FI MU

Faculty of Informatics
Masaryk University

Bisimulation Equivalence is Decidable for One-Counter Processes

by

Petr Jančar

FI MU Report Series FIMU-RS-97-06

 May 1997

Bisimulation Equivalence is Decidable for One-Counter Processes [1]

Petr Jančar
Univ. of Ostrava and Techn. Univ. of Ostrava, Czech Republic
e-mail: jancar@osu.cz

Abstract. It is shown that bisimulation equivalence is decidable for the processes generated by (nondeterministic) pushdown automata where the pushdown behaves like a counter, in fact. Also regularity, i.e. bisimulation equivalence with some finite-state process, is shown to be decidable for the mentioned processes.

1 Introduction

In recent years, growing effort has been devoted to the area of verification of (potentially) infinite-state systems. An important studied question is that of (un)decidability for various (behavioural) equivalences. A prominent role among these equivalences is played by *bisimulation equivalence*, or *bisimilarity*, which is more appropriate for (concurrent, reactive etc.) systems than e.g. the traditional language equivalence (cf. [Mil89]). Roughly speaking, two processes (states of systems) are bisimilar iff for any evolving of one process caused by performing an action labelled a there is an action labelled a which causes evolving of the other process in such a way that the resulting processes (states) are again bisimilar.

Several recent results help to highlight and understand the decidability boundaries for bisimilarity, which are different from those for language equivalence. It is e.g. known that bisimilarity is decidable for Basic Parallel Processes [CHM93] while the language equivalence is undecidable for them [Hir93]. More relevant here are context-free processes (generated by context-free grammars), also called BPA-processes, where the language equivalence is well-known to be undecidable while bisimilarity is decidable [CHS95]. Pushdown automata (which are in the 'language sense' equivalent to context-free grammars) generate a richer family than that of context-free processes when considering bisimulation equivalence. These *pushdown processes* can be identified with 'state-pushdown' configurations, whose behaviour is determined by the transition rules (not allowing ε-rules).

[1] Supported by the Grant Agency of the Czech Republic, Grant No. 201/97/0456, and also by the Univ. of Ostrava grant No. 031/97

Recently Stirling [Sti96] has shown the decidability of bisimilarity for *normed* pushdown processes, while the question remains open for the whole class.

Here we show the decidability of bisimilarity for another subclass of pushdown processes: we will not impose the restriction of normedness but we consider the case when the pushdown behaves like a counter, in fact; i.e. there is only one stack symbol, besides a special bottom symbol which enables to test 'emptiness' of the pushdown. Let us call such processes as *one-counter processes*. The decidability result for one-counter processes also confirms the conjecture by the author [Jan93] that bisimilarity for labelled Petri nets with one unbounded place is decidable (while two unbounded places suffice for undecidability).

Semidecidability of *nonbisimilarity* of pushdown processes can be derived easily in the standard way applied for image finite systems. Therefore semidecidability of bisimilarity is what matters here. In similar cases, the key point is to show that the *bisimilarity* case has always a finite (or finitely presented) witness whose validity can be checked algorithmically. In our case, at the one-counter processes, the role of such witnesses is played by (descriptions of) semilinear sets; this approach was already used in [Jan93] or [Esp95].

Roughly speaking, the existence of such witnesses (i.e. semilinear bisimulations) for one-counter processes can be anticipated from the intuition that two bisimilar processes have to have the same 'distance' (minimum number of steps) to a 'bottom process' (configuration with only the bottom symbol in the pushdown=counter) when such bottom processes matter at all; it can be guessed that then the counter heights of such processes have to be, in principle, linearly related. The possibility of an algorithmic checking of a witness' validity can be easily observed due to the decidability of Presburger arithmetic (although this deep result is surely not needed in its whole).

Another natural decidability question is that of *regularity* of a given process, which will in our context mean the bisimulation equivalence with some finite-state process. This problem has been shown to be decidable for labelled Petri nets [JE96], which include BPP-processes. In [BCS96], the decidability is shown for BPA-processes (where the 'language regularity' is well-known to be undecidable). The question for the whole class of pushdown processes is still open (while for the class of normed pushdown processes is easily seen to be decidable). As an additional result, we demonstrate that regularity is also decidable for one-counter processes.

In fact, one-counter processes can be 'almost' identified with labelled Petri nets with one unbounded place; but unlike Petri nets they can 'test for zero'. Nevertheless the strategy used in the proof of decidability of regularity for labelled Petri nets [JE96] applies for them as well.

Section 2 contains definitions and claims the results; the proofs are given in Section 3. Section 4 adds some further comments.

2 Definitions and Results

We begin with recalling some standard notions.

A *labelled transition system*, a *system* for short, is a tuple $\mathcal{T} = (\mathcal{S}, \{\xrightarrow{a}\}_{a\in\mathcal{A}})$ where $\mathcal{S}$ is the set of *states*, $\mathcal{A}$ is the set of *actions* (or *action names*) and each $\xrightarrow{a}$ is a binary *(transition) relation* on $\mathcal{S}$ ($\xrightarrow{a}\subseteq \mathcal{S}\times\mathcal{S}$). By $E \to F$ ($E, F \in \mathcal{S}$) we mean that $E \xrightarrow{a} F$ for some a; $\to^*$ denotes the reflexive and transitive closure of the relation $\to$. By $E \to^* \mathcal{S}'$ ($\mathcal{S}'$ is *reachable* from E), where $\mathcal{S}' \subseteq \mathcal{S}$, we mean $E \to^* F$ for some $F \in \mathcal{S}'$. In the obvious sense, we also use $E \xrightarrow{u} F$ where $u \in \mathcal{A}^*$; $|u|$ denotes the length of the sequence u.

A transition system $\mathcal{T} = (\mathcal{S}, \{\xrightarrow{a}\}_{a\in\mathcal{A}})$ is *finite* iff $\mathcal{S}$ and $\mathcal{A}$ are finite. $\mathcal{T}$ is *image finite* iff $succ(E) = \bigcup_{a\in\mathcal{A}} succ_a(E)$ is finite for any $E \in \mathcal{S}$, where we define $succ_a(E) = \{E' \mid E \xrightarrow{a} E'\}$.

Speaking of a *process* E, we always consider it as (being associated with) a state in a transition system which is clear from the context. When necessary, we denote the relevant transition system by $\mathcal{T}(E)$. Using the term of a *finite*, or rather a *finite-state*, *process* E, we mean that $\mathcal{T}(E)$ is finite; similarly for an *image finite process*.

A binary relation $\mathcal{R}$ between processes is a *bisimulation relation* provided that whenever $(E, F) \in \mathcal{R}$, for each action a

if $E \xrightarrow{a} E'$ then there is F' s.t. $F \xrightarrow{a} F'$ and $(E', F') \in \mathcal{R}$, and
if $F \xrightarrow{a} F'$ then there is E' s.t. $E \xrightarrow{a} E'$ and $(E', F') \in \mathcal{R}$.

Two processes E and F are *bisimulation equivalent*, or *bisimilar*, written $E \sim F$, if there is a bisimulation relation $\mathcal{R}$ relating them.

The family $\{\sim_n \mid n \geq 0\}$ (of relations between processes) is defined inductively:

1/ $E \sim_0 F$ for all processes E, F
2/ $E \sim_{n+1} F$ iff for each a

if $E \xrightarrow{a} E'$ then there is F' s.t. $F \xrightarrow{a} F'$ and $E' \sim_n F'$, and
if $F \xrightarrow{a} F'$ then there is E' s.t. $E \xrightarrow{a} E'$ and $E' \sim_n F'$.

Let us recall some 'folklore' results.

Proposition 2.1. *For image finite processes, $E \sim F$ iff $\forall n \geq 0 : E \sim_n F$.*

Let us call $\mathcal{T} = (\mathcal{S}, \{\xrightarrow{a}\}_{a \in \mathcal{A}})$ an *admissible system* iff the state set $\mathcal{S}$ is finite or countably infinite (identified with a set of sequences over a finite alphabet), the action set $\mathcal{A}$ is finite, $\mathcal{T}$ is image finite, and all the successor functions $succ_a : \mathcal{S} \longrightarrow 2^{\mathcal{S}}$ are effectively computable.

Proposition 2.2. *Considering only admissible transition systems, all the relations $E \sim_n F$ ($n \in \mathcal{N}$) are decidable. Therefore the problem $E \not\sim F$ is semidecidable.*

Now we define the pushdown processes (cf. e.g. [Sti96]); loosely speaking, these are state-pushdown configurations of a given (nondeterministic) pushdown automaton without ε-rules. Then we introduce the 'one-counter case'.

Suppose a given collection (i.e. a pushdown automaton viewed as a 'pushdown process generator') $M = (\mathcal{P}, \Gamma, \mathcal{A}, \mathcal{B})$ where $\mathcal{P} = \{p_1, p_2, \ldots, p_k\}$ is a finite set of *states*, $\Gamma = \{X_1, X_2, \ldots, X_m\}$ is a finite set of *stack symbols*, $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$ is a finite set of *actions*, and $\mathcal{B}$ is a finite set of basic transitions, each of the form $pX \xrightarrow{a} q\alpha$ where p, q are states, a is an action, X is a stack symbol and α is a sequence of stack symbols (i.e. $\alpha \in \Gamma^*$). The transition system $\mathcal{T}_M$ generated by M has the expressions $p\alpha$ ($p \in \mathcal{P}$, $\alpha \in \Gamma^*$), called *pushdown processes*, as states, $\mathcal{A}$ is its action set, and the transition relations are in the straightforward way determined by the basic transitions together with the following *prefix rule*: if $pX \xrightarrow{a} q\alpha$ then $pX\beta \xrightarrow{a} q\alpha\beta$ (for any $\beta \in \Gamma^*$).

When $\Gamma = \{X, Z\}$ and any basic transition is of the form $pX \xrightarrow{a} q\alpha$ or $pZ \xrightarrow{a} q\alpha Z$ where $\alpha \in \{X\}^*$ (we call $M = (\mathcal{P}, \Gamma, \mathcal{A}, \mathcal{B})$ a *one-counter machine* in such a case), then any $pXX \ldots XZ$ is called a *one-counter process*. For convenience, a process pX^mZ will be denoted by $p(m)$ ($m \in \mathcal{N}$, where $\mathcal{N}$ denotes the set of all nonnegative integers).

Notice that any process reachable from a one-counter process is a one-counter process as well. Thus for a one-counter machine M we can safely suppose that $\mathcal{T}_M$ has states of the form $p(m)$ only.

Our main aim here is to show

Theorem 2.3. *Bisimulation equivalence is decidable for one-counter processes.*

More precisely it means that there is an algorithm which inputs (descriptions of) two one-counter processes $p(m)$, $p'(m')$ together with the respective one-counter machines M, M', and after a finite amount of time answers whether or not $p(m) \sim p'(m')$.

An additional result is expressed in the following theorem; here a process E is called *regular* iff there is a finite-state process p s.t. $E \sim p$.

Theorem 2.4. *Regularity (wrt bisimilarity) is decidable for one-counter processes.*

Each of the two decidability results is implied by two semidecision procedures. We can immediately note that semidecidability of *nonbisimilarity* $E \not\sim F$ follows from Proposition 2.2 since one-counter systems (as well as pushdown systems) are obviously admissible.

We finish this section by recalling some known notions and results which are then used in the proofs in Section 3.

Given a transition system $\mathcal{T} = (\mathcal{S}, \{\stackrel{a}{\longrightarrow}\}_{a\in\mathcal{A}})$, we define the class of all *n-incompatible processes* as $INC_n^{\mathcal{T}} = \{E \mid \forall F \in \mathcal{S} : E \not\sim_n F\}$.

More specific variants of the following two propositions were used in [JM95], [JE96].

Proposition 2.5. *For any n, $E \sim F$ implies that $E \sim_n F$ and $E \not\rightarrow^* INC_n^{\mathcal{T}(F)}$. In addition, the implication can be reversed for any n s.t. $\sim_{n-1}$ coincides with $\sim_n$ (and hence with $\sim$) on $\mathcal{T}(F)$.*

Corollary 2.6. *Let A be a finite transition system with k states. For any states p, q, it holds that $p \sim_{k-1} q$ iff $p \sim_k q$ (iff $p \sim q$). It yields for any process E and a state p of A: $E \sim p$ iff $E \sim_k p$ and $E \not\rightarrow^* INC_k^A$.*

The *distance* of a process E to F, denoted by $Dist(E, F)$, is the length of the shortest sequence u s.t. $E \stackrel{u}{\longrightarrow} F$; if F is not reachable from E, we put $Dist(E, F) = \infty$. For a set $\mathcal{F}$ of processes, we define $Dist(E, \mathcal{F}) = min\{Dist(E, F) \mid F \in \mathcal{F}\}$.

Proposition 2.7. *If $E \sim F$ then $Dist(E, \mathcal{F}) = Dist(F, \mathcal{F})$ for any quotient class $\mathcal{F}$ of $\sim_n$ on the set of all processes.*

We need the notion of *semilinear sets*. An important fact is that they are precisely the *sets expressible in Presburger arithmetic* (cf. [GS66]); we will use it implicitly when arguing that some sets are semilinear.

A set $V \subseteq \mathcal{N}^r$ of vectors ($r \geq 1$) is *linear* if there is a *base vector* $\vec{y}$ and *period vectors* $\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_m$ in $\mathcal{N}^r$ such that $V = \{\vec{y} + \sum_{i=1}^{m} c_i\vec{x}_i \mid c_i \in \mathcal{N}\}$.
V is *semilinear* if it is a finite union of linear sets.

In fact, here we are mainly interested in dimensions $r = 1, 2$. The next fact on *one-dimensional* semilinear sets is easily derivable:

Proposition 2.8. *Suppose a set $V \subseteq \mathcal{N}$. Then:*

1/ If there are $c, \delta \in \mathcal{N}$ s.t. $\forall m > c : m \in V \Rightarrow m + \delta \in V$ then V is semilinear.

2/ If V is semilinear then there are constants c and Δ s.t. for any $m > c$, the value $m \bmod \Delta$ determines whether $m \in V$ or $m \notin V$.

3 Proofs

In this section we always (implicitly) suppose a given one-counter machine M with k states (and the stack alphabet $\{X, Z\}$); the states are denoted by p, q (often primed or with subscripts).

Subsection 3.1 proves the crucial fact of this paper (Proposition 3.3) which shows that the set $\{(m, n) \mid p(m) \sim q(n)\}$ is semilinear for any p, q. Subsections 3.2 and 3.3 then prove the theorems.

In the proofs we need the notion of the underlying automaton A_M which behaves like M as long as the bottom of the stack is not reached, and also the notion of processes which are 'Basically Incompatible' with (states of) A_M:

The *underlying finite automaton* A_M (viewed as a finite transition system) has the same set of states as M, and it has the transition $p \xrightarrow{a} q$ iff M has a basic transition $pX \xrightarrow{a} q\alpha$ ($\alpha \in \{X\}^*$).

We define $BInc = \{p(m) \mid p(m) \in INC_k^{A_M}\} = \{p(m) \mid p(m) \not\sim_k q$ for each state $q\}$.

When we observe that $p(m) \sim_k p$ for $m \geq k$, the next lemma is clear:

Lemma 3.1. *If $p(m) \in BInc$ then $m < k$. Therefore $BInc$ is a finite, and effectively computable, set.*

Due to corollary 2.6 we can add (recall that k denotes the number of states of M and hence also of A_M):

Lemma 3.2. *For $m \geq k$ (and any state p), $p(m) \not\sim p$ iff $p(m) \to^* BInc$.*

Notation. By $p(m) \to^*_{\geq r} q(n)$ ($r \in \mathcal{N}$) we mean that there is a path $p(m) = q_1(n_1) \to q_2(n_2) \to \ldots \to q_s(n_s) = q(n)$ s.t. $n_i \geq r$ for $i = 1, 2, \ldots, s$. By $p(m) \to^*_{POS} q(n)$ (POSitive) we mean that $p(m) \to^*_{\geq 1} q(n)$.

Observe the obvious fact (used implicitly in what follows): if $r \geq 1$ then $p(m) \to^*_{\geq r} q(n)$ iff $p(m + \delta) \to^*_{\geq r+\delta} q(n + \delta)$ for any $\delta \in \mathcal{N}$. In particular $p(m) \to^*_{POS} q(n)$ implies $p(m + \delta) \to^*_{POS} q(n + \delta)$.

3.1 Semilinearity Proof

This subsection is devoted to a proof of the next crucial proposition:

Proposition 3.3. *For any one-counter machine and its states p, q, the set $\{(m,n) \mid p(m) \sim q(n)\}$ is semilinear.*

First observe that if $p(m) \rightarrow^* BInc$ and $q(n) \not\rightarrow^* BInc$ then surely $p(m) \not\sim q(n)$ (cf. Proposition 2.7). Therefore the set $B = \{(m,n) \mid p(m) \sim q(n)\}$ can be written as $B = B_1 \cup B_2$ where

$$B_1 = \{(m,n) \mid p(m) \sim q(n), p(m) \not\rightarrow^* BInc, q(n) \not\rightarrow^* BInc\},$$

$$B_2 = \{(m,n) \mid p(m) \sim q(n), p(m) \rightarrow^* BInc, q(n) \rightarrow^* BInc\}.$$

Therefore it suffices to show semilinearity of B_1 and B_2.

The next lemma is a means for proving semilinearity of B_1.

Lemma 3.4. *For any state p (of the one-counter machine M), the set $\{m \mid p(m) \rightarrow^* BInc\}$ is semilinear; therefore also $\{m \mid p(m) \not\rightarrow^* BInc\}$ is semilinear.*

Proof. Recall that we suppose M with k states; let $\mathcal{P}$ be the state set.

We have to show semilinearity of $R = \{m \mid p(m) \rightarrow^* BInc\}$. For any $Q \subseteq \mathcal{P}$ we define the set $R_Q \subseteq R$ as follows: $m \in R_Q$ iff there is a 'witness' path

$$p(m) = q_1(n_1) \rightarrow q_2(n_2) \rightarrow \ldots \rightarrow q_s(n_s) \in BInc \tag{1}$$

s.t. $q_i \in Q$ for $i = 1, 2, \ldots, s'$ where $s' \leq s$ is the maximum number s.t. $n_i \geq 1$ for $i = 1, 2, \ldots, s'$ (the path goes through states from Q solely while after the first reaching of the stack bottom—if it happens at all—there are no restrictions).

It is clear that $R_{\mathcal{P}} = R$ and it suffices to show semilinearity of all R_Q. We proceed by induction on $|Q|$.

When $Q = \emptyset$ then R_Q is obviously semilinear ($R_Q = \emptyset$ or $R_Q = \{0\}$).

Now we show semilinearity of R_Q, $|Q| > 0$, while supposing semilinearity for each $R_{Q'}$, $|Q'| < |Q|$. Let some $m \geq 2k$ be in R_Q (otherwise R_Q is finite, hence semilinear) and let (1) be a relevant witness path; recall that $k > n_s$ (Lemma 3.1). We can take the leftmost subsequence $q_{i_1}(m)$, $q_{i_2}(m-1)$, $\ldots$, $q_{i_{k+1}}(m-k)$; due to the pigeonhole principle, there is $q = q_{i_a} = q_{i_b}$ for $a \neq b$. Therefore $p(m) \rightarrow^*_{\geq n'_1} q(n'_1) \rightarrow^*_{\geq n'_2} q(n'_2) \rightarrow^* q_s(n_s) \in BInc$ where $\delta = n'_1 - n'_2 > 0$, $n'_2 > 0$; hence $q(n+\delta) \rightarrow^*_{\geq n} q(n)$ for any $n > 0$.

We can write $R_Q = R^q_Q \cup R_{Q \setminus \{q\}}$ where

$$R^q_Q = \{m \in R_Q \mid \text{there is a witness path with } q = q_i \text{ for some } i, 1 \leq i \leq s'\}.$$

Since $m \in R_Q^q$ obviously implies $m+\delta \in R_Q^q$, R_Q^q is semilinear (cf. Proposition 2.8 1/); semilinearity of $R_{Q\setminus\{q\}}$ follows from the induction hypothesis. $\square$

Corollary 3.5. *$B_1 = \{(m,n) \mid p(m) \sim q(n), p(m) \not\to^* BInc, q(n) \not\to^* BInc\}$ is semilinear.*

Proof. Given $r < k$, consider $B_1(r,-) = \{n \mid (r,n) \in B_1\}$ Note that for any $n \in B_1(r,-)$, $n \geq k$ implies $q(n) \sim q$. Therefore when $B_1(r,-)$ is infinite, it is the union of a finite set and the set $\{n \geq k \mid q(n) \not\to^* BInc\}$; in any case, $B_1(r,-)$ is semilinear. Semilinearity of $B_1(-,r) = \{m \mid (m,r) \in B_1\}$ can be established similarly. B_1 can be written

$$B_1 = \bigcup_{r=0}^{k-1}\{(r,n) \mid n \in B_1(r,-)\} \,\cup\, \bigcup_{r=0}^{k-1}\{(m,r) \mid m \in B_1(-,r)\} \,\cup\, B_1'$$

where

$$B_1' = \{(m,n) \mid m \geq k, n \geq k, p(m) \sim q(n), p(m) \not\to^* BInc, q(n) \not\to^* BInc\}.$$

B_1' is either empty (when $p \not\sim q$) or equals to $\{(m,n) \mid m \geq k, n \geq k, p(m) \not\to^* BInc, q(n) \not\to^* BInc\}$ (when $p \sim q$).

Thus semilinearity of B_1 is clear. $\square$

We also need another corollary.

Corollary 3.6. *There are constants c and Δ s.t. for any p and any $m > c$, the value $m \bmod \Delta$ determines whether or not $p(m) \to^* BInc$.*

Proof. For any state p, we get the relevant c_p, Δ_p due to Proposition 2.8 2/. The constant c desired here can be taken as the maximum of c_p's and Δ can be taken as the product of Δ_p's. $\square$

Our aim now is to show semilinearity of

$$B_2 = \{(m,n) \mid p(m) \sim q(n), p(m) \to^* BInc, q(n) \to^* BInc\}$$

Notation. $Dist(p(m), BInc)$ will be denoted by $Dist(p(m))$ for short.

Since $Dist(p(m)) = Dist(q(n))$ is a necessary condition for $p(m) \sim q(n)$, we will explore which relation it imposes for m and n. First we show that $Dist(p(m))$ is, in fact, linear (when finite) in m with the provision that the coefficient depends on m mod Δ. Here and further, Δ is taken from Corollary 3.6.

Lemma 3.7. *There is a constant $d \in \mathcal{N}$, and for any state p and any congruence class $\langle i \rangle_{mod\ \Delta}$ $(0 \le i \le \Delta - 1)$ there is a rational constant k' s.t. the following holds for any $m, m \equiv i(mod\ \Delta)$: if $Dist(p(m))$ is finite then*

$$Dist(p(m)) \in \langle k'm - d, k'm + d \rangle.$$

Proof. Suppose some p and $\langle i \rangle_{\text{mod } \Delta}$. In the proof, for each number denoted by m we implicitly suppose $m \equiv i(\text{mod } \Delta)$. We show that there are k' and d' s.t. $Dist(p(m)) \in \langle k'm - d', k'm + d' \rangle$, by which we will be done (the desired d can be taken as the maximum of all relevant constants d').

Observe that $p(m) \rightarrow^* BInc$, for a large m, implies a *decreasing cycle*:

$$p(m) \rightarrow^*_{POS} q(n+\delta) \rightarrow^*_{\ge n} q(n) \rightarrow^* BInc \text{ for some } q, n > 0, \delta > 0.$$

Let $Q = \{ q \mid p(m) \rightarrow^*_{POS} q(n) \rightarrow^* BInc \text{ for some } m, n \}$. Now let q' be a state of Q which allows a decreasing cycle $q'(n+\delta_w) \xrightarrow{w}_{\ge n} q'(n)$ (for some w, $\delta_w > 0$, and all $n \ge 1$) with the *best decreasing rate*—i.e. $\delta_w/|w|$ is maximal possible. The existence of such q' can be easily derived (by 'pigeonhole principle reasoning' we could suppose $|w| \le k$). Moreover we can safely suppose that δ_w is a multiple of Δ (otherwise we take w^Δ which yields the same decreasing rate), and thus $q'(n+\delta_w) \rightarrow^* BInc$ iff $q'(n) \rightarrow^* BInc$ for $n > c$, c taken from Proposition 3.6.

Let us choose $m > c + \delta_w + k$ s.t. $p(m) \xrightarrow{u}_{POS} q'(n) \rightarrow^* BInc$ for some u and $n, c < n \le c + \delta_w$; denote $\delta_u = m - n$. Note that $p(m + j\Delta) \xrightarrow{u}_{POS} q'(n + j\Delta) \rightarrow^* BInc$ for any $j \ge 0$.

Now let $d_0 = |u|$ and

$$d_1 = max\{Dist(p'(c+x)) \mid x \in \{0, 1, \ldots, \delta_w\} \text{ and } Dist(p'(c+x)) \text{ is finite}\}$$

Then it is clear that for any $m > c + \delta_w + k$

$$Dist(p(m)) \le d_0 + \Big((m - \delta_u - c)/\delta_w\Big)|w| + d_1$$

On the other hand it is easily verifiable that

$$Dist(p(m)) \ge \Big((m - \delta_u - c)/\delta_w - 1\Big)|w|.$$

Calculating the desired k', d' is now a technical routine (d' has to be chosen large enough to 'cover' the finitely many $m \le c + \delta_w + k$ as well). □

Corollary 3.8. *There is a constant* $d \in \mathcal{N}$ *s.t. for any* p, q *and congruence classes* $\langle i \rangle_{mod\ \Delta}$, $\langle j \rangle_{mod\ \Delta}$, *there is a rational constant* k' *s.t. the following holds for any* m, n, $m \equiv i(mod\ \Delta)$, $n \equiv i(mod\ \Delta)$: *if* $Dist(p(m)) = Dist(q(n)) < \infty$ *then* $n \in \langle k'm - d, k'm + d \rangle$.

Proof. Because there are constants k_1, k_2 and d' s.t. $Dist(p(m)) \in \langle k_1 m - d'$, $k_1 m + d' \rangle$ and $Dist(q(n)) \in \langle k_2 n - d', k_2 n + d' \rangle$ then it must hold $k_2 n - d' \leq k_1 m + d'$ and $k_2 n + d' \geq k_1 m - d'$. Hence we have $mk_1/k_2 - 2d'/k_2 \leq n \leq mk_1/k_2 + 2d'/k_2$. ☐

Recall that our aim is to show semilinearity of B_2. We already know that there is $d \in \mathcal{N}$ and a finite set $K = \{k_1, k_2, \ldots, k_r\}$ of rational constants s.t. it suffices, for each $k' \in K$, to show semilinearity of the set

$$B_{k'} = \{(m,n) \mid p(m) \sim q(n), n \in \langle k'm - d, k'm + d \rangle\}.$$

(The union of $B_{k'}$'s consists of B_2 and a subset of B_1 which is obviously semilinear, i.e. expressible in the Presburger arithmetic).

In fact, we will consider only the subset of $B_{k'}$ where $m > c$ for a sufficiently large c (the rest being finite and therefore causing no problems); c will be chosen so that for any m, n, $m > c$, $|n - k'm| \leq d$, the following holds: for any p', q' and any moves $p'(m) \xrightarrow{a} p''(m')$, $q'(n) \xrightarrow{a} q''(n')$ it is ensured that $|n' - k''m'| > d$ for each $k'' \in K$, $k'' \neq k'$ (a pair of moves cannot lead from '$B_{k'}$-area' into '$B_{k''}$-area').

Given k', let us denote $Cut(m) = \cap_{i=0}^{\infty} Cut_i(m)$ where $Cut_i(m) = \{(p', q', x) \mid x \in \{-d, -d+1, \ldots, d\}, p'(m) \sim_i q'(round(k'm) + x)\}$.

Observe that there surely is an infinite sequence $m_0 < m_1 < m_2 < \ldots$ s.t. for all $i \geq 0$: $k'm_i$ is integer, $m_{i+1} - m_i \equiv 0(\text{mod } \Delta)$, $k'm_{i+1} - k'm_i \equiv 0(\text{mod } \Delta)$. Since, for any m, $Cut(m)$ is a boundedly finite set, there are surely m, m' satisfying the assumption of the next lemma; and it is easily observable that the lemma demonstrates semilinearity of $B_{k'}$ and thus finishes the proof of Proposition 3.3.

Lemma 3.9. *When* $Cut(m) = Cut(m')$ *for sufficiently large* m *where* $m < m'$, $k'm, k'm'$ *are integers,* $m' - m \equiv 0(mod\ \Delta)$, $k'm' - k'm \equiv 0(mod\ \Delta)$, *then* $Cut(m+\delta) = Cut(m' + \delta)$ *for any* $\delta \geq 0$.

Proof. We show $Cut(m + \delta) \subseteq Cut(m' + \delta)$ while the other inclusion will be completely symmetric.

In fact, we show by induction on i that $(p, q, x) \in Cut(m + \delta)$ implies $(p, q, x) \in Cut_i(m' + \delta)$ for all i; for $i = 0$ it is trivial as well as for $\delta = 0$.

Induction hypothesis: for any p, q, x, δ, if $(p, q, x) \in Cut(m + \delta)$ then $(p, q, x) \in Cut_i(m' + \delta)$.

Now we consider arbitrary (but fixed) $p, q, x, \delta \geq 1$ s.t. $(p, q, x) \in Cut(m+\delta)$ and we show that $(p, q, x) \in Cut_{i+1}(m' + \delta)$ by which the whole proof will be finished.

In other words, denoting $m_1 = m+\delta$, $n_1 = round(k'(m+\delta))+x$, $m_2 = m'+\delta$, $n_2 = round(k'(m' + \delta)) + x$, we suppose $p(m_1) \sim q(n_1)$ and we have to show $p(m_2) \sim_{i+1} q(n_2)$.

Let $p(m_2) \xrightarrow{a} p'(m_2 + y)$ $(-1 \leq y \leq max$, max depending on the machine $M)$. There is the corresponding move $p(m_1) \xrightarrow{a} p'(m_1+y)$ and there has to be a move $q(n_1) \xrightarrow{a} q'(n_1+z)$ $(-1 \leq z \leq max)$ s.t. $p'(m_1+y) \sim q'(n_1+z)$. We claim that the corresponding move $q(n_2) \xrightarrow{a} q'(n_2+z)$ yields $p'(m_2+y) \sim_i q'(n_2+z)$.

When $|k'(m_1 + y) - (n_1 + z)| \leq d$ (hence also $|k'(m_2 + y) - (n_2 + z)| \leq d$), it follows from the inductive hypothesis. Otherwise $Dist(p'(m_1 + y)) = Dist(q'(n_1 + z)) = \infty$ and $p' \sim q'$. But then also $Dist(p'(m_2 + y)) = Dist(q'(n_2 + z)) = \infty$ (recall the property of Δ); therefore $p'(m_2 + y) \sim q'(n_2 + z)$.

The remaining parts of the proof are completely similar. □

3.2 Decidability of Bisimilarity

Now we can provide a proof for Theorem 2.3:

Theorem. *Bisimulation equivalence is decidable for one-counter processes.*

Proof. First notice that we can always consider the bisimilarity problem instance '$p(m) \sim q(n)$?' where $p(m)$, $q(n)$ are associated to the same one-counter machine (which can be achieved by taking the union of two machines—i.e. union of action sets, and disjoint union of state sets and basic transition sets).

Recall that it suffices to show *semi*decidability for '$p(m) \sim q(n)$?' (cf. Proposition 2.2). Now due to Proposition 3.3 it suffices to generate all bisimulation candidates $\mathcal{R}$ s.t. the set $\{(m', n') \mid (p'(m'), q'(n')) \in \mathcal{R}\}$ is semilinear for each pair of states p', q', and for each such candidate to check if $\mathcal{R}$ actually is a bisimulation containing $(p(m), q(n))$. (Descriptions of) such candidate relations can be obviously generated in a systematic way, and the condition to be checked is easily seen to be expressible in Presburger arithmetic, which is decidable (cf. e.g. [Opp78]). □

3.3 Decidability of Regularity

Here we provide a proof for Theorem 2.4:

Theorem. *Regularity (wrt bisimilarity) is decidable for one-counter processes.*

Proof. Semidecidability of regularity of $p(m)$ follows from Theorem 2.3. (We can generate all finite state processes $\mathcal{F}$, viewed as special cases of one-counter processes, and to check for each of them whether $p(m) \sim \mathcal{F}$).

Semidecidability of nonregularity will follow when we show that $p(m)$ is nonregular iff there is a path

$$p(m) \rightarrow^* p'(m_1) \rightarrow^*_{POS} p'(m_2) \rightarrow^*_{POS} q'(n_1) \rightarrow^*_{POS} q'(n_2) \rightarrow^* BInc$$

where $m_1 < m_2, n_1 > n_2$.

The existence of such a path ensures for any $i \geq 0$ that

$$p(m) \rightarrow^* p'(m_2 + i(n_1 - n_2)(m_2 - m_1)) \rightarrow^* q'(n_1 + i(m_2 - m_1)(n_1 - n_2)) \rightarrow^* BInc$$

which implies that there are reachable states with arbitrarily large (but finite) distances to $BInc$—and this obviously implies nonregularity of $p(m)$. The opposite direction can be also easily established. $\square$

4 Further Comments

The example of a pushdown process used in [Sti96]

$$pX \xrightarrow{a} pXX, pX \xrightarrow{c} q\varepsilon, pX \xrightarrow{b} r\varepsilon, qX \xrightarrow{d} sX, sX \xrightarrow{d} q\varepsilon, rX \xrightarrow{d} r\varepsilon$$

can be easily transformed in a one-counter process with the isomorphic transition system. This process can serve as an example of a one-counter process which is not equivalent to a BPA-process, nor a BPP-process, and when adding a rule $pX \xrightarrow{f} q_{fin}$ we get a one-counter process not equivalent to any normed pushdown process.

References

[BCS96] Burkart O., Caucal D. and Steffen B.: Bisimulation collapse and the process taxonomy; in Proc. CONCUR'96, *Lecture Notes in Computer Science*, Vol. 1119 (Springer, 1996) 247–262

[CHM93] Christensen S., Hirshfeld Y. and Moller F.: Bisimulation equivalence is decidable for all Basic Parallel Processes, in Proc. CONCUR'93, *Lecture Notes in Computer Science*, Vol. 715 (Springer, 1993) 143–157

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

[Esp95] Esparza J.: Petri nets, commutative context-free grammars, and Basic Parallel Processes; in Proc. Fundamentals of Computation Theory (FCT) 1995, *Lecture Notes in Computer Science*, Vol. 965 (Springer, 1995) 221–232

[GS66] Ginsburg S. and Spanier E.: Semigroups, Presburger formulas, and languages; *Pacific J. of Mathematics* **16** (1966) 285–296

[Hir93] Hirshfeld Y.: Petri nets and the equivalence problem; in Proc. Computer Science Logic (CSL) '93, *Lecture Notes in Computer Science*, Vol. 832 (Springer, 1994) 165–174

[Jan93] Jančar P.: Decidability questions for bisimilarity of Petri nets and some related problems; Techn.rep. ECS-LFCS-93-261, Dept. of comp. sci., Univ. of Edinburgh, UK, April 1993
(cf. also Jančar P.: Undecidability of Bisimilarity for Petri Nets and Related Problems; *Theoretical Computer Science* **148** (1995) 281–301)

[JE96] Jančar P., Esparza J.: Deciding finiteness of Petri nets up to bisimulation; in Proc. ICALP'96, Paderborn, Germany, July 1996, *Lecture Notes in Computer Science*, Vol. 1099 (Springer, 1996) 478–489

[JM95] Jančar P., Moller F.: Checking regular properties of Petri nets; in Proc. CONCUR'95, Philadelphia, U.S.A., August 1995, *Lecture Notes in Computer Science*, Vol. 962 (Springer, 1995) 348–362

[Mil89] Milner R.: *Communication and Concurrency* (Prentice Hall, 1989)

[Opp78] Oppen D.C.: A $2^{2^{2^{pn}}}$ upper bound on the complexity of Presburger Arithmetic, *J. of Comp. and System Sci.* **16** (1978) 323–332

[Sti96] Stirling C.: Decidability of bisimulation equivalence for normed pushdown processes; in Proc. CONCUR'96, *Lecture Notes in Computer Science*, Vol. 1119 (Springer, 1996) 217–232

Publications in the FI MU Report Series are in general accessible via WWW and anonymous FTP:

`http://www.fi.muni.cz/informatics/reports/`
`ftp  ftp.fi.muni.cz (cd pub/reports)`

Copies may be also obtained by contacting:

**Faculty of Informatics
Masaryk University
Botanická 68a
602 00 Brno
Czech Republic**