ actions to eliminate the extra process constants Q_j from the first process and then using Proposition 1). We are now ready to prove the following lemma.

Lemma 2. *If C is true then $(P_1, \Delta) \approx (P_2, \Delta)$.*

Proof. Let P_1' and P_2' denote successors of P_1 and P_2, respectively, in the bisimulation game. The defender's strategy is to satisfy the following conditions during the game

- $\mathsf{set}_Q(P_1') \supseteq \mathsf{set}_Q(P_2')$ and
- never delete (using τ actions) any process constant Q_j, $1 \leq j \leq k$, in the process P_2', unless it is necessary for satisfying the first condition.

Of course these conditions are true at the beginning of the game. Using the argument above this lemma, we can see that whenever the attacker makes a move in the process P_2', he immediately looses, since the defender can make the resulting processes weakly bisimilar. This means that the only possible winning strategy for the attacker is to keep playing in P_1'. However, now the defender can always fulfil the conditions of his strategy. On a move containing x_i resp. $\overline{x}_i$ there is only one possible response for the defender. Whenever the attacker makes a y move, the defender chooses one of the rules $Y_i \xrightarrow{y} X_{i+1}||\beta_i$ and $Y_i \xrightarrow{y} X_{i+1}||\overline{\beta_i}$, such that the formula $\forall x_{i+1} \exists y_{i+1} \ldots \forall x_n \exists y_n . C_1 \wedge \ldots \wedge C_k$ is still true. Since we have the rules $X_i \xrightarrow{q_j} X_i$ and $Y_i \xrightarrow{q_j} Y_i$ for any i, j such that $1 \leq i \leq n$ and $1 \leq j \leq k$, the only possibility for the attacker to win is to perform some sequence

$$\widetilde{x}_1, y, \widetilde{x}_2, y, \ldots, \widetilde{x}_n, y$$

possibly including also some τ actions and then reach some state P_1', where $\mathsf{set}(P_1') \subseteq \{Q_1, \ldots, Q_k\}$. Since C is true the defender can always get to a corresponding state P_2', where $\mathsf{set}(P_1') = \mathsf{set}(P_2')$. Hence (using Proposition 1) the attacker looses again. This means that the defender has a winning strategy and so $(P_1, \Delta) \approx (P_2, \Delta)$. □

Theorem 1. *Weak bisimilarity of normed BPP is PSPACE-hard.*

Proof. Observe that all the process constants in Δ are normed and that the reduction is in polynomial time. The theorem is then an immediate consequence of Lemma 1 and Lemma 2. □

Corollary 1. *Weak bisimilarity of BPP is PSPACE-hard.*

Proof. Directly from Theorem 1. □

Remark 1. Theorem 1 can be easily extended to 1-safe Petri nets where each transition has exactly one input place (for the definition of 1-safe Petri nets see e.g. [JM96]). It is enough to introduce for each $\alpha_i/\overline{\alpha_i}$ and $\beta_i/\overline{\beta_i}$, $1 \leq i \leq n$, a new set of process constants $\{Q_1, \ldots, Q_k\}$ to ensure that in each reachable marking there is at most one token in every place. Related results about 1-safe Petri nets can be found in [JM96].

Another problem we will analyse, is weak regularity of BPP processes.

Problem: Weak regularity of (normed) BPP
Instance: A (normed) BPP process (P, Δ).
Question: Is there a finite-state process (F, Δ') such that $(P, \Delta) \approx (F, \Delta')$?

Mayr has proved that weak regularity of BPP is Π_2^P-hard [May00a], demonstrating a reduction from the weak bisimilarity problem between a pair of special processes with finitely many reachable states. It can be easily seen that his proof works also for a general pair of weakly regular processes and moreover it preserves normedness.

Theorem 2 ([May00a]). *Let (P_1, Δ) and (P_2, Δ) be weakly regular BPP processes. We can construct in polynomial time a BPP process (P, Δ') such that*

$$(P_1, \Delta) \approx (P_2, \Delta) \iff (P, \Delta') \text{ is weakly regular.}$$

Moreover, if (P_1, Δ) and (P_2, Δ) are normed, so is (P, Δ').

Observe that the processes P_1 and P_2 from the proof of *PSPACE*-hardness of weak bisimilarity (Theorem 1) are regular and moreover they are normed. This gives the following theorem with an immediate corollary.

Theorem 3. *Weak regularity of normed BPP is PSPACE-hard.*

Proof. Because of Theorem 2, there is a reduction from a *PSPACE*-hard problem of weak bisimilarity for normed BPP to weak regularity of normed BPP. □

Corollary 2. *Weak regularity of BPP is PSPACE-hard.*

4 Hardness of Weak Bisimilarity and Regularity for BPA

In this section we consider the same problems for BPA, as we did for BPP.

Problem: Weak bisimilarity of (normed) BPA
Instance: Two (normed) BPA processes (P_1, Δ) and (P_2, Δ).
Question: $(P_1, \Delta) \approx (P_2, \Delta)$?

Problem: Weak regularity of (normed) BPA
Instance: A (normed) BPA process (P, Δ).
Question: Is there a finite-state process (F, Δ') such that $(P, \Delta) \approx (F, \Delta')$?

First, we show that there is a reduction from weak bisimilarity of regular BPA to weak regularity. The idea of the proof is similar to the case of BPP mentioned above from [May00a].

Theorem 4. *Let (P_1, Δ) and (P_2, Δ) be weakly regular BPA processes. We can construct in polynomial time a BPA process (P, Δ') such that*

$$(P_1, \Delta) \approx (P_2, \Delta) \iff (P, \Delta') \text{ is weakly regular.}$$

Moreover, if (P_1, Δ) and (P_2, Δ) are normed, so is (P, Δ').

Proof. Assume that (P_1, Δ) and (P_2, Δ) are weakly regular BPA processes. We construct a BPA process (P, Δ') with

$$\mathcal{C}\mathit{onst}(\Delta') \overset{\text{def}}{=} \mathcal{C}\mathit{onst}(\Delta) \cup \{A, B, C, B_1, B_2\}$$

and

$$\mathcal{A}\mathit{ct}(\Delta') \overset{\text{def}}{=} \mathcal{A}\mathit{ct}(\Delta) \cup \{a\}$$

where A, B, C, B_1, B_2 are new process constants and a is a new action. Then $\Delta' \overset{\text{def}}{=} \Delta \cup \Delta^1 \cup \Delta^2$, where Δ^1 and Δ^2 are defined as follows. The set of transition rules Δ^1 is given by

$$\begin{array}{ll}
A \xrightarrow{a} A.B & A \xrightarrow{\tau} \epsilon \\
B \xrightarrow{a} \epsilon & B \xrightarrow{\tau} \epsilon \\
 & \\
C \xrightarrow{a} B_1 & C \xrightarrow{a} P_1 \\
B_1 \xrightarrow{a} B_1 & B_1 \xrightarrow{a} P_1
\end{array}$$

and Δ^2 is given by

$$\begin{array}{ll} C \xrightarrow{a} B_2 & \quad C \xrightarrow{a} P_2 \\ B_2 \xrightarrow{a} B_2 & \quad B_2 \xrightarrow{a} P_2. \end{array}$$

Let $P \overset{\text{def}}{=} A.C$. Observe that if (P_1, Δ) and (P_2, Δ) are normed, so is (P, Δ'). We show now that our reduction is correct.

Lemma 3. *If $(P_1, \Delta) \not\approx (P_2, \Delta)$ then (P, Δ') is not weakly regular.*

Proof. Suppose that $(P_1, \Delta) \not\approx (P_2, \Delta)$. Then we demonstrate that there are infinitely many weakly nonbisimilar states reachable from P. Let us consider $B^i.C$ for any natural number i. Of course $P \longrightarrow^* B^i.C$ and we claim that $(B^i.C, \Delta') \not\approx (B^j.C, \Delta')$ for any $i \neq j$. Without loss of generality assume that $i < j$. The attacker has the following winning strategy (playing only in the second process – see Figure 2). He performs a sequence of j actions a in $B^j.C$, thus reaching C. Since B^i cannot do this sequence, the defender has to reach C eventually (let us say after i' steps, where $i' \leq i$). As neither P_1 nor P_2 can perform a, he has only two choices when responding to the action a – either $C \xrightarrow{a} B_1$ or $C \xrightarrow{a} B_2$. Assume that he chooses B_1 (the other case is symmetric). Now the defender's only possibility

$$\begin{tikzcd}
B^i.C \arrow[d, "a^{i'}"] & \approx^? & B^j.C \arrow[d, "a^{i'}"] \\
C \arrow[d, "a"] & & B^{j-i'}.C \arrow[d, "a"] \\
B_1 \arrow[d, "a^{j-i'-1}"] & & B^{j-i'-1}.C \arrow[d, "a^{j-i'-1}"] \\
B_1 \arrow[d, "a"] & & C \arrow[d, "a"] \\
P_1 & \not\approx & P_2
\end{tikzcd}$$

Fig. 2. The winning strategy for the attacker $(i < j)$.

is to stay in B_1 for another $a^{j-i'-1}$ moves of the attacker. After the attacker has reached C (in the second process), he chooses to go to P_2 in the next round. If the defender stays in B_1 he looses immediately and if he moves to P_1 he looses as well, since $(P_1, \Delta') \not\approx (P_2, \Delta')$. □

Lemma 4. *If $(P_1, \Delta) \approx (P_2, \Delta)$ then (P, Δ') is weakly regular.*

Proof. Assume that $(P_1, \Delta) \approx (P_2, \Delta)$, which implies that $(P, \Delta') \approx (P, \Delta'')$, where $\Delta'' = \Delta' - \Delta^2$ (weak bisimilarity is a congruence on BPA). Notice that (B_1, Δ'') is weakly regular, so it is enough to show that $(A.C, \Delta'') \approx (B_1, \Delta'')$. Obviously, $(C, \Delta'') \approx (B_1, \Delta'')$, which implies that for any $n \geq 0$, $(B^n.C, \Delta'') \approx (B_1, \Delta'')$ since $B_1 \xrightarrow{a} B_1$ and $B^n \xrightarrow{\tau^*} \epsilon$. This gives that $(A.B^n.C, \Delta'') \approx (B_1, \Delta'')$ for any $n \geq 0$, which in particular means that $(A.C, \Delta'') \approx (B_1, \Delta'')$. □

Theorem 4 is an immediate consequence of Lemma 3 and Lemma 4. □

In the paper by Stribrna [Str98] it is shown (Theorem 2.5) that weak bisimilarity for totally normed BPA is *NP*-hard. The proof is by reduction from a variant of the bin-packing (knapsack) problem and the processes in this proof have finitely many reachable states (and so they are weakly regular). Thus we can use Theorem 4 to obtain the following result with an obvious corollary.

Theorem 5. *Weak regularity of normed BPA is NP-hard.*

Corollary 3. *Weak regularity of BPA is NP-hard.*

We remind the reader of the fact that *PSPACE*-hardness of weak bisimilarity for BPA achieved by Stribrna [Str98] does not imply *PSPACE*-hardness of weak regularity for BPA, since the described processes are not regular. In the next theorem, however, we prove that weak regularity for BPA is not only *NP*-hard but also *co-NP*-hard. This we demonstrate by showing that weak bisimilarity for BPA is *co-NP*-hard, where the involved processes are finite-state (nevertheless they are unnormed in this case).

Theorem 6. *Weak regularity of BPA is co-NP-hard.*

Proof. We reduce the complement of 3-SAT [Pap94] to weak bisimilarity of BPA and then we use Theorem 4.

Problem: 3-SAT COMPLEMENT
Instance: A natural number n and a Boolean formula ϕ in disjunctive normal form with implicants of length 3 and with Boolean variables $x_1, \ldots, x_n$.
Question: Is $\forall x_1 \forall x_2 \ldots \forall x_n . \phi$ true?

Let

$$D \equiv \forall x_1 \forall x_2 \ldots \forall x_n . D_1 \vee D_2 \vee \ldots \vee D_k$$

be an instance of 3-SAT COMPLEMENT, where each implicant D_j, $1 \leq j \leq k$, is a conjunction of three literals. Let us define the following BPA processes $(X_1, \mathit{\Delta})$ and $(X'_1, \mathit{\Delta})$, where

$$\mathcal{C}onst(\mathit{\Delta}) \stackrel{\text{def}}{=} \{ D^1_1, \ldots, D^1_k, D^2_1, \ldots, D^2_k, D^3_1, \ldots, D^3_k, \\ X_1, \ldots, X_n, X_{n+1}, X'_1, \ldots, X'_n, X'_{n+1}, Y_1, \ldots, Y_k, A, S \}$$

and

$$\mathcal{A}ct(\mathit{\Delta}) \stackrel{\text{def}}{=} \{ d^1_1, \ldots, d^1_k, d^2_1, \ldots, d^2_k, d^3_1, \ldots, d^3_k, \\ x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n, a, s \}.$$

For each i, $1 \leq i \leq n$, let

α_i be a sequential composition (in some fixed ordering) of process constants D^r_j ($1 \leq r \leq 3$ and $1 \leq j \leq k$) such that
- D^1_j appears in α_i iff the literal x_i occurs in D_j in the first position
- D^2_j appears in α_i iff the literal x_i occurs in D_j in the second position
- D^3_j appears in α_i iff the literal x_i occurs in D_j in the third position

$\overline{\alpha_i}$ be a sequential composition (in some fixed ordering) of process constants D^r_j ($1 \leq r \leq 3$ and $1 \leq j \leq k$) such that
- D^1_j appears in $\overline{\alpha_i}$ iff the literal $\neg x_i$ occurs in D_j in the first position
- D^2_j appears in $\overline{\alpha_i}$ iff the literal $\neg x_i$ occurs in D_j in the second position
- D^3_j appears in $\overline{\alpha_i}$ iff the literal $\neg x_i$ occurs in D_j in the third position.

The set of transition rules Δ is given by

$$\begin{array}{lll}
X_i \xrightarrow{x_i} X_{i+1}.\alpha_i & X'_i \xrightarrow{x_i} X'_{i+1}.\alpha_i & \text{for } 1 \leq i \leq n \\
X_i \xrightarrow{\overline{x}_i} X_{i+1}.\overline{\alpha_i} & X'_i \xrightarrow{\overline{x}_i} X'_{i+1}.\overline{\alpha_i} & \text{for } 1 \leq i \leq n \\
X_{n+1} \xrightarrow{a} Y_j & X'_{n+1} \xrightarrow{a} Y_j & \text{for } 1 \leq j \leq k \\
 & X'_{n+1} \xrightarrow{a} A &
\end{array}$$

$$\begin{array}{l}
A \xrightarrow{a} A \\
A \xrightarrow{\tau} \epsilon \\
\\
S \xrightarrow{s} S
\end{array}$$

$$\begin{array}{lllll}
Y_j \xrightarrow{d_j^1} S & Y_j \xrightarrow{d_j^2} S & Y_j \xrightarrow{d_j^3} S & & \text{for } 1 \leq j \leq k \\
 & Y_j \xrightarrow{a} Y_j & & & \text{for } 1 \leq j \leq k \\
 & Y_j \xrightarrow{\tau} \epsilon & & & \text{for } 1 \leq j \leq k \\
\\
D_j^1 \xrightarrow{d_j^1} S & D_j^2 \xrightarrow{d_j^2} S & D_j^3 \xrightarrow{d_j^3} S & & \text{for } 1 \leq j \leq k \\
D_j^1 \xrightarrow{\tau} \epsilon & D_j^2 \xrightarrow{\tau} \epsilon & D_j^3 \xrightarrow{\tau} \epsilon & & \text{for } 1 \leq j \leq k.
\end{array}$$

The intuition is that the attacker plays in X'_1 and generates some truth assignment. When he reaches the process constant A, the defender chooses an implicant that is satisfied by the truth assignment by performing a transition $X_{n+1} \xrightarrow{a} Y_j$. The attacker can now test whether this implicant is indeed satisfied.

Lemma 5. *If* $(X_1, \Delta) \approx (X'_1, \Delta)$ *then* D *is true.*

Proof. For the sake of contradiction suppose that D is false, i.e. there is some assignment of truth values for $x_1, \ldots, x_n$ such that $D_1 \vee D_2 \vee \ldots \vee D_k$ is false, which means that for each j, $1 \leq j \leq k$, there is at least one false literal in D_j. We show that the attacker has a winning strategy in the bisimulation game. First, the attacker plays in X'_1 generating this false assignment and finally he uses the transition $X'_{n+1} \xrightarrow{a} A$. The defender can only respond by performing the same actions $x_i/\overline{x}_i$ with the final transition $X_{n+1} \xrightarrow{a} Y_j$ for some j (observe that the defender cannot use the transition $Y_j \xrightarrow{\tau} \epsilon$, otherwise the attacker wins immediately). Now the attacker changes the processes and plays $Y_j \xrightarrow{d_j^r} S$, where r is a position of a false literal in D_j. This means that the defender looses, since he has no response to this move. □

Lemma 6. *If D is true then $(X_1, \Delta) \approx (X'_1, \Delta)$.*

Proof. We show that the defender has a winning strategy. Whatever the attacker performs during the first n moves the defender imitates in the other process. Finally we get a pair of processes $X_{n+1}\alpha$ and $X'_{n+1}\alpha$. If the attacker chooses the rule $X_{n+1} \xrightarrow{a} Y_j$ for some j then he looses, since the defender can do the same move in $X'_{n+1}\alpha$ and make the resulting processes equal. The same happens if the attacker chooses the rule $X'_{n+1} \xrightarrow{a} Y_j$ for some j in the second process. So the only possibility for the attacker to win is to move under a to $A.\alpha$ in the second process. The defender answers by performing $X_{n+1} \xrightarrow{a} Y_j$, where D_j is the implicant which makes the formula $D_1 \vee D_2 \vee \ldots \vee D_k$ true. Now the attacker has to switch processes since if he continues in $A.\alpha$ doing the τ action, he looses again (the defender can make the two processes equal). In the process $Y_j.\alpha$ the attacker has essentially two possibilities. He can perform $Y_j \xrightarrow{d_j^r} S$ for some r, $1 \leq r \leq 3$. However, the defender can perform some sequence of τ actions to enable d_j^r in the second process and then he performs the transition $D_j^r \xrightarrow{d_j^r} S$. As S is unnormed, the resulting processes are bisimilar (since $(S.\beta, \Delta) \approx (S.\beta', \Delta)$ for any β and β'). The other attacker's possibility is to perform first $Y_j \xrightarrow{\tau} \epsilon$, but then he looses as well (the resulting processes can be made equal). Thus the defender has a winning strategy, which means that $(X_1, \Delta) \approx (X'_1, \Delta)$. □

The proof of Theorem 6 is then a consequence of Lemma 5, Lemma 6, Theorem 4 and the fact that both (X_1, Δ) and (X'_1, Δ) are finite-state processes. □

Corollary 3 and Theorem 6 show that weak regularity for BPA is both *NP* and *co-NP*-hard. We use these results to obtain *DP*-hardness. The class *DP* is defined as follows [Pap94]. A language L is in *DP* iff there are two languages $L_1 \in NP$ and $L_2 \in co\text{-}NP$ such that $L = L_1 \cap L_2$. Obviously $NP \cup co\text{-}NP$ is contained in *DP* and moreover the other inclusion is unlikely. We show that weak regularity is *DP*-hard by demonstrating a reduction from the SAT-UNSAT problem [Pap94].

Problem: SAT-UNSAT
Instance: Two Boolean formulae ϕ_1 and ϕ_2.
Question: Is ϕ_1 satisfiable and ϕ_2 is not?

Theorem 7. *Weak regularity of BPA is DP-hard.*

Proof. As we know that weak regularity is both *NP* and *co-NP*-hard, we can construct in polynomial time processes $(P_1, \varDelta)$ and $(P_2, \varDelta)$ such that $(P_1, \varDelta)$ is weakly regular iff ϕ_1 is satisfiable, and $(P_2, \varDelta)$ is weakly regular iff ϕ_2 is not satisfiable. Let us now construct a process $(P, \varDelta')$ such that $(P, \varDelta')$ is weakly regular iff ϕ_1 is satisfiable and ϕ_2 is not. We define $\mathcal{C}\mathit{onst}(\varDelta') \overset{\text{def}}{=} \mathcal{C}\mathit{onst}(\varDelta) \cup \{P\}$ and $\mathcal{A}\mathit{ct}(\varDelta') \overset{\text{def}}{=} \mathcal{A}\mathit{ct}(\varDelta) \cup \{a_1, a_2\}$ where P is a new process constant and a_1, a_2 are new actions. The set $\varDelta'$ contains all the rules from $\varDelta$ together with

$$P \xrightarrow{a_1} P_1 \qquad P \xrightarrow{a_2} P_2.$$

Obviously $(P, \varDelta')$ is regular iff both $(P_1, \varDelta)$ and $(P_2, \varDelta)$ are regular. This proves that $(P, \varDelta')$ is weakly regular iff ϕ_1 is satisfiable and ϕ_2 is not. □

5 Conclusion

In the following tables we summarise known results about weak bisimilarity and regularity problems for BPA, BPP and PA. The results obtained in this paper are in boldface. Question mark means that there has not been any known lower bound yet.

	$\approx$	$\approx$ of normed processes
BPA	*PSPACE*-hard [Str98]	*NP*-hard [Str98]
BPP	*NP*-hard [Str98] Π_2^P-hard [May00a] **PSPACE-hard**	*NP*-hard [Str98] **PSPACE-hard**
PA	*PSPACE*-hard [Str98] **PSPACE-hard**	*NP*-hard [Str98] **PSPACE-hard**

For the case of $\approx$ in the class of PA, the result in this paper is more general, since our processes are weakly regular, which is not the case for the result by Stribrna.

	weak regularity	weak regularity of normed processes
BPA	? **DP-hard**	? **NP-hard**
BPP	Π_2^P-hard [May00a] **PSPACE-hard**	? **PSPACE-hard**
PA	Π_2^P-hard [May00a] **PSPACE-hard**	? **PSPACE-hard**

We remind the reader of the fact that *DP*-hardness means in particular both *NP* and *co-NP*-hardness.

Acknowledgement. I would like to thank my advisor Mogens Nielsen for his kind supervision and encouragement.

References

[BE97] Olaf Burkart and Javier Esparza. More infinite results. *Bulletin of the European Association for Theoretical Computer Science*, 62:138–159, June 1997. Columns: Concurrency.

[BW90] J.C.M. Baeten and W.P. Weijland. *Process Algebra.* Number 18 in Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 1990.

[CHM93] S. Christensen, Y. Hirshfeld, and F. Moller. Bisimulation is decidable for basic parallel processes. In *Proceedings of CONCUR'93*, volume 715 of *LNCS*, pages 143–157. Springer-Verlag, 1993.

[CHS95] S. Christensen, H. Hüttel, and C. Stirling. Bisimulation equivalence is decidable for all context-free processes. *Information and Computation*, 121:143–148, 1995.

[Hir96] Yoram Hirshfeld. Bisimulation trees and the decidability of weak bisimulations. In *Proceedings of the the First International Workshop on Verification of Infinite State Systems (Infinity'96)*, volume 5 of *ENTCS*. Springer-Verlag, 1996.

[HJM96a] Yoram Hirshfeld, Mark Jerrum, and Faron Moller. A polynomial algorithm for deciding bisimilarity of normed context-free processes. *Theoretical Computer Science*, 158(1–2):143–159, 1996.

[HJM96b] Yoram Hirshfeld, Mark Jerrum, and Faron Moller. A polynomial-time algorithm for deciding bisimulation equivalence of normed Basic Parallel Processes. *Mathematical Structures in Computer Science*, 6(3):251–259, 1996.

[JKM98] P. Jancar, A. Kucera, and R. Mayr. Deciding bisimulation-like equivalences with finite-state processes. In *Proceedings of the Annual International Colloquium on Automata, Languages and Programming (ICALP'98)*, volume 1443 of *LNCS*. Springer-Verlag, 1998.

[JM96] Lalita Jategaonkar and Albert R. Meyer. Deciding true concurrency equivalences on safe, finite nets. *Theoretical Computer Science*, 154(1):107–143, 1996.

[KM99] A. Kucera and R. Mayr. Weak bisimilarity with infinite-state systems can be decided in polynomial time. In *Proceedings of the 10th International Conference on Concurrency Theory (CONCUR'99)*, volume 1664 of *LNCS*. Springer-Verlag, 1999.

[May00a] Richard Mayr. On the complexity of bisimulation problems for basic parallel processes. In *Proceedings of 27st International Colloquium on Automata, Languages and Programming (ICALP'00)*, LNCS. Springer-Verlag, 2000. To appear.

[May00b] Richard Mayr. Process rewrite systems. *Information and Computation*, 156(1):264–286, 2000.

[Mil89] R. Milner. *Communication and Concurrency.* Prentice-Hall, 1989.

[Mol96] F. Moller. Infinite results. In *Proceedings of CONCUR'96*, volume 1119 of *LNCS*, pages 195–216. Springer-Verlag, 1996.

[Pap94] Christos H. Papadimitriou. *Computational Complexity.* Addison-Wesley, New York, 1994.

[Par81] D.M.R. Park. Concurrency and automata on infinite sequences. In *Proceedings 5^{th} GI Conference*, volume 104 of *LNCS*, pages 167–183. Springer-Verlag, 1981.

[Plo81] G. Plotkin. A structural approach to operational semantics. Technical Report Daimi FN-19, Department of Computer Science, University of Aarhus, 1981.

[Sti95] Colin Stirling. Local model checking games. In *Proceedings of the 6th International Conference on Concurrency Theory (CONCUR'95)*, volume 962 of *LNCS*, pages 1–11. Springer-Verlag, 1995.

[Str98] Jitka Stribrna. Hardness results for weak bisimilarity of simple process algebras. In *Proceedings of the MFCS'98 Workshop on Concurrency*, volume 18 of *ENTCS*. Springer-Verlag, 1998.

[Tho93] Wolfgang Thomas. On the Ehrenfeucht-Fraïssé game in theoretical computer science (extended abstract). In *Proceedings of the 4th International Joint Conference CAAP/FASE, Theory and Practice of Software Development (TAPSOFT'93)*, volume 668 of *LNCS*, pages 559–568. Springer-Verlag, 1993.

Recent BRICS Report Series Publications

RS-00-16 **Jiří Srba.** ***Complexity of Weak Bisimilarity and Regularity for BPA and BPP*****. June 2000. 20 pp. To appear in Aceto and Victor, editors,** ***Expressiveness in Concurrency: Fifth International Workshop EXPRESS '00 Proceedings*****, ENTCS, 2000.**

RS-00-15 **Daniel Damian and Olivier Danvy.** ***Syntactic Accidents in Program Analysis: On the Impact of the CPS Transformation*****. June 2000. Extended version of an article to appear in** ***Proceedings of the fifth ACM SIGPLAN International Conference on Functional Programming*****, 2000.**

RS-00-14 **Ronald Cramer, Ivan B. Damgård, and Jesper Buus Nielsen.** ***Multiparty Computation from Threshold Homomorphic Encryption*****. June 2000. ii+38 pp.**

RS-00-13 **Ondřej Klíma and Jiří Srba.** ***Matching Modulo Associativity and Idempotency is NP-Complete*****. June 2000. 19 pp. To appear in** ***Mathematical Foundations of Computer Science: 25 th International Symposium*****, MFCS '00 Proceedings, LNCS, 2000.**

RS-00-12 **Ulrich Kohlenbach.** ***Intuitionistic Choice and Restricted Classical Logic*****. May 2000. 9 pp.**

RS-00-11 **Jakob Pagter.** ***On Ajtai's Lower Bound Technique for R-way Branching Programs and the Hamming Distance Problem*****. May 2000. 18 pp.**

RS-00-10 **Stefan Dantchev and Søren Riis.** ***A Tough Nut for Tree Resolution*****. May 2000. 13 pp.**

RS-00-9 **Ulrich Kohlenbach.** ***Effective Uniform Bounds on the Krasnoselski-Mann Iteration*****. May 2000. 34 pp.**

RS-00-8 **Nabil H. Mustafa and Aleksandar Pekeč.** ***Democratic Consensus and the Local Majority Rule*****. May 2000. 38 pp.**

RS-00-7 **Lars Arge and Jakob Pagter.** ***I/O-Space Trade-Offs*****. April 2000. To appear in** ***7th Scandinavian Workshop on Algorithm Theory*****, SWAT '98 Proceedings, LNCS, 2000.**

RS-00-6 **Ivan B. Damgård and Jesper Buus Nielsen.** ***Improved Non-Committing Encryption Schemes based on a General Complexity Assumption*****. March 2000. 24 pp.**