Bisimilarity of one-counter processes is PSPACE-complete

Stanislav Böhm[1], Stefan Göller[2], and Petr Jančar[1]

[1] Technical University of Ostrava, Department of Computer Science, Czech Republic
[2] Universität Bremen, Institut für Informatik, Germany

Abstract. A one-counter automaton is a pushdown automaton over a singleton stack alphabet. We prove that the bisimilarity of processes generated by nondeterministic one-counter automata (with no ε-steps) is in PSPACE. This improves the previously known decidability result (Jančar 2000), and matches the known PSPACE lower bound (Srba 2009). Moreover, we prove PTIME-completeness of regularity of one-counter processes (i.e., their finiteness up to bisimilarity).

1 Introduction

Among the different notions of behavioral equivalences the notion of (strong) *bisimulation* plays an important rôle (cf, e.g., [13]). For instance, various logics can be characterized as the bisimulation-invariant fragment of richer logics. A famous theorem due to van Benthem states that the properties expressible in modal logic coincide with the bisimulation-invariant properties expressible in first-order logic [25]. Similar such characterizations have been obtained for the modal μ-calculus [6] and for CTL* [14]. Another important notion is *weak bisimulation* that generalizes strong bisimulation by allowing distinguished ε-moves in the transitions that allow to mimic internal behavior.

There are numerous further notions of equivalences. For more a more detailed treatment of the different behaviorial equivalences in the context of concurrency theory we refer to [26].

Hence it is natural to formulate the *(weak/strong) bisimilarity problem*, i.e. to decide if two given states of a given transition system are weakly/strongly bisimilar. On *finite transition systems* both weak and strong bisimilarity is well-known to be complete for deterministic polynomial time [1].

In the last twenty years a lot of research has been devoted to checking behavioral equivalence of infinite-state systems, see [20] for an up-to-date record. In the setting of infinite-state systems, see also [11] for Mayr's classification of infinite-state systems, the situation is less clear. There are numerous classes of infinite-state systems for which *decidability* of bisimilarity is not known. Two such intricate open problems are (i) weak bisimilarity on basic parallel processes (a subclass of Petri nets) and (ii) bisimilarity of PA/PAD. On the positive side we mention an important result by Sénizergues who shows that bisimilarity on equational graphs [17] (a slight generalization of pushdown graphs) is decidable. See also in Stirling's unpublished paper [22] for a shorter proof of this by using ideas from concurrency theory.

When focussing on the *computational complexity* of bisimilarity checking of infinite-state systems for which this problem is decidable, the sitution becomes even worse. There are only very few classes for which the precise computational complexity of checking bisimilarity is known. For instance, when coming back to the above-mentioned positive results by Sénizergues/Stirling concerning (slight extensions of) pushdown graphs, a primitive recursive upper bound is not yet known. To mention one of the few results on infinite systems where the upper and lower complexity bounds match, we refer to [8], where it is shown that bisimilarity on basic parallel processes is PSPACE-complete.

In this paper we study the computational complexity of deciding strong bisimilarity over processes generated by one-counter automata. One-counter automata are pushdown automata over a singleton stack alphabet. In recent years, one-counter automata have gained interest in the verification community, see for example [2, 4, 5, 3, 23]. On one-counter processes weak bisimilarity is shown to be undecidable in [12] via a reduction from the emptiness problem of Minsky machines.

For strong bisimilarity the third author established decidability in [7], however without providing any precise complexity bounds. In an unpublished article [27] Yen analyses the approach of [7] and is able to derive a triply exponential space upper bound from it. A PSPACE lower bound for bisimilarity is proven by Srba [21]. This lower bound already holds over one-counter automata that cannot test for zero and whose actions can moreover be restricted to be *visible* (so called *visibly one-counter nets*), i.e. that the label of

the action determines if the counter is incremented, decremented, or not modified respectively. For visibly one-counter automata it is proven in [21] that strong bisimilarity is in PSPACE via a reduction the model checking problem of the modal μ-calculus over one-counter processes [18]. For bisimilarity on general one-counter processes, in particular when dropping the visibility restriction, the situation is surely more involved.

The main main result of this paper is that we close the complexity gap for bisimilarity on one-counter processes from above and hence establish PSPACE-completeness. We provide a nondeterministic procedure implementable in polynomial space which generates a bisimulation relation *on-the-fly*. In a nutshell, for checking bisimilarity for a given pair $(p(m), q(n))$ of processes, the output of our procedure is either (i) surely bisimilar, (ii) surely non-bisimilar, or (iii) it cannot make any sure statement and declares the currently checked pair of processes as a *candidate*. Our algorithm needs in fact only polynomial time for making sure answers (i) and (ii). For checking if a candidate pair is bisimilar our procedure guesses the bisimilarity status of pairs of processes that are close in a polynomially bounded neighborhood of $(p(m), q(n))$. We establish correctness of our procedure by proving that we need to postpone candidate checking only for exponentially many steps.

Another natural problem we consider is deciding *regularity* (with respect to bisimulation) which asks if, for a given a one-counter process, there is a state of some finite system that is bisimilar to it. Decidability of this problem was proven in [7] and according to [21] it follows from [1] and [19] that the problem is also hard for P. We prove that regularity is P-complete and hence give a new upper bound and a simpler lower bound proof than the one that one obtains by combining [1] and [19].

This paper is organized as follows. In Section 2 we introduce basic notation and define the algorithmic problems that we are interested in. The PSPACE upper bound for bisimilarity of one-counter processes is proven in Section 3. However, the proofs of some of the technical lemmas in Section 3 are postponed to Section 4 and Section 5. Our results on regularity checking of one-counter proceeses are proven in Section 6.

2 Definitions

Let $\mathbb{N}$ denote the set of nonnegative integers $\{0, 1, 2, \ldots\}$, and $\mathbb{Z}$ the set of all integers. For each $i, j \in \mathbb{Z}$ we define $[i, j] = \{k \in \mathbb{Z} \mid i \leq k \leq j\}$ and $[j] = [1, j]$. Given a set X, by $|X|$ we denote its cardinality.

Transition systems. A *(labeled) transition system* is a triple $T = (S, \mathsf{A}, \{\xrightarrow{a} \mid a \in \mathsf{A}\})$, where S is a set of *states*, A is a set of *actions*, and $\xrightarrow{a} \subseteq S \times S$ is a set of a-labeled *transitions* for each action $a \in \mathsf{A}$. We define $\longrightarrow = \bigcup_{a \in \mathsf{A}} \xrightarrow{a}$ and prefer to use the infix notation $s_1 \xrightarrow{a} s_2$ (resp. $s_1 \longrightarrow s_2$) instead of $(s_1, s_2) \in \xrightarrow{a}$ (resp. $(s_1, s_2) \in \longrightarrow$). We say that T is *finite* if S and A are finite; we then define the *size* of T as $|T| = |S| + |\mathsf{A}| + \sum_{a \in \mathsf{A}} |\xrightarrow{a}|$.

Bisimulation equivalence. Let $T = (S, \mathsf{A}, \{\xrightarrow{a} \mid a \in \mathsf{A}\})$ be a transition system. A binary relation $R \subseteq S \times S$ is *bisimulation* if for each $(s_1, s_2) \in R$ the following *bisimulation condition* holds:

- for each $s_1' \in S$ and each $a \in \mathsf{A}$, where $s_1 \xrightarrow{a} s_1'$, there is some $s_2' \in S$ such that $s_2 \xrightarrow{a} s_2'$ and $(s_1', s_2') \in R$, and
- for each $s_2' \in S$ and each $a \in \mathsf{A}$, where $s_2 \xrightarrow{a} s_2'$, there is some $s_1' \in S$ such that $s_1 \xrightarrow{a} s_1'$ and $(s_1', s_2') \in R$.

We say that states s_1 and s_2 are *bisimilar*, abbreviated by $s_1 \sim s_2$, whenever there exists a bisimulation R such that $(s_1, s_2) \in R$. We observe that bisimilarity is an equivalence relation on S. We note that the union of bisimulations is a bisimulation and that $\sim$ is the maximal bisimulation on S. Bisimilarity is naturally defined also between states of different transition systems (by considering their disjoint union).

One-counter automata. A *one-counter automaton (OCA)* is a tuple $M = (Q, \mathsf{A}, \delta_0, \delta_{>0})$, where Q is a finite non-empty set of *control states*, A is a finite set of actions, $\delta_0 \subseteq Q \times \{0,1\} \times \mathsf{A} \times Q$ is a finite set of *zero transitions*, and $\delta_{>0} \subseteq Q \times \{-1,0,1\} \times \mathsf{A} \times Q$ is a finite set of *positive transitions*. We note that there are no ε-steps in M. The *size* of a one-counter automaton is defined as $|M| = |Q| + |\mathsf{A}| + |\delta_0| + |\delta_{>0}|$. Each one-counter automaton $M = (Q, \mathsf{A}, \delta_0, \delta_{>0})$ defines the transition system $T_M = (Q \times \mathbb{N}, \mathsf{A}, \{\xrightarrow{a} \mid a \in \mathsf{A}\})$, where $(q,n) \xrightarrow{a} (q', n+i)$ if and only if either $n = 0$ and $(q,i,a,q') \in \delta_0$, or $n > 0$ and $(q,i,a,q') \in \delta_{>0}$. We will also denote this by $(q,n) \xrightarrow{(q,i,a,q')} (q, n+i)$ and furthermore extend this relation to *sequences of transitions* in the obvious way. We define $\longrightarrow = \bigcup_{a \in \mathsf{A}} \xrightarrow{a}$.

A *one-counter net* is a one-counter automaton, where $\delta_0 \subseteq \delta_{>0}$. State (q,m) of T_M, also called *one-counter process*, will be usually written as $q(m)$. Elements of $\delta_0 \cup \delta_{>0}$ are called *transitions*. Without formalities we use the natural notions like a *path* $p(m) \xrightarrow{\sigma} q(n)$ where σ is a *sequence of transitions*.

Decision problems. We are particularly interested in the following two decision problems.

BISIMILARITY OF ONE-COUNTER PROCESSES

INPUT: A one-counter automaton M with two one-counter processes $p_0(m_0)$ and $q_0(n_0)$ of T_M, where both m_0 and n_0 are given in binary.
QUESTION: $p_0(m_0) \sim q_0(n_0)$?

We say that a *one-counter process* $q(n)$ is *$\sim$-regular* (or *finite up to bisimilarity*) if there is a finite transition system with some state s such that $q(n) \sim s$.

$\sim$REGULARITY OF ONE-COUNTER PROCESSES

INPUT: A one-counter automaton M and a one-counter process $p_0(m_0)$ of T_M, where m_0 is given in binary.
QUESTION: Is $p_0(m_0)$ $\sim$-regular?

Stratified bisimilarity and finite transition systems Given a transition system $T = (S, \mathsf{A}, \{\xrightarrow{a} \mid a \in \mathsf{A}\})$, on S we define the family of i-equivalences, $i \in \mathbb{N}$, $\sim_0 \supseteq \sim_1 \supseteq \sim_2 \supseteq \cdots$ as follows. We put $\sim_0 = S \times S$, and we have $s_1 \sim_{i+1} s_2$ if the following two conditions hold:

- for each $s_1' \in S$, $a \in \mathsf{A}$, where $s_1 \xrightarrow{a} s_1'$, there is some $s_2' \in S$ such that $s_2 \xrightarrow{a} s_2'$ and $s_1' \sim_i s_2'$;
- for each $s_2' \in S$, $a \in \mathsf{A}$, where $s_2 \xrightarrow{a} s_2'$, there is some $s_1' \in S$ such that $s_1 \xrightarrow{a} s_1'$ and $s_1' \sim_i s_2'$.

The following proposition is an instance of the result for image finite systems [13].

Proposition 1. *On states of T_M we have $\sim \; = \; \bigcap_{i \geq 0} \sim_i$.*

Standard partition arguments imply the following proposition [10, 16].

Proposition 2. *Given a finite transition system $F = (Q, \mathsf{A}, \{\xrightarrow{a} \mid a \in \mathsf{A}\})$, where $k = |Q|$, we have $\sim_{k-1} = \sim_k = \sim$ on Q. Moreover, (the partition of Q corresponding to) $\sim$ can be computed in polynomial time.*

3 A PSPACE upper bound for bisimilarity

In this section we prove that bisimilarity of one-counter processes is in PSPACE. If the context does not indicate otherwise, in what follows we (often implicitly) assume a fixed one-counter automaton $M = (Q, \mathsf{A}, \delta_0, \delta_{>0})$, using k for $|Q|$.

We proceed in five steps.

In Section 3.1 we show that when comparing a one-counter processes $p(m)$ with states of the *underlying finite transition system* of M (where the control states of M are the states and we have $q \xrightarrow{a} q'$ if in M

there is an a-labeled positive transition from q to q'), one can already gain some information concerning bisimilarity. In particular, inspired by [7], we prove that there is a polynomial-time computable set of *incomparable processes* that are useful to proving that certain pairs of processes are *surely bisimilar* or *surely non-bisimilar*. A necessary condition for two processes to be bisimilar it that their minimal distances to any incomparable process are the same.

In Section 3.2 we prove that for each process $q(n)$, where n is sufficently large, already the residue class modulo an exponentially large number determines if $q(n)$ can reach some incomparable process. Moreover, if the minimal distance from $q(n)$ to an incomparable process is finite, then we prove that this distance can be expressed as $\alpha \cdot n + \beta$, where α and β are rationals which can take only few values.

We call the pairs of one-counter processes that are neither surely bisimilar nor surely non-bisimilar *candidates*. We prove in Section 3.3 that candidates lie either in a small initial area or in few thin belts.

In Section 3.4 we view the (bisimulation) relations between one-counter processes from a different angle by regarding *colorings*, which are simply mappings from $Q \times Q \times \mathbb{N} \times \mathbb{N} \to \{\circ, \bullet\}$. We call such a coloring locally consistent, if it does not violate the bisimulation condition with respect to the transition system T_M. Hence, there is a natural one-to-one correspondence between locally consistent colorings and bisimulations. Then we prove a characterization of bisimilarity of one-counter processes: Two one-counter processes $p(m)$ and $q(n)$ are bisimilar if and only if there is a coloring χ that maps (p, q, m, n) to $\bullet$ and that is locally consistent only in some exponentially sized subset of $Q \times Q \times \mathbb{N} \times \mathbb{N}$.

We implement the characterization of bisimilarity given in Section 3.4 in Section 3.5: We guess such a suitable coloring and check local consistency. However, a naïve implementation would only yield a NEXPTIME upper bound. For proving implementability in PSPACE, we employ the result obtained in Section 3.3, namely that the actual guessing only needs to be done for candidate pairs: they in a small initial area or in in few thin belts.

The proofs of some lemmas of this section are postponed to later sections. We will prove precise bounds and give explicit polynomials. Therefore, we decided to list all constants $c_1 < c_2 < c_3 < c_4 < c_5$ that appear in the rest of the paper below:

$$\boxed{c_1 = 4}$$
$$\boxed{c_2 = 7c_1 = 28}$$
$$\boxed{c_3 = 2c_2 = 56}$$
$$\boxed{c_4 = 4c_3 = 224}$$
$$\boxed{c_5 = 4c_4 = 896}$$

3.1 The underlying finite transition system F_M and the set INC

We start by observing that if the counter value is large, then M behaves, for a long time, like a (nondeterministic) finite transition system; this is expressed by the following proposition. By F_M we denote the *finite transition system underlying* M; we put $F_M = (Q, \mathsf{A}, \{\xrightarrow{a} \mid a \in \mathsf{A}\})$, where $\xrightarrow{a} = \{(q_1, q_2) \in Q \times Q \mid \exists i : (q, i, a, q') \in \delta_{>0}\}$. ($F_M$ thus behaves as if the counter is positive, ignoring the counter changes.) In what follows, $p, q, r \in Q$ are viewed as control states of M or as states of F_M, depending on context.

Proposition 3. $p(m) \sim_m p$. *(Here $p(m)$ is a state of T_M, while p is a state of F_M.)*

This implies, e.g., that if $p \not\sim q$ (i.e., $p \not\sim_k q$) and $m, n \geq k$, then $p(m) \not\sim_k q(n)$ (and thus $p(m) \not\sim q(n)$). If $p \sim q$ then we can have $p(m) \not\sim q(n)$, due to the possibility of reaching zero. For making this more precise, we define the following set (as in [7]).

$$\text{INC} = \{\, r(\ell) \mid \forall q \in Q : r(\ell) \not\sim_k q \,\}.$$

The configurations in INC are *incompatible with* F_M in the sense that they are not bisimilar upto k moves with any state of F_M. The next proposition is straighforward.

Proposition 4. *If $r(\ell) \in$ INC then $\ell < k$. Moreover, INC can be constructed in polynomial time.*

Let $p(m)$ and $q(n)$ be processes. Let us define the *distance* between $p(m)$ and $q(n)$ as $\text{dist}(p(m), q(n)) = \min\{i \geq 0 \mid p(m) \longrightarrow^i q(n)\}$. It is obvious that if $p(m), q(n)$ are bisimilar then they must agree on the distance to INC; this is formalized by the next lemma. We define

$$\text{dist}(p(m)) \quad = \quad \min\{\text{dist}(p(m), r(l)) \mid r(l) \in \text{INC}\}$$

as the length of the shortest distance to some process in INC. Note that we put $\text{dist}(p(m)) = \omega$ if INC is unreachable from $p(m)$, denoted $p(m) \not\longrightarrow^* \text{INC}$.

Lemma 5. *If $p(m) \sim q(n)$ then dist$(p(m)) =$ dist$(q(n))$.*

The next lemma clarifies the opposite direction in the case of infinite distances.

Lemma 6. *If dist$(p(m)) = \omega$ then $p(m) \sim r$ for some $r \in Q$. Thus if dist$(p(m)) =$ dist$(q(n)) = \omega$ then $p(m) \sim q(n)$ if and only if there is some $r \in Q$ such that $p(m) \sim_k r \sim_k q(n)$.*

Proof. Firstly, we prove that the relation

$$R \quad = \quad \{(q_1(n_1), q_2(n_2)) \mid q_1(n_1) \sim_k q_1(n_2), \text{dist}(q_1(n_1)) = \text{dist}(q_2(n_2)) = \omega\}$$

is a bisimulation. For this, let $(q_1(n_1), q_2(n_2)) \in R$ and assume $q_1(n_1) \xrightarrow{a} q_1'(n_1')$ for some $a \in \mathsf{A}$. Since in particular $q_1(n_1) \notin \text{INC}$ there is some $r \in Q$ such that $q_1(n_1) \sim_k r$. Furthermore there is some $r' \in Q$ and some $q_2'(n_2')$ such that $q_2(n_2) \xrightarrow{a} q_2'(n_2)$ satisfying $q_1'(n_1') \sim_{k-1} r' \sim_{k-1} q_2'(n_2')$.It follows $q_1'(n_1') \sim_k r' \sim_k q_2'(n_2')$ by Proposition 2. Thus $(q_1'(n_1'), q_2'(n_2')) \in R$ as desired. The case when $q_2(n_2) \xrightarrow{a} q_2'(n_2')$ for some $a \in \mathsf{A}$ can be proven analogously.
Secondlly, since R is a bisimulation and $\text{dist}(p(m)) = \text{dist}(q(n)) = \omega$ we can deduce

$$p(m) \sim q(n) \quad \Leftrightarrow \quad (p(m), q(n)) \in R \quad \Leftrightarrow \quad p(m) \sim_k q(n) \quad \Leftrightarrow \quad \exists r \in Q : p(m) \sim_k r \sim_k q(n).$$

□

In Subsection 3.2 we look in more detail at the function $dist(p(m))$, which provides a useful constraint on bisimilar pairs. But before that, we partition the set $(Q \times \mathbb{N}) \times (Q \times \mathbb{N})$ into three categories. We say that a pair $(p(m), q(n))$ is

- *surely-positive* if $p(m) \sim_k q(n)$ and $dist(p(m)) = dist(q(n)) = \omega$
  (and thus surely $p(m) \sim q(n)$ by Lemma 6),
- *surely-negative* if $p(m) \not\sim_k q(n)$ or $dist(p(m)) \neq dist(q(n))$
  (and thus surely $p(m) \not\sim q(n)$),
- *candidate* otherwise, i.e., if $p(m) \sim_k q(n)$ and $dist(p(m)) = dist(q(n)) < \omega$.

In the following, let $\textsc{Sure} = \textsc{SurePos} \cup \textsc{SureNeg}$ denote the union of all surely positive pairs SUREPOS and all surely negative pairs SURENEG. By CAND we denote the set of candidates. Without risk of confusion, we will treat pairs of processes $\langle p(m), q(n)\rangle$ as the four-tuple $(p, q, m, n) \in Q \times Q \times \mathbb{N} \times \mathbb{N}$ and vice versa.

Lemma 7. *Membership in* SUREPOS *and* SURENEG *is decidable in polynomial time. Moreover, for each $(p, q, m, n) \in$* SURE *membership in* SUREPOS *is determined already by p, q and the residue classes of m and of n modulo LCM$[k]$, provided $m, n > c_3 k^6$.*

Proof. The lemma follows immediately from Lemma 8 and from the fact that membership in $\sim_k$ obviously decidable in polynomial time. □

3.2 On distances to INC

The goal of this this section is to extract more information from states that have the same distance to INC. We prove that for states $p(m)$, where m is sufficiently but polynomially large, $\text{dist}(p(m)) \stackrel{?}{=} \omega$ is determined already by the residue class of m modulo some exponentially big number and p. Moreover, we have that $\text{dist}(p(m)) < \omega$ implies that $\text{dist}(p(m))$ is precisely $\alpha_i \cdot m + \beta_i$ for rationals α_i and β_i, whose denominator is in $\{1, \ldots, k\}$ and that moreover only depend on the state p and on m's residue class i modulo some exponentially bounded number.

Before me make this statement more precise, let us introduce some more notation. Let $\text{LCM}[k]$ be the least common multiple of the numbers $1, \ldots, k$. Nair proved in [15] that $2^k \leq \text{LCM}[k] \leq 4^k$ in case $k \geq 9$. A *ratio* is a fraction $\alpha = \frac{a}{b}$, where $1 \leq a \leq b \leq k$.

Lemma 8. *For every $q \in Q$ and every $0 \leq i < \text{LCM}[k]$ there exists some ratio $\alpha = \alpha(q, i)$ and some offset $\beta = \beta(q, i) \in \mathbb{Q}$ with $|\beta| \leq c_3 k^4$ such that for every $n > c_3 k^6$ with $n \equiv i$ mod $\text{LCM}[k]$ the following two statements hold:*

(1) The residue class i determines if $\text{dist}(q(n)) = \omega$.
(2) If $\text{dist}(q(n)) < \omega$, then $\text{dist}(q(n)) = \alpha \cdot n + \beta$.

Moreover $\text{dist}(q(n))$ is computable in polynomial time (even) when n is given in binary.

Section 4 is devoted to proving Lemma 8.

3.3 Candidates lie in some small initial square and then in few thin belts

An *area* is a set $B \subseteq \mathbb{N} \times \mathbb{N}$ of points. By $\overline{B} = \mathbb{N} \times \mathbb{N} \setminus B$ we denote the *complement* of B. Let $B_{>z} = \{(x, y) \in B \mid x, y > z\}$ for each $z \in \mathbb{N}$.

For each point $(x, y) \in \mathbb{N} \times \mathbb{N}$, let $\text{cube}(x, y) = \{(x', y') \in \mathbb{N} \times \mathbb{N} : |x - x'| \leq 1 \text{ and } |y - y'| \leq 1\}$. We define $\text{cube}(B) = \{\text{cube}(x, y) \mid (x, y) \in B\}$. Two areas B_1, B_2 are called *independent* if $\text{cube}(B_1) \cap B_2 = \emptyset$ (or equivalently $B_1 \cap \text{cube}(B_2) = \emptyset$). Observe that in particular independent areas are disjoint.

A *slope* is a rational $\mu \in \mathbb{Q}$ such that $\mu = \frac{a}{b}$ for some $a, b \in [k^2]$. Let $c_4 = 4c_3$. For each slope μ let $B(\mu)$ be the *belt* corresponding to μ be the following area:

$$B(\mu) \;=\; \left\{(x, y) \in \mathbb{N} \times \mathbb{N} \mid \mu \cdot x - c_4 k^4 \leq y \leq \mu \cdot x + c_4 k^4\right\}$$

Note that there are at most k^4 slopes/belts.

Let $\mathcal{B} = \bigcup_\mu B(\mu)$ denote *belt area*, i.e. the union of all areas covered by belts. The following lemma states that candidates lie in some initial polynomially-sized square or in the belt area. A visualization of the following lemma is given by Figure 1. Let us define $c_5 = 4c_4$.

Lemma 9. $\text{CAND} \;\subseteq\; Q \times Q \times ([c_5 k^{10}]^2 \cup \mathcal{B})$.

Proof. The lemma follows from the following two statements:

(1) If $\text{dist}(p(x)) = \text{dist}(q(y)) < \omega$ and $x, y > c_4 k^8$, then $(x, y) \in B(\mu)$ for some μ.
(2) Assume $\text{dist}(p(x)) = \text{dist}(q(y))$ and either (i) $0 \leq x \leq c_4 k^8$ and $y > c_5 k^{10}$ or (ii) $x > c_5 k^{10}$ and $0 \leq y \leq c_4 k^8$. Then $\text{dist}(p(x)) = \text{dist}(p(y)) = \omega$.

For point (1) let us fix $p, q \in Q$ and $x, y > c_4 k^8$ such that $\text{dist}(p(x)) = \text{dist}(q(y)) < \omega$. Let i (resp. j) be be residue class of x (resp. y) modulo $\text{LCM}[k]$. By Lemma 8 there are ratios $\alpha(p, i)$ and $\alpha(q, j)$ and offsets $\beta(p, i)$ and $\beta(q, j)$ with $|\beta(p, i)|, |\beta(q, j)| \leq c_3 \cdot k^4$ such that

$$\text{dist}(p(x)) = \alpha(p, i) \cdot x + \beta(p, i) \qquad \text{and} \qquad \text{dist}(q(y)) = \alpha(q, j) \cdot y + \beta(q, j)$$

Since $\text{dist}(p(x)) = \text{dist}(q(y))$ we have

$$y \quad = \quad \frac{\alpha(p, i) \cdot x + \beta(p, i) - \beta(q, j)}{\alpha(q, j)}$$

which implies $y = \mu \cdot x + d$, where where $\mu = \frac{\alpha(p,i)}{\alpha(q,j)}$ and $d = \frac{\beta(p,i)-\beta(q,j)}{\alpha(q,j)}$. Moreover we have $|d| \leq c_4 k^4$. Thus $(x, y) \in B(\mu)$.

For point (2) we prove the implication only for assumption (i). The case for assumption (ii) can be proven analogously. Let assume $0 \leq x \leq c_4 k^8$ and $y > c_5 k^{10}$. Assume by contradiction $\text{dist}(p(x)) = \text{dist}(q(y)) < \omega$. On the one hand, it follows from Lemma 8

$$\text{dist}(p(x)) \quad \leq \quad k \cdot x + c_3 k^4 \quad \leq \quad c_4 k^9 + c_3 k^4 \quad \leq \quad 2c_4 k^9.$$

On the other hand, since $y > c_5 k^{10} > c_3 k^6$ we have by Lemma 8

$$\text{dist}(q(y)) \quad \geq \quad \frac{1}{k} \cdot y - c_3 k^4 \quad > \quad c_5 k^9 - c_3 k^4 \quad = \quad 4c_4 k^9 - c_3 k^4 \quad > \quad 2c_4 k^9.$$

Thus $\text{dist}(p(x)) < \text{dist}(q(y))$, a contradiction. □

The following lemma states that different belts are independent once we are outside some polynomially large initial area.

Lemma 10. *$B(\mu)_{>c_5 k^8}$ and $B(\mu')_{>c_5 k^8}$ are independent provided $\mu \neq \mu'$.*

Proof. It suffices to prove that for all slopes μ, μ' with $\mu' \neq \mu$ and all $x > c_5 k^8$ we have

$$\begin{array}{lll} \mu' > \mu & \Rightarrow & \mu \cdot x + c_4 k^4 + 1 \ < \ \mu' \cdot x - c_4 k^4 - 1 \quad \text{and} \\ \mu' < \mu & \Rightarrow & \mu' \cdot x + c_4 k^4 + 1 \ < \ \mu \cdot x - c_4 k^4 - 1. \end{array}$$

We only treat the case $\mu' > \mu$, the case $\mu' < \mu$ can be proven analogously. Observe that $\frac{1}{k^4} \leq \mu' - \mu$. The desired inequality follows by deducing from $c_5 k^8 < x$ the following:

$$c_5 k^4 < (\mu' - \mu) \cdot x \ \Rightarrow \ \mu \cdot x + \frac{c_5}{2} k^4 < \mu' \cdot x - \frac{c_5}{2} k^4 \ \overset{c_5 = 4c_4}{\Rightarrow} \ \mu \cdot x + c_4 k^4 + 1 < \mu' \cdot x - c_4 k^4 - 1$$

□

3.4 Interpretation of $\sim$ in terms of colorings

A *coloring* is a mapping $\chi : Q \times Q \times \mathbb{N} \times \mathbb{N} \to \{\bullet, \circ\}$. Note that each coloring gives rise to a binary relation on the one-counter processes generated by M. Conversely each binary relation on the set of one-counter processes gives rise to a coloring. We define the *bisimulation coloring* χ_M that corresponds to the bisimilarity relation $\sim$ of M as expected:

$$\chi_M(p, q, x, y) \quad = \quad \begin{cases} \bullet & \text{if } p(x) \sim q(y) \\ \circ & \text{otherwise} \end{cases} \qquad \text{for each } p, q \in Q \text{ and } x, y \in \mathbb{N}$$

Let χ be a coloring. We call the tuple $(p, q, x, y) \in Q \times Q \times \mathbb{N} \times \mathbb{N}$ is *locally consistent* whenever $\chi(p, q, x, y) = \bullet$ implies the bisimulation conditions, i.e.

(1) If $p(x) \xrightarrow{a} p'(x')$ for some $p'(x')$, then $q(y) \xrightarrow{a} q'(y')$ for some $q'(y')$ with $\chi(p', q', x', y') = \bullet$.
(2) If $q(y) \xrightarrow{a} q'(y')$ for some $q'(y')$, then $p(x) \xrightarrow{a} p'(x')$ for some $p'(x')$ with $\chi(p', q', x', y') = \bullet$.

We call χ *locally consistent* if χ locally consistent for every element of $Q \times Q \times \mathbb{N} \times \mathbb{N}$. Note that $p(x) \sim q(y)$ if and only if there is some locally consistent coloring χ such that $\chi(p, q, x, y) = \bullet$. The next lemma establishes a characterization of bisimilarity of one-counter processes in terms of colorings. In a nutshell, it says for proving bisimilarity of two one-counter processes $p(x)$ and $q(y)$ it is sufficient to look at a coloring χ that agrees with χ_M on the sure pairs, that satisfies $\chi(p, q, x, y) = \bullet$, and that is locally consistent only in an exponentially-sized area.

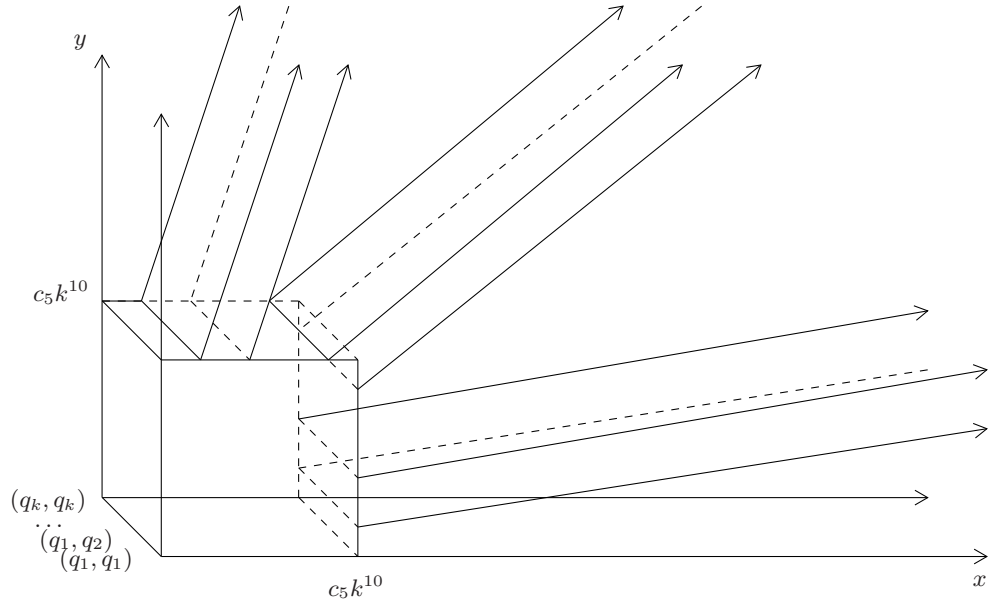

Fig. 1. Candidates lie in some initial square and then in independent belts

Lemma 11 (Characterization of bisimilarity). *We have $p_0(x_0) \sim q_0(y_0)$ if and only if there is some coloring χ such that*

(1) χ agrees with χ_M on SURE*,*
(2) each element of $Q \times Q \times [0, \Omega]^2$ is locally consistent, and
(3) $\chi(p_0, q_0, x_0, y_0) = \bullet$.

where $\Omega \;=\; x_0 + 2c_5k^{10} + 2^{c_5k^6} \cdot (LCM[k^2])^2$.

Lemma 11 can be seen as the core of the correctness proof of our polynomial space procedure that we provide in the next section. Lemma 11 is proven in Section 5.

3.5 The polynomial space procedure

Theorem 12. *Bisimilarity of one-counter processes is* PSPACE*-complete.*

Proof. The PSPACE lower bound for this problem was proven by Srba in [21].

For the PSPACE upper bound, let us fix some one-counter automaton $M = (Q, \mathsf{A}, \delta_0, \delta_{>0})$ with $k = |Q|$ and two one-counter processes $p_0(x_0)$ and $q_0(y_0)$ of T_M. We now use the characterization of $p_0(x_0) \sim q_0(y_0)$ given by Lemma 11. Let $\Omega \;=\; x_0 + 2c_5k^{10} + 2^{c_5k^6} \cdot (\mathrm{LCM}[k^2])^2$ be the natural from Lemma 11. We demonstrate that we can check the existence of some coloring χ that satisfies conditions (1), (2) and (3) of Lemma 11 in polynomial space. Note that point (1), i.e. checking if χ agrees with χ_M on the set SURE of sure pairs can be solved even in polynomial time by Lemma 7. Let us explain how to decide in polynomial space if point (2) holds, i.e. if χ is locally consistent on all $Q \times Q \times \Omega^2$. Since χ's coloring on SURE is decidable in polynomial time, it suffices to guess χ's coloring CAND inside $Q \times Q \times [0, \Omega + 1]^2$. Note that we cannot guess simply all of χ's colors inside $[0, \Omega + 1]^2$ at once, since there are exponentially many such colors to be guessed. This would lead to a NEXPTIME upper bound only. Instead, we guess these colors on-the-fly. For this, it will be useful to view the set CAND of all candidate pairs as the union

$$\mathrm{CAND} \quad = \quad \mathrm{CAND}_0 \cup \mathrm{CAND}_1 \cup \mathrm{CAND}_2 \cup \cdots$$

where CAND_i contains the *candidate pairs at vertical level i*, i.e. the pairs $\langle p(x), q(y)\rangle \in \mathrm{CAND}$ with $x = i$. By Lemma 9 we know that $\mathrm{CAND} \subseteq Q \times Q \times ([0, c_5 k^{10}]^2 \cup \mathcal{B})$. Since $\mathcal{B}$ was the union of all belt areas and since there are at most k^4 belts of thickness $2c_3k^4 + 1$ each, we obtain that CAND_i is polynomially bounded for each $i \geq 0$.

For each set $C \subseteq Q \times Q \times \mathbb{N} \times \mathbb{N}$, define $\mathrm{cube}(C) = \{\langle p'(x'), q'(y')\rangle \mid \exists \langle p(x), q(y)\rangle \in C : (x', y') \in \mathrm{cube}(x, y)\}$ to be the neighbors of C that can influence the bisimilarity condition of members of C. Our nondeterministic algorithm is depicted in algorithm environment 1.

Algorithm 1 Checking if $p_0(x_0) \sim q_0(y_0)$ via some locally consistent coloring inside $Q \times Q \times [0, \Omega]^2$

1: **for all** $i = 1$ up to Ω **do**
2: Guess χ's colors on CAND_{i-1},CAND_i and CAND_{i+1} if not already guessed
3: Check local consistency for each $(p, q, x, y) \in \mathrm{cube}(\mathrm{CAND}_i)$ with $x = i$.
4: Forget χ's colors on CAND_{i-1} but not $\chi(p_0, q_0, x_0, y_0)$ if inside.
5: **end for**
6: **return** $\chi(p_0, q_0, x_0, y_0) = \bullet$.

It is clear that we can implement Algorithm 1 in polynomial space. □

4 Proof of Lemma 8

Let $\Gamma = Q \times \{-1, 0, 1\} \times \mathsf{A} \times Q$ be the set of all possible transitions of our one-counter automaton M. Let s, t and be states in T_M. A *path in T_M from s to t* is a finite sequence of transitions $\sigma = \gamma_1 \cdots \gamma_l$ such that $q_0(n_0) \xrightarrow{\gamma_1} q_1(q_1) \cdots \xrightarrow{\gamma_l} q_l(n_l)$ with $q_0(n_0) = s$ and $q_l(n_l) = t$. By $|\sigma| = l$ we denote the *length* of σ. We call σ *minimal*, if the length of every path from s to t is at least $|\sigma|$. We also denote this by $\mathrm{dist}(s, t) = |\sigma|$. We call σ *positive* if $n_i > 0$ for each $i \in [0, l]$ and *zero* otherwise. A path σ is called *elementary cycle* if it induces an elementary cycle in the control state set Q. Such a cycle has length at most $|Q|$, and its effect on the counter value is non-zero and thus in $\{-|Q|, -|Q| + 1, \ldots, |Q|\}$.

We note that the following Lemma from [24] was proven in the context of *deterministic* one-counter automata (with ε-steps) but the lemma obviously applies to our nondeterministic case as well (since we can view the transitions themselves as the actions). Lemma 2 in [24] can directly expressed in our setting as follows.

Lemma 13 (Lemma 2 in [24]). *If there is a positive path from $p(m)$ to $q(n)$ and $m-n \geq k^2$ and $n \geq k^2$ then there is such a shortest path $p(m) \xrightarrow{\sigma} q(n)$ such that $\sigma = \sigma_1\sigma_2^i\sigma_3$ where $|\sigma_1\sigma_3| < k^2$ and σ_2 is an elementary decreasing cycle with $|\sigma_2| \leq k$.*

From the previous lemma and a simple pigeonhole argument, we can prove the following lemma. We define $c_1 = 4$.

Lemma 14. *If there is a path from $p(m)$ to $q(n)$ and $n < k$, then there is such a shortest path $p(m) \xrightarrow{\sigma} q(n)$ such that $\sigma = \sigma_1(\sigma_2)^l\sigma_3$, where $|\sigma_1\sigma_3| \leq c_1k^3$ and where σ_2 is an elementary decreasing cycle (if $l > 0$) and $|\sigma_2| \leq k$.*

Proof. Before we prove the lemma, we will prove the following claim.

Claim: For every $p'(m')$ with $m' \leq 2k^2$ and $p'(m') \longrightarrow^* q(n)$ every minimal path π from $p'(m')$ to $q(n)$ does not visit any process of counter value strictly larger than $3k^2$; hence in particular $|\pi| \leq 3k^3$.

Proof of Claim: Fix some minimal path $\pi = q_1(n_1) \xrightarrow{\pi_1} q_2(n_2) \cdots \xrightarrow{\pi_t} q_t(n_t)$ from $p'(m')$ to $q(n)$. Assume by contradiction some process $q_j(n_j)$ where $n_j > 3k^2$ is maximal among all counter values n_i. For each $h \in [m', n_j]$, define

$$f(h) = \max\{i \leq j \mid n_i = h\} \qquad \text{and} \qquad g(h) = \min\{i \geq j \mid n_i = h\}.$$

Since, by assumption $n_j - m' > 3k^2 - 2k^2 = k^2$, there are $p_1, p_2 \in Q$ and $m' \leq h < h' \leq n_j$ such that $f(h) = f(h') = p_1$ and $g(h') = g(h) = p_2$ by the pigeonhole principle. Let $d = h' - h > 0$. Now we can modify the path π replacing the subpath from $f(h)$ to $g(h)$ by the subpath from $f(h')$ to $g(h')$, where all heights are lowered by d. But the resulting path contradicts minimality of π.

This concludes the proof of the claim.

Recall that $c_1 = 4$. To prove the lemma, we distinguish two cases,:

- $m \leq 2k^2$: Then we can apply the above claim and we are done.
- $m > 2k^2$: Let us fix some shortest path π from $p(m)$ to $q(n)$. Hence there is some intermediate proceess $p'(k^2)$ on π such that π's (positive) subpath from $p(m)$ to $p'(k^2)$ can be replaced by a shortest positive path $p(m) \xrightarrow{\tau} p'(k^2)$ corresponding to the form of Lemma 13. This means τ is of the form $\tau = \tau_1(\tau_2)^l\tau_3$, where $|\tau_1\tau_3| < k^2$ and τ_2 is an elementary decreasing cycle with $|\tau_2| \leq k$. By the above claim, the length of π's subpath from $p'(k^2)$ to $q(n)$, let us call this subpath π', has length at most $3k^3$. We put $\sigma_1 = \tau_1$, $\sigma_2 = \tau_2$ and $\sigma_3 = \tau_3\pi'$. The path $\sigma = \sigma_1\sigma_2^l\sigma_3$ is hence a shortest path from $p(m)$ to $q(n)$ with $|\sigma_1\sigma_3| \leq k^2 + 3k^3 \leq c_1k^3$ and thus the lemma follows.

□

We define the constant $c_2 = 7c_1$.

Lemma 15. *For every $q \in Q$, every $0 \leq i < LCM[k]$ and every $p(m)$ with $m < k$ there exists some ratio $\alpha = \alpha(q, i, p(m))$ and some offset $\beta = \beta(q, i, p(m)) \in \mathbb{Q}$ with $|\beta| \leq c_2k^4$ such that for every $n > c_2k^6$ with $n \equiv i$ mod $LCM[k^2]$ the following two statements hold:*

(1) The residue class i determines if dist$(q(n), p(m)) = \omega$
(2) If $q(n) \longrightarrow^* p(m)$, then dist$(q(n), p(m)) = \alpha \cdot n + \beta$.

Proof. Let us fix some $n_1, n_2 > c_2k^6$ with $n_1 \equiv n_2 \equiv i$ mod LCM$[k]$. We assume that $n_1 < n_2$ and let $D = n_2 - n_1$, which is a multiple of LCM$[k]$.

Let us first prove point (1). We prove that $q(n_2) \longrightarrow^* p(m)$ implies $q(n_1) \longrightarrow^* p(m)$ (the converse direction can be proven analogously). So let us assume $q(n_2) \longrightarrow^* p(m)$. Hence there is a path $\sigma = \sigma_1(\sigma_2)^l\sigma_3$ with $q(n_2) \xrightarrow{\sigma} p(m)$ that satisfies the conditions of Lemma 14. Observe that $l > 0$ and since $|\sigma_2| \leq k$ we have that $|\sigma_2|$ divides LCM$[k]$. Moreover since $m + |\sigma_1\sigma_3| \leq k + c_1k^3 < c_2k^6$ it follows that there exists some $l' < l$ such that $\sigma_1\sigma_2^{l'}\sigma_3$ is a path from $q(n_1)$ to $p(m)$. Thus $q(n_1) \longrightarrow^* p(m)$.

Let us prove point (2). Let us assume $q(n_1) \longrightarrow^* p(m)$ and $q(n_2) \longrightarrow^* p(m)$. Then there is a minimal path τ_1 (resp. τ_2) from $q(n_1)$ to $p(m)$ (resp. from $q(n_2)$ to $p(m)$) that satisfies the conditions of Lemma 14. Let γ_1 (resp. γ_2) denote the elementary decreasing cycle of τ_1 (resp. τ_2), let d_1 (resp. d_2) denote its counter effect (which is a negative integer from $\{-k, \ldots, -1\}$).

We will first prove that dist$(q(n_2), p(m)) =$ dist$(q(n_1), p(m)) + \alpha \cdot D$, where α is some ratio that is determined by q, i, and $p(m)$. Define the ratio $\alpha_j = \frac{|\gamma_j|}{d_j}$ for each $j \in \{1, 2\}$. We have the following claim, whose proof we postpone to the end of the lemma.

Claim: $\alpha_1 = \alpha_2$.

So let $\alpha = \alpha_1 = \alpha_2$. Let us prove dist$(q(n_2), p(m)) =$ dist$(q(n_1), p(m)) + \alpha \cdot D$. Assume first by contradiction that dist$(q(n_2), p(m)) <$ dist$(q(n_1), p(m)) + \alpha \cdot D$. In analogy to the proof of point (1) one can prove that by traversing the elementary decreacing cycle γ_2 in τ_2 fewer times one can construct a path from $q(n_1)$ to $p(m)$ of length smaller than $|\tau_1|$, hence contradicting minimality of τ_1. The case dist$(q(n_2), p(m)) >$ dist$(q(n_1), p(m)) + \alpha \cdot D$ can be dealt with analogously.

To finally prove the lemma it remains to prove an upper bound for the absolute value of β, where $\beta \in \mathbb{Q}$ is the rational that satisfies dist$(q(n_1), p(m)) = \alpha \cdot n_1 + \beta$. Assume τ_1 is of the form $\sigma\gamma_1^l\psi$. Recall that γ_1 is the elementary decreasing cycle of τ_1. Let H be the counter gain/loss of $\sigma\psi$. Since $|\sigma\psi| \leq c_1k^3$ we have $-c_1k^3 \leq H \leq c_1k^3$. Then it follows

$$\text{dist}(q(n_1), p(m)) \quad = \quad \frac{n_1 - m - H}{d_1} \cdot |\gamma_1| + |\sigma\psi| \quad = \quad \alpha \cdot n_1 \underbrace{-\alpha \cdot (m + H) + |\sigma\psi|}_{\beta}.$$

Since $1 \leq \alpha \leq k$ and $c_2 = 6c_1$ it follows (generously)

$$-c_2k^4 \quad \leq \quad -3c_1k^4 \quad \leq \quad \beta \quad \leq \quad 3c_1k^4 \quad \leq \quad c_2k^4. \tag{1}$$

Proof of the above claim: Without loss of generality let us assume $\alpha_1 > \alpha_2$. Let τ_1' be the path from $q(n_1)$ to $p(m)$ that is obtained from τ_2 by traversing its elementary decreasing cycle γ_2 appropriately often (i.e. fewer). We prove that $|\tau_1'| < |\tau_1|$, hence contradicting minimality of τ_1. We derive the contradiction $|\tau_1| - |\tau_1'| > 0$ as follows:

$$\begin{array}{rcl} |\tau_1| - |\tau_1'| & \geq & \alpha_1 \cdot n_1 - \beta - \alpha_2 \cdot n_1 - \beta \\ & \stackrel{\text{eq.(1)}}{\geq} & (\alpha_1 - \alpha_2) \cdot n_1 - 6c_1k^4 \\ & \geq & \dfrac{1}{k^2} \cdot n_1 - 6c_1k^4 \\ & > & \dfrac{1}{k^2} \cdot c_2k^6 - 6c_1k^4 \\ & > & 0 \end{array}$$

□

We define the constant $c_3 = 2c_2$. We conclude this section with the proof of Lemma 8.

Proof of Lemma 8

Point (1) of Lemma 8 follows immediately from $c_3 > c_2$ and from point (1) of Lemma 15.

For point (2) let us fix some $n > c_3k^6$ such that $n \equiv i \bmod \text{LCM}[k]$. Let $p_1(m_1), \ldots, p_l(m_l)$ be an enumeration of the set $\{p(m) \in \text{INC} \mid q(n) \longrightarrow^* p(m)\}$ (which is uniquely determined by q and i by point (1)). Note that $m_j < k$ by Proposition 4 for each j. Let us fix ratios $\alpha_1, \ldots, \alpha_l$ and offsets $\beta_1, \ldots, \beta_l$ with $|\beta_j| \leq c_2k^4$ for each $1 \leq j \leq l$ corresponding to Lemma 15.

Define $\alpha = \min\{\alpha_j \mid 1 \leq j \leq l\}$ and let $\beta = \min\{\beta_j \mid \alpha_j = \alpha, 1 \leq j \leq l\}$. We prove that $\text{dist}(q(n)) = \alpha \cdot n + \beta$. Since $|\beta_j| \leq c_2k^4$ for each j by Lemma 15 it suffices to prove that $\alpha \cdot n + c_2k^4 \leq \alpha' \cdot n - c_2k^4$ for each ratio $\alpha' > \alpha$. The latter holds since $c_3k^6 \leq n$ implies

$$c_3k^4 \leq \frac{n}{k^2} \;\Rightarrow\; c_3k^4 \leq (\alpha' - \alpha) \cdot n \;\Rightarrow\; 2c_2k^4 \leq \alpha' \cdot n - \alpha \cdot n \;\Rightarrow \alpha \cdot n + c_2k^4 \leq \alpha' \cdot n - c_2k^4.$$

Let us now prove argue that $\text{dist}(q(n))$ is computable in polynomial time. There are at most k^2 many members in INC, each of which has counter value strictly less than k by Proposition 4. We can restrict ourselves to searching for minimal paths of the form $\sigma = \sigma_1(\sigma_2)^l\sigma_3$ in the spirit of Lemma 14. Since there are potentially at most $2c_1k^4$ many one-counter processes where σ_1 ends and at most $2c_1k^4$ many processes where σ_3 starts, we can try all possible combinations of these and test if they can be connected by repeatedly executing some decreasing elementary cycle σ_2 (that we only need to test polynomially many combinations of). □

5 Proof of Lemma 11

Proof. We prove the lemma by showing that *if* there is a coloring χ that satisfies points (1), (2) and (3), i.e.

(1) χ agrees with χ_M on SURE,
(2) each element of $Q \times Q \times [0, \Omega]^2$ is locally consistent, and
(3) $\chi(p_0, q_0, x_0, y_0) = \bullet$.

then there exists a coloring χ' that is locally consistent and moreover $\chi'(p_0, q_0, x_0, y_0) = \bullet$ (and thus $p(x) \sim p(y)$). Recall that

$$\Omega \;=\; x_0 + 2c_5k^{10} + 2^{c_5k^6} \cdot (\text{LCM}[k^2])^2.$$

So let us fix a coloring χ that satisfies points (1),(2) and (3).

We set χ' to agree with χ_M on SURE. It remains to define χ' on members of CAND. We will give the coloring of χ' for each candidate $(p,q,x,y) \in \text{CAND}$ dependent on the belt in which (x,y) lies. More precisely, we are in particular interested in candidates $(p,q,x,y) \in \text{CAND}$ with $x > 2c_5k^{10} + x_0$. For the latter candidates it follows (even when $x_0 = 0$) that $(x,y) \in \mathcal{B}$ by Lemma 9. Moreover it follows $y > c_5k^8$ due to

$$y \quad \geq \quad \frac{1}{k^2} \cdot x - c_4k^4 \quad > \quad 2c_5k^8 - c_4k^4 \quad > c_5k^8.$$

Hence for each $(p,q,x,y) \in \text{CAND}$ with $x > 2c_5k^{10}$ we have that (x,y) lies in precisely one belt $B(\mu)$.

Let us fix one belt $\mathcal{B}(\mu)$ with slope μ. We aim to prove that the colors of χ will repeat periodically in the belt $\mathcal{B}(\mu)$ as depicted in Figure 2. To prove this, we look at certain vertical positions $x > 2c_5k^{10} + x_0$ with $x \equiv 0 \bmod \text{LCM}[k^2]^2$ that we call *cuts*. Since the denominator of each slope is some number from $\{1,\ldots,k^2\}$ it follows that $\mu x \equiv 0 \bmod \text{LCM}[k]$ for each cut x. If x is a cut, note that the elements inside the belt $B(\mu)$ with vertical value x are precisely the pairs $\{(x, \mu x + d) \mid d \in [-c_4k^4, c_4k^4]\}$.

Define the *cut square* (as depicted in Figure 2) to be the mapping

$$S_x : Q \times Q \times [-c_4k^4, c_4k^4] \to \{\circ, \bullet\} \quad \text{with} \quad S_x(p,q,d) = \chi(p,q,x,\mu x + d)$$

for each cut x. Note that there are at most $2^{k^2 \cdot (2c_4k^4+1)} < 2^{c_5k^6} - 1$ many different cut squares. Hence between $2c_5k^{10} + x_0$ and $2c_5k^{10} + x_0 + 2^{c_5k^6} \cdot \text{LCM}[k^2]^2 = \Omega$ there two distinct cuts $x_1 < x_2$ with $S_{x_1} = S_{x_2}$ by the pigeonhole principle. This siutation is depicted in Figure 2. Let $\Upsilon = x_2 - x_1$.

Recall that on members of SURE the mapping χ' is defined the same way as χ_M (or χ). We will define that on candidates $(p,q,x,y) \in \text{CAND}$ with $(x,y) \in \mathcal{B}(\mu)$, the coloring χ' differs from χ *only (if at all) in case* $x > x_2$. Note that for each candidates (p,q,x,y) *inside* $\mathcal{B}(\mu)$ with $x > x_2$ we can express (x,y) as $(x_1 + i\Upsilon + s, \mu(x_1 + i\Upsilon) + t)$ for some unique vector $(s,t) \in \mathbb{N} \times \mathbb{N}$ provided $i \geq 1$ is maximal. We then define $\chi'(p,q,x,y)$ as $\chi(p,q,x_1 + s, \mu x_1 + t)$.

Since $x \equiv x_1 + s \bmod \text{LCM}[k]$ and $y \equiv \mu x_1 + t \bmod \text{LCM}[k]$ and $x, y \gg c_3k^6$, we have that

$$(p,q,x,y) \text{ is locally consistent} \qquad \text{if and only if} \qquad (p,q,x_1+s,\mu x_1+t) \text{ is locally consistent}$$

by Lemma 7. Thus, χ' is locally consistent and $\chi'(p_0,q_0,x_0,y_0) = \chi(p_0,q_0,x_0,y_0) = \bullet$.

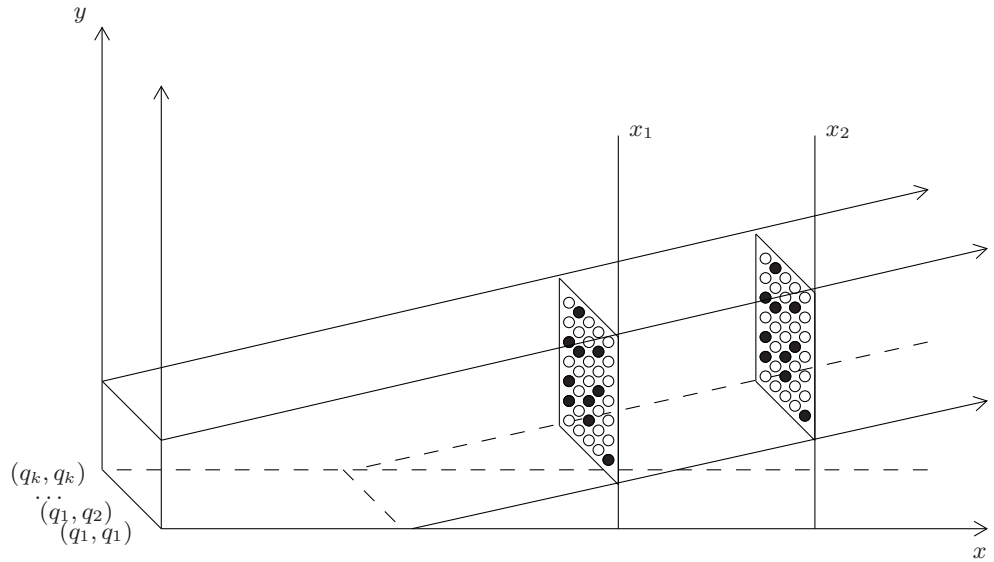

Fig. 2. The cut squares S_{x_1} and S_{x_2} are the same.

□

6 $\sim$-Regularity

We can easily derive the next lemma, which tells us that $p(m)$ is not $\sim$-regular iff it allows to reach states with arbitrarily large finite distances to INC.

Lemma 16. *Given $p(m)$ for a one counter automaton M, $p(m)$ is not $\sim$-regular iff for any $d \in \mathbb{N}$ there is $q(n)$ such that $p(m) \rightarrow^* q(n)$ and $d \leq dist(q(n)) < \omega$.*

The next proposition gives a more convenient characterization.

Proposition 17. *$p(m)$ is not $\sim$-regular iff $p(m) \rightarrow^* q(m+2k)$ where $q(m+2k) \rightarrow^*$ INC. (Recall that $k = |Q|$ for the set Q of control states of M.)*

Proof. 'Only if' is obvious.
On any path $p(m) \xrightarrow{\sigma_1} q(m+2k) \xrightarrow{\sigma_2}$ INC we have to cross the level $(m+k)$ when going up as well as when going down to INC (recall that $\ell < k$ for any $r(\ell) \in$ INC). The elementary cycles, which must necessary appear when going up and down, can be suitably pumped to show the condition in Lemma 16. □

Lemma 18. *Deciding $\sim$-regularity of one-counter processes is in* PTIME.

Proof. We check the condition from Proposition 17. Given $p(m)$, we can compute all $q(m+2k)$ which have finite distances to INC by a polynomial algorithm by Lemma 8. When $m = 0$, the reachability of a suitable $q(2k)$ ($q(2k) \rightarrow^*$ INC) can be checked straightforwardly. If $m > 0$ then a shortest path $p(m) \xrightarrow{\sigma} q(m+2k)$ either does not go through zero, i.e. through any $p'(0)$, in which case it does not need to cross the level $m - k^2$ (as can be verified by standard arguments, it is similar as in the claim in the proof of the Lemma 14), or it does reach some $p'(0)$. Such $p'(0)$ is surely not $\sim$-regular either (since $p'(0) \rightarrow^* q(m+2k) \rightarrow^*$ INC), and the previous case $m = 0$ can be used. Because reachability of $p'(0)$ from $p(m)$ can be decided in polynomial time by Lemma 8 we are done. □

Lemma 19. *Deciding $\sim$-regularity (even) of one-counter nets is* PTIME*-hard.*

Proof. We use a reduction from bisimilarity on finite transition systems which is PTIME-complete [1]. Given a finite transition system $(Q, \mathsf{A}, \{\xrightarrow{a}\}_{a \in \mathsf{A}})$, and $f, g \in Q$, it is easy to construct a one counter net which has the following behaviour: in $s_0(m)$, $m > 0$, it has transitions $s_0(m) \xrightarrow{a} s_0(m+1)$, $s_0(m) \xrightarrow{a} s_0(m-1)$, $s_0(m) \xrightarrow{b} f(m)$, $s_0(m) \xrightarrow{b} g(m)$. In $s_0(0)$ we only have $s_0(0) \xrightarrow{a} s_0(1)$ and $s_0(0) \xrightarrow{b} f(0)$. Any state $f(n)$ just mimicks f (not changing the counter); similarly $g(n)$ mimicks g. It is easy to verify that $s_0(n)$ is regular iff $f \sim g$. □

Theorem 20. *Deciding $\sim$-regularity of one-counter processes is* PTIME*-complete.*

References

1. J. L. Balcázar, J. Gabarró, and M. Santha. Deciding Bisimilarity is P-Complete. *Formal Asp. Comput.*, 4(6A):638–648, 1992.
2. T. Brázdil, V. Brozek, K. Etessami, A. Kucera, and D. Wojtczak. One-Counter Markov Decision Processes. In *Proc. of SODA*, pages 863–874. IEEE, 2010.
3. S. Demri and A. Sangnier. When model-checking freeze ltl over counter machines becomes decidable. In *Proc. of FOSSACS*, volume 6014 of *Lecture Notes in Computer Science*, pages 176–190. Springer, 2010.
4. S. Göller, R. Mayr, and A. W. To. On the computational complexity of verifying one-counter processes. In *Proc. of LICS*, pages 235–244. IEEE Computer Society Press, 2009.
5. C. Haase, S. Kreutzer, J. Ouaknine, and J. Worrell. Reachability in succinct and parametric one-counter automata. In *Proc. of CONCUR*, volume 5710 of *Lecture Notes in Computer Science*, pages 369–383. Springer, 2009.
6. D. Janin and I. Walukiewicz. On the Expressive Completeness of the Propositional mu-Calculus with Respect to Monadic Second Order Logic. In *Proc. of CONCUR*, volume 1119 of *Lecture Notes in Computer Science*, pages 263–277. Springer, 1996.

7. P. Jančar. Decidability of bisimilarity for one-counter processes. *Information Computation*, 158(1):1–17, 2000.
8. P. Jančar. Strong bisimilarity on basic parallel processes is pspace-complete. In *Proc. of LICS*, pages 218–227. IEEE Computer Society, 2003.
9. P. Jančar, J. Esparza, and F. Moller. Petri nets and regular processes. *J. Comput. Syst. Sci.*, 59(3):476–503, 1999.
10. P. C. Kanellakis and S. A. Smolka. CCS expressions, finite state processes, and three problems of equivalence. *Information and Computation*, 86(1):43–68, May 1990.
11. R. Mayr. Process Rewrite Systems. *Information and Computation*, 156(1):264–286, 2000.
12. R. Mayr. Undecidability of weak bisimulation equivalence for 1-counter processes. In *Proc. of ICALP*, volume 2719 of *Lecture Notes in Computer Science*, pages 570–583, 2003.
13. R. Milner. *Communication and Concurrency*. International Series in Computer Science. Prentice Hall, 1989.
14. F. Moller and A. M. Rabinovich. Counting on CTL*: on the expressive power of monadic path logic. *Inf. Comput.*, 184(1):147–159, 2003.
15. M. Nair. On Chebyshev-type inequalities for primes. *The American Mathematical Monthly*, 89(2):126–129, 1982.
16. R. Paige and R. E. Tarjan. Three partition refinement algorithms. *SIAM Journal on Computing*, 16(6):973–989, Dec. 1987.
17. G. Sénizergues. The bisimulation problem for equational graphs of finite out-degree. *SIAM J. Comput.*, 34(5):1025–1106, 2005.
18. O. Serre. Parity games played on transition graphs of one-counter processes. In L. Aceto and A. Ingólfsdóttir, editors, *Proc. of FOSSACS*, number 3921 in Lecture Notes in Computer Science. Springer, 2006.
19. J. Srba. Strong bisimilarity and regularity of basic process algebra is pspace-hard. In *Proc. of ICALP*, volume 2380 of *Lecture Notes in Computer Science*, pages 716–727. Springer, 2002.
20. J. Srba. *Roadmap of Infinite results*, volume Vol 2: Formal Models and Semantics. World Scientific Publishing Co., 2004. http://www.brics.dk/~srba/roadmap.
21. J. Srba. Beyond language equivalence on visibly pushdown automata. *Logical Methods in Computer Science*, 5(1:2), 2009.
22. C. Stirling. Decidability of Bisimulation Equivalence for Pushdown Processes. *unpublished*, 2000.
23. A. W. To. Model checking fo(r) over one-counter processes and beyond. In *Proc. of CSL*, volume 5771 of *Lecture Notes in Computer Science*, pages 485–499. Springer, 2009.
24. L. G. Valiant and M. Paterson. Deterministic one-counter automata. *J. Comput. Syst. Sci.*, 10(3):340–350, 1975.
25. J. van Benthem. *Modal Correspondence Theory*. PhD thesis, University of Amsterdam, 1976.
26. R. J. van Glabbeek. The linear time-branching time spectrum (extended abstract). In *CONCUR*, volume 458 of *Lecture Notes in Computer Science*, pages 278–297. Springer, 1990.
27. H.-C. Yen. Complexity Analysis of Some Verification Problems for One-Counter Machines. unpublished manuscript.