Liveness Verification of Reversal-bounded Multicounter Machines with a Free Counter *

(Extended Abstract)

Zhe Dang[1], Oscar H. Ibarra[2] and Pierluigi San Pietro[3]

[1]School of Electrical Engineering and Computer Science
Washington State University
Pullman, WA 99164
[2]Department of Computer Science
University of California
Santa Barbara, CA 93106
[3]Dipartimento di Elettronica e Informazione
Politecnico di Milano, Italia

Abstract. We investigate the Presburger liveness problems for nondeterministic reversal-bounded multicounter machines with a free counter (NCMFs). We show the following:

- The ∃-Presburger-i.o. problem and the ∃-Presburger-eventual problem are both decidable. So are their duals, the ∀-Presburger-almost-always problem and the ∀-Presburger-always problem.
- The ∀-Presburger-i.o. problem and the ∀-Presburger-eventual problem are both undecidable. So are their duals, the ∃-Presburger-almost-always problem and the ∃-Presburger-always problem.

These results can be used to formulate a weak form of Presburger linear temporal logic and develop its model-checking theories for NCMFs. They can also be combined with [12] to study the same set of liveness problems on an extended form of discrete timed automata containing, besides clocks, a number of reversal-bounded counters and a free counter.

1 Introduction

An infinite-state system can be obtained by augmenting a finite automaton with one or more unbounded storage devices. The devices can be, for instance, counters (unary stacks), pushdown stacks, queues, and/or Turing tapes. However, an infinite-state system can easily achieve Turing-completeness, e.g., when two counters are attached to a finite automaton (resulting in a “Minsky machine”). For these systems, even simple problems such as membership are undecidable.

In the area of model-checking, the search for (efficient) techniques for verifying infinite-state systems has been an ongoing research effort. Much work has been devoted to investigating various restricted models of infinite-state systems that are amenable to

* Supported in part by NSF grant IRI-9700370

automatic verification. The work is motivated by the successes of "efficient" model-checking techniques for finite-state systems such as hardware devices and reactive systems [20], and the need for developing practical techniques for deciding verification properties of infinite-state systems.

The infinite-state models that have been investigated include timed automata [1], pushdown automata [3, 14], various versions of counter machines [5, 13, 18], and various queue machines [2, 4, 16, 17, 21].

Counter machines are considered a natural model for specifying reactive systems containing integer variables. They have also been found to have a close relationship to other popular models of infinite-state systems, such as timed automata [1]. In [6], it was shown that, as far as binary reachability (the set of configuration pairs such that one can reach the other) is concerned, a timed automaton can be transformed into a particular type of counter machine without nested cycles [5]. In contrast to [6], timed automata (with discrete time) are mapped to counter machines with reversal-bounded counters in [8]. In the case of dense time, the same mapping applies using some pattern technique [7].

Thus, studying various restricted models of counter machines may help researchers to develop verification theories concerning infinite-state systems such as timed automata augmented with unbounded storage [8].

In this paper, we focus on a class of restricted counter machines, called nondeterministic reversal-bounded multicounter machines with a free counter (NCMFs). More precisely, an NCMF M is a nondeterministic finite automaton augmented with a finite number of reversal-bounded counters (thus, in any computation, each counter can change mode from nondecreasing to nonincreasing and vice-versa at most r times for some given nonnegative integer r) and one free counter (which need not be reversal-bounded). A fundamental result is that the emptiness problem for languages accepted by NCMFs is decidable [15]. But here we do not use NCMFs as language recognizers; instead, we are interested in the behaviors they generate. So, unless otherwise specified, an NCMF has no input tape. Reversal-bounded counters are useful in verification of reactive systems. For instance, a reversal-bounded counter can be used to count the number of times a particular external event occurs in a reactive system – in this case, the counter is simply 0-reversal-bounded, i.e., non-decreasing. Allowing a free counter, together with other reversal-bounded counters, makes the reactive system infinite-state. More application issues of NCMFs and the results in this paper can be found at the end of the paper.

The study of safety properties and liveness properties of infinite-state systems is of great importance in the area of formal verification. Safety properties look at only finite (execution) paths; mostly they can be reduced to reachability problems. In [18], it was shown that the Presburger safety analysis problem is decidable for NCMFs and their generalizations. A typical example of a Presburger safety property that we might want to verify for an NCMF M with counters x_1, x_2 and x_3 is the following: Starting from counter values satisfying $x_1 - x_2 + 3x_3 > 5$, M can only reach counter values satisfying $x_1 + 2x_2 - 4x_3 < 8$.

In this paper, we systematically study a number of Presburger liveness problems for NCMFs. An example is a ∃-Presburger-i.o. problem like: Given an NCMF M with counters x_1, x_2 and x_3, does there exist an ω-path (i.e., infinite execution path) p for M such that $x_1 + 2x_2 - 4x_3 < 8$ is satisfied on p infinitely often? The research presented in this paper is inspired by the recent work in [12] that investigates the same set of Presburger liveness problems for discrete timed automata. But the techniques we develop here are completely different from ones in [12]. Clocks in a discrete timed automaton, when considered as counters, are synchronous. So, in some way, a discrete timed automaton can be treated as a reversal-bounded multicounter machine (an NCMF without the free counter) [8]. The ability of an NCMF to use a free counter makes the Presburger liveness proofs much more complicated. The main results of this paper show that the $\exists$-Presburger-i.o. problem is decidable for NCMFs. This result leads us to conjecture that the $\exists$-Presburger-i.o. problem is also decidable for (discrete timed) pushdown processes when the counts on individual stack symbols are part of the Presburger property being verified [8].

The paper is organized as follows. Section 2 introduces the main definitions. Section 3 shows the decidability of the $\exists$-Presburger-i.o. and $\exists$-Presburger-eventual problems. Section 4 generalizes the proofs in [12] to show the undecidability of the $\forall$-Presburger-i.o. and the $\forall$-Presburger-eventual problems. Section 5 is a conclusion.

2 Preliminaries

Let $X = \{x_0, \cdots, x_k\}$ be a finite set of integer variables. Formula $\Sigma_{0\leq i\leq k} a_i x_i \# b$, where a_i and b are integers, is called an *atomic linear constraint*, if $\#$ is $>$ or $=$. The formula is called an *atomic mod-constraint*, if $\#$ is $\equiv_d$ for some $d > 0$. A *linear-conjunction* is a conjunction of a finite number of atomic linear constraints. A *linear-mod-conjunction* is a conjunction of a finite number of atomic linear constraints and atomic mod-constraints. It is well known that a Presburger formula [19] (first-order formula over integers with addition) can always be written as a disjunctive normal form of atomic linear constraints and atomic mod-constraints, i.e., a disjunction of linear-mod-conjunctions. A set P is *Presburger-definable* if there exists a Presburger formula F on X such that P is exactly the set of the solutions for X that make F true. It is well known that the class of Presburger-definable sets does not change if quantifications are allowed. Hence, when considering Presburger formulas, we will allow quantifiers over integer variables. A *standard test* on X is a Boolean combination of *atomic tests* in the form of $x\#c$, where $\#$ denotes $\leq, \geq, <, >$, or $=$, c is an integer, $x \in X$. Let $\mathcal{T}_X$ be the set of all standard tests on X.

A nondeterministic multicounter machine (NCM) M is a nondeterministic machine with a finite set of (control) states and a finite number of integer counters. Each counter can add 1, subtract 1, or stay unchanged. M can also test whether a counter is equal to, greater than, or less than an integer constant by performing a standard test. Without loss of generality, in this paper we consider M without event labels on transitions, since these labels can be built into the control states.

Formally, a *nondeterministic multicounter machine (NCM)* M is a tuple $\langle S, X, E\rangle$ where S is a finite set of *(control) states*, X is a finite set of integer counters, and $E \subseteq S \times \mathcal{T}_X \times \{-1, 0, 1\}^{|X|} \times S$ is a finite set of *edges* or *transitions*. Each edge $\langle s, t, \mathbf{incr}, s'\rangle$ denotes a transition from state s to state s' with $t \in \mathcal{T}_X$ being the *test* or the enabling condition. **incr** $\in \{-1, 0, 1\}^{|X|}$ denotes the effect of the edge: each counter in X is incremented by the amount specified in vector **incr**.

The semantics of NCMs is defined as follows. We use $\boldsymbol{V}$ to denote counter vectors (i.e., vectors of counter values). We use $\boldsymbol{V}_i$ to denote the value of counter x_i in $\boldsymbol{V}$, for $0 \leq i \leq k$. A *configuration* $\langle s, \boldsymbol{V} \rangle \in S \times \mathbf{Z}^{|X|}$ is a pair of a control state s and a counter vector $\boldsymbol{V}$. $\langle s, \boldsymbol{V} \rangle \rightarrow_M \langle s', \boldsymbol{V}' \rangle$ denotes a *one-step transition* from configuration $\langle s, \boldsymbol{V} \rangle$ to configuration $\langle s', \boldsymbol{V}' \rangle$ satisfying the following conditions:

- There is an edge $\langle s, t, \mathbf{incr}, s' \rangle$ in M connecting state s to state s',
- The enabling condition of the edge is satisfied, that is, $t(\boldsymbol{V})$ is true,
- Each counter changes according to the edge, i.e., $\boldsymbol{V}' = \boldsymbol{V} + \mathbf{incr}$.

A *path* is a finite sequence

$$\langle s_0, \boldsymbol{V}^0 \rangle \cdots \langle s_n, \boldsymbol{V}^n \rangle$$

such that $\langle s_i, \boldsymbol{V}^i \rangle \rightarrow_M \langle s_{i+1}, \boldsymbol{V}^{i+1} \rangle$ for each $0 \leq i \leq n-1$. An *ω-path* is an infinite sequence $\langle s_0, \boldsymbol{V}^0 \rangle \cdots \langle s_n, \boldsymbol{V}^n \rangle \cdots$ such that each prefix $\langle s_0, \boldsymbol{V}^0 \rangle \cdots \langle s_n, \boldsymbol{V}^n \rangle$ is a path. We write $\langle s, \boldsymbol{V} \rangle \rightsquigarrow_M \langle s', \boldsymbol{V}' \rangle$ if the configuration $\langle s, \boldsymbol{V} \rangle$ reaches the configuration $\langle s', \boldsymbol{V}' \rangle$ through a path in M. The binary relation $\rightsquigarrow_M$ is called *binary reachability*.

It is well known that counter machines with two counters have an undecidable halting problem. Thus, in order to investigate any nontrivial decidable verification problems for NCMs, we have to restrict the behaviors of the counters. A counter is *r-reversal-bounded* if it changes mode between nondecreasing and nonincreasing at most r times. For instance, the following sequence of counter values:

$$0, 0, 1, 1, 2, 2, 3, 3, 4, 4, 3, 2, 1, 1, 1, 1, \cdots$$

exhibits only one counter reversal. M is *reversal-bounded* if each counter in M is r-reversal-bounded for some r. M is a *reversal-bounded NCM with a free counter* (NCMF) if M has a number of reversal-bounded counters and an unrestricted counter (that need not be reversal-bounded). From now on, an NCM (NCMF) refers to a machine with reversal-bounded counters (and one free counter). We assume throughout that whenever we are given an NCM (NCMF), the reversal-bound r is also specified.

A fundamental result for NCMFs is that the binary reachability is Presburger. This characterization is quite useful, since it is well known that the emptiness and the validity problems for Presburger formulas are decidable.

Theorem 1. *The binary reachability is effectively Presburger definable for a reversal-bounded nondeterministic multicounter machine with a free counter. [15, 18]*

This fundamental result allows us to automatically verify a *Presburger safety analysis problem* for an NCMF M [8, 18]: from configurations in I, M can only reach configurations in P, where I and P are Presburger definable sets of configurations. This problem is equivalent to $\neg\exists\alpha\exists\beta(\alpha \in I \wedge \alpha \rightsquigarrow_M \beta \wedge \beta \in \neg P)$, which, from Theorem 1, is Presburger and therefore decidable.

In this paper, we systematically investigate *Presburger liveness analysis problems* for NCMFs by considering their ω-paths. We follow the notations in [12]. Let M be an NCMF, I and P be two Presburger-definable sets of configurations, and p be an ω-path $\langle s_0, \boldsymbol{V}^0 \rangle \cdots \langle s_n, \boldsymbol{V}^n \rangle \cdots$. We say that p *starts* from I if $\langle s_0, \boldsymbol{V}^0 \rangle \in I$. Define

- p is *P-i.o.* if P is satisfied infinitely often on the ω-path, i.e., there are infinitely many n such that $\langle s_n, \boldsymbol{V}^n\rangle \in P$.
- p is *P-always* if for each n, $\langle s_n, \boldsymbol{V}^n\rangle \in P$.
- p is *P-eventual* if there exists n such that $\langle s_n, \boldsymbol{V}^n\rangle \in P$.
- p is *P-almost-always* if there exists n such that for all $n' > n$, $\langle s_{n'}, \boldsymbol{V}^{n'}\rangle \in P$.

The $\exists$-Presburger-i.o. (resp. always, eventual and almost-always) problem for NCMF M is to decide whether the following statement holds:

there is an ω-path p starting from I that is P-i.o. (resp. P-always, P-eventual and P-almost-always).

The $\forall$-Presburger-i.o. (resp. always, eventual and almost-always) problem for NCMF M is to decide whether the following statement holds:

for every ω-path p, if p starts from I, then p is P-i.o. (resp. P-always, P-eventual and P-almost-always).

We use $\boldsymbol{X}$ to denote the vector of the $k+1$ counters $x_0, x_1, \cdots, x_k$ in M, with x_0 the free counter and with $x_1, \cdots, x_k$ the reversal-bounded counters.

3 Decidable Results

In this section, we show that both the $\exists$-Presburger-i.o. problem and the $\exists$-Presburger-eventual problem are decidable for NCMFs.

3.1 The $\exists$-Presburger-i.o. problem is decidable

The $\exists$-Presburger-i.o. problem is to determine the existence of an ω-path p (called a *witness*) $\langle s_0, \boldsymbol{V}^0\rangle \cdots \langle s_n, \boldsymbol{V}^n\rangle \cdots$ of an NCMF M such that p is P-i.o. with respect to I. Since P is a Presburger definable set of configurations, by definition, $P(\boldsymbol{X}, s)$ can be written in a disjunctive normal form, $\bigvee P_i(\boldsymbol{X}, s)$, where each $P_i(\boldsymbol{X}, s)$ is a linear-mod-conjunction of atomic linear constraints and atomic mod-constraints over counters and control states (control states are encoded as bounded integers) in M. Obviously, p is P-i.o. iff p is P_i-i.o. for some i. Therefore, without loss of generality, we assume P itself is a linear-mod-conjunction.

There are only finitely many control states $S = \{\hat{s}_1, \cdots, \hat{s}_m\}$ in M. Therefore, $P(\boldsymbol{X}, s)$ can be written as $\bigvee_{\hat{s}_i \in S} s = \hat{s}_i \wedge P(\boldsymbol{X}, \hat{s}_i)$. p is P-i.o. iff p is $P(\cdot, \hat{s}_i)$-i.o. *on some control state* $\hat{s}_i$: there are infinitely many n such that $s_n = \hat{s}_i$ and $P(\boldsymbol{V}^n, \hat{s}_i)$. Therefore, the $\exists$-Presburger-i.o. problem is reduced to the problem of deciding whether there exist a control state s and a witness p starting from I such that $p = \langle s_0, \boldsymbol{V}^0\rangle \cdots \langle s_n, \boldsymbol{V}^n\rangle \cdots$ is P-i.o. on s, where P is a linear-mod-conjunction on counters $\boldsymbol{X}$ only. Assume that $P(\boldsymbol{X})$ is $P^{\text{linear}}(\boldsymbol{X}) \wedge P^{\text{mod}}(\boldsymbol{X})$, where P^{linear} is a linear-conjunction over $\boldsymbol{X}$ and P^{mod} is a mod-conjunction over $\boldsymbol{X}$. The following lemma states that, as far as an infinite often property is concerned, P^{mod} can be eliminated by building "mod" into the control states of M.

Lemma 1. *Given M – an NCMF with counters $\boldsymbol{X}$ and with control states S, I – a Presburger-definable set of configurations of M, P – a linear-mod-conjunction over $\boldsymbol{X}$, and s – a control state in S, we can effectively construct M' – an NCMF with counters*

$\boldsymbol{X}$ and with control states S', I' – a Presburger-definable set of configurations of M', P' – a linear-conjunction over $\boldsymbol{X}$, and s' – a control state in S', such that the following two statements are equivalent:

- *In M, there exists a witness p starting from I such that p is P-i.o. on state s,*
- *In M', there exists a witness p' starting from I' such that p' is P'-i.o. on state s'.*

Because of Lemma 1, it suffices to investigate the existence of a P-i.o witness p on state s with P in the form of a linear-conjunction over m linear constraints:

$$\sum_{0 \leq i \leq k} a_{ij} x_i \#_j b_j \tag{1}$$

where $\#_j$ stands for $>$ or $=$, for $1 \leq j \leq m$. We use $\mathbf{A}$, $\#$, and $\mathbf{b}$ to denote the coefficient matrix (m by $k+1$) of a_{ij}, the column (m by 1) of comparisons $\#_j$, and the column (m by 1) of numbers b_j. Thus, P shown in (1) can be written as

$$\mathbf{A}\boldsymbol{X}\#\mathbf{b}. \tag{2}$$

We say $(k+1)$-ary vector $\boldsymbol{\Delta}$ is *P-positive* if $\mathbf{A}\boldsymbol{\Delta} \geq \mathbf{0}$. From definition, an ω-path p of $\langle s_0, \boldsymbol{V}^0\rangle \cdots \langle s_n, \boldsymbol{V}^n\rangle \cdots$ is a desired witness iff the following conditions are satisfied:

(IO-1). p starts from I; i.e., $I(s_0, \boldsymbol{V}^0)$ holds,
(IO-2). There are infinitely many numbers $n_1, \cdots, n_i, \cdots$ (with $0 < n_1 < \cdots < n_i < \cdots$) such that $s_{n_i} = s$ and $P(\boldsymbol{V}^{n_i})$ for each i.

The following lemma states that condition (IO-2) can be strengthened: for each i, $\boldsymbol{V}^{n_{i+1}} - \boldsymbol{V}^{n_i}$ is P-positive.

Lemma 2. *Let P be a linear conjunction as in (2). Let s be a state in an NCMF M. For any ω-path p of M, condition (IO-2) is equivalent to the following condition:*

(IO-2′). There are infinitely many numbers $n_1, \cdots, n_i, \cdots$ (with $0 < n_1 < \cdots < n_i < \cdots$) such that $s_{n_i} = s$, $P(\boldsymbol{V}^{n_i})$, and $\boldsymbol{V}^{n_{i+1}} - \boldsymbol{V}^{n_i}$ is P-positive, for each i.

Up to now, we have not used the condition that counters $x_1, \cdots, x_k$ are reversal-bounded and that counter x_0 is free. Let C be the largest absolute value of the integer constants appearing in all the tests in M. The idea is that, on the ω-path p, each reversal-bounded counter will eventually behave as a 0-reversal-bounded (i.e., either nondecreasing or nonincreasing) counter after the last reversal has been made. Once a reversal-bounded counter behaves as 0-reversal-bounded, it will either stay unchanged between $-C$ and C forever, or move beyond C (or $-C$) and never come back. That is, there is n_0 such that each reversal-bounded counter x_i, $1 \leq i \leq k$, has one of the following $2C+3$ *modes*:

(MD1-c) with $-C \leq c \leq C$. For all $n \geq n_0$, $\boldsymbol{V}_i^n = \boldsymbol{V}_i^{n+1} = c$. That is, x_i is always c that is between $-C$ and C after n_0,
(MD2). For all $n \geq n_0$, $C < \boldsymbol{V}_i^n \leq \boldsymbol{V}_i^{n+1}$. That is, x_i is nondecreasing and always greater than C,
(MD3). For all $n \geq n_0$, $-C > \boldsymbol{V}_i^n \geq \boldsymbol{V}_i^{n+1}$. That is, x_i is nonincreasing and always smaller than $-C$.

Let *mode vector* $\boldsymbol{\theta} \in (\{\text{MD1-}c : -C \leq c \leq C\} \cup \{\text{MD2}, \text{MD3}\})^k$ assign to each reversal-bounded counter x_i a mode $\boldsymbol{\theta}_i$. Each ω-path p has a unique mode vector. Now we fix any mode vector $\boldsymbol{\theta}$.

M can be effectively modified into an NCMF $M^{\boldsymbol{\theta}}$ such that the reversal-bounded counters in $M^{\boldsymbol{\theta}}$ behave according to the mode vector $\boldsymbol{\theta}$. An edge $\langle s^1, t, \mathbf{incr}, s^2\rangle$ in M is *compatible* with a mode vector $\boldsymbol{\theta}$, if, for each reversal-bounded counter x_i with $1 \leq i \leq k$, the following conditions hold:

- If x_i is in mode MD1-c for some $-C \leq c \leq C$, x_i will not change on the edge; i.e., $\mathbf{incr}_i = 0$ if $\boldsymbol{\theta}_i =$MD1-c,
- If x_i is in mode MD2, x_i will not decrease on the edge; i.e., $\mathbf{incr}_i \geq 0$ if $\boldsymbol{\theta}_i =$ MD2,
- If x_i is in mode MD3, x_i will not increase on the edge; i.e., $\mathbf{incr}_i \leq 0$ if $\boldsymbol{\theta}_i =$ MD3,

The modification starts with deleting all the edges in M that are not compatible with $\boldsymbol{\theta}$ from M. Then, more tests are added to the remaining edges to make sure that the reversal-bounded counters always have the desired values. More precisely, for each x_i with $1 \leq i \leq k$ and for each remaining edge $\langle s^1, t, \mathbf{incr}, s^2\rangle$ in M, if x_i is in mode MD2, then we add a test of $x_i > C$ to the original test t of the edge. Doing this will guarantee that the values of x_i before and after this edge are greater than C (no matter whether $\mathbf{incr}_i = 0$ or $\mathbf{incr}_i = 1$). The cases when x_i is in mode MD3 can be handled similarly. If, however, x_i is in mode MD1-c for some $-C \leq c \leq C$, we simply add a test of $x_i = c$ to the original test t of the edge. The result $M^{\boldsymbol{\theta}}$ is also an NCMF with 0-reversal-bounded counters.

Obviously, from the choice of constant C, $M^{\boldsymbol{\theta}}$ is insensitive to the actual starting values of the 0-reversal-bounded counters. That is, if (1) $\langle s^1, \boldsymbol{V}^1\rangle$ can reach $\langle s^2, \boldsymbol{V}^1 + \boldsymbol{\Delta}^1\rangle$ through a path p_1 in $M^{\boldsymbol{\theta}}$, and (2) $\langle s^2, \boldsymbol{V}^2\rangle$ can reach $\langle s^3, \boldsymbol{V}^2 + \boldsymbol{\Delta}^2\rangle$ through a path p_2 in $M^{\boldsymbol{\theta}}$, such that the free counter x_0 has the same value at the end of p_1 and at the beginning of p_2, i.e., $\boldsymbol{V}^1_0 + \boldsymbol{\Delta}^1_0 = \boldsymbol{V}^2_0$, then each 0-reversal-bounded counter x_i with $1 \leq i \leq k$ in p_2 can start from $\boldsymbol{V}^1_i + \boldsymbol{\Delta}^1_i$ (instead of $\boldsymbol{V}^2_i$) and at the end of p_2, x_i has value $\boldsymbol{V}^1_i + \boldsymbol{\Delta}^1_i + \boldsymbol{\Delta}^2_i$ (instead of $\boldsymbol{V}^2_i + \boldsymbol{\Delta}^2_i$). Thus, path p_1 can be extended according to path p_2. The reason is that after changing the starting value of x_i, the test of x_i on each edge on path p_2 gives the same truth value as the old starting value, and, hence, path p_2 can be perfectly followed after p_1. This is summarized in the following technical lemma.

Lemma 3. *For any control states s^1, s^2 and s^3, for any mode vector $\boldsymbol{\theta}$, for any (k+1)-ary vectors $\boldsymbol{V}^1$, $\boldsymbol{V}^2$, $\boldsymbol{\Delta}^1$, and $\boldsymbol{\Delta}^2$, if $\boldsymbol{V}^1_0 + \boldsymbol{\Delta}^1_0 = \boldsymbol{V}^2_0$, $\langle s^1, \boldsymbol{V}^1\rangle \leadsto_{M^{\boldsymbol{\theta}}} \langle s^2, \boldsymbol{V}^1 + \boldsymbol{\Delta}^1\rangle$ and $\langle s^2, \boldsymbol{V}^2\rangle \leadsto_{M^{\boldsymbol{\theta}}} \langle s^3, \boldsymbol{V}^2 + \boldsymbol{\Delta}^2\rangle$, then $\langle s^2, \boldsymbol{V}^1 + \boldsymbol{\Delta}^1\rangle \leadsto_{M^{\boldsymbol{\theta}}} \langle s^3, \boldsymbol{V}^1 + \boldsymbol{\Delta}^1 + \boldsymbol{\Delta}^2\rangle$.*

Let $I' = \{\beta : \exists \alpha \in I(\alpha \leadsto_M \beta)\}$. I' is the set of reachable configurations from configurations in I. From Theorem 1, I' is Presburger. The following lemma states that the $\exists$-Presburger i.o. problem of M can be reduced to one for 0-reversal-bounded NCMFs $M^{\boldsymbol{\theta}}$.

Lemma 4. *There exists a witness p in M starting from I that is P-i.o. at state s iff for some mode vector $\boldsymbol{\theta}$, there exists a witness p' in $M^{\boldsymbol{\theta}}$ starting from I' that is P-i.o. at state s.*

For any state s and mode vector $\boldsymbol{\theta}$, we define a predicate $Q^{s,\boldsymbol{\theta}}(v, v')$ as follows. $Q^{s,\boldsymbol{\theta}}(v, v')$ iff there exist two vectors $\boldsymbol{V}$ and $\boldsymbol{\Delta}$ such that the following statements are satisfied: (Q1). v and v' are the values of the free counter; i.e., $v = \boldsymbol{V}_0$ and $v' = \boldsymbol{V}_0 + \boldsymbol{\Delta}_0$; (Q2). Both $\boldsymbol{V}$ and $\boldsymbol{V} + \boldsymbol{\Delta}$ satisfy P; i.e., $P(\boldsymbol{V}) \wedge P(\boldsymbol{V} + \boldsymbol{\Delta})$; (Q3). Configuration $\langle s, \boldsymbol{V}\rangle$ can reach configuration $\langle s, \boldsymbol{V} + \boldsymbol{\Delta}\rangle$ in $M^{\boldsymbol{\theta}}$; i.e., $\langle s, \boldsymbol{V}\rangle \leadsto_{M^{\boldsymbol{\theta}}} \langle s, \boldsymbol{V} + \boldsymbol{\Delta}\rangle$; (Q4). $\boldsymbol{\Delta}$ is P-positive; (Q5). Finally, configuration $\langle s, \boldsymbol{V}\rangle$ is reachable from some configuration in I; i.e., $\langle s, \boldsymbol{V}\rangle \in I'$.

Lemma 5. *For any state s and mode vector $\boldsymbol{\theta}$, $Q^{s,\boldsymbol{\theta}}$ is Presburger.*

It is easy to check that $Q^{s,\boldsymbol{\theta}}$ is transitive.

Lemma 6. *For any state s and mode vector $\boldsymbol{\theta}$, $Q^{s,\boldsymbol{\theta}}$ is transitive. That is, for all integers v_1, v_2, and v_3, $Q^{s,\boldsymbol{\theta}}(v_1, v_2) \wedge Q^{s,\boldsymbol{\theta}}(v_2, v_3)$ implies $Q^{s,\boldsymbol{\theta}}(v_1, v_3)$.*

Before we go any further, we need to uncover the intuitive meaning underlying the definition of $Q^{s,\boldsymbol{\theta}}$. $Q^{s,\boldsymbol{\theta}}(v, v')$ indicates the following scenario. Through a path in $M^{\boldsymbol{\theta}}$, $M^{\boldsymbol{\theta}}$ can send the free counter x_0 from value v to v', with some properly chosen starting values for the 0-reversal-bounded counters ((Q1) and (Q3)). On the path, $M^{\boldsymbol{\theta}}$ starts from control state s and finally moves back to the same control state, as given in (Q3). Therefore, this path is a loop on the control state s. It is noticed that the starting configuration and the ending configuration of the path both satisfy P (as given in (Q2)), and in particular, the counter changes $\boldsymbol{\Delta}$ is P-positive (as given in (Q4)).

If we can repeat the loop, then the resulting ω-path is P-i.o. (this is because of Lemma 2 and the fact that $\boldsymbol{\Delta}$ is P-positive.) and, from (Q5), starts from I'. However, this loop may not repeat. The reason is that the starting value v of the free counter decides the path of the loop and therefore, when $M^{\boldsymbol{\theta}}$ executes the loop for a second time, the starting value v' of the free counter may lead to a different path. Thus, trying to repeat the same loop is too naive. However, the key technique shown below attempts to concatenate infinitely many (different) loops into an ω-path that is a P-i.o. witness.

Let v^ω be an ω-sequence of integers

$$v_0, v_1, \cdots, v_n, \cdots.$$

v^ω is an *ω-chain* of $Q^{s,\boldsymbol{\theta}}$ if $Q^{s,\boldsymbol{\theta}}(v_n, v_{n+1})$ holds for all $n \geq 0$. According to Lemma 6, $Q^{s,\boldsymbol{\theta}}$ is transitive. Therefore, if v^ω is an ω-chain then $Q^{s,\boldsymbol{\theta}}(v_n, v_m)$ holds for any $n < m$. The following lemma states that the existence of an ω-chain for $Q^{s,\boldsymbol{\theta}}$ is decidable.

Lemma 7. *It is decidable whether a transitive Presburger predicate over two variables has an ω-chain. Thus, from Lemma 5 and Lemma 6, it is decidable whether $Q^{s,\boldsymbol{\theta}}$ has an ω-chain.*

We now show that the existence of a P-i.o witness p at state s starting from I is equivalent to the existence of an ω-chain of $Q^{s,\boldsymbol{\theta}}$ for some mode vector $\boldsymbol{\theta}$.

Lemma 8. *There is an ω-path p that is P-i.o. at state s and starts from I iff, for some mode vector $\boldsymbol{\theta}$, $Q^{s,\boldsymbol{\theta}}$ has an ω-chain.*

Finally, combining Lemma 7 and Lemma 8, we have,

Theorem 2. *The* $\exists$*-Presburger-i.o. problem is decidable for reversal-bounded multicounter machines with a free counter.*

The $\exists$-Presburger-i.o. problem is equivalent to the negation of the $\forall$-Presburger-almost-always problem. Thus,

Theorem 3. *The* $\forall$*-Presburger-almost-always problem is decidable for reversal bounded multicounter machines with a free counter.*

3.2 The $\exists$-Presburger-eventual problem is decidable

Given two Presburger-definable sets I and P of configurations for NCMF M, the $\exists$-Presburger-eventual problem is to decide whether there exists a P-eventual ω-path p starting from I. Recall that the Presburger-definable set I' is the set of all configurations in P that are reachable from a configuration in I. In the following lemma, **true** means the set of all configurations. It is easy to see that

Lemma 9. *There is a* P*-eventual* ω*-path starting from* I *iff there is a* **true***-i.o.* ω*-path starting from* I'*.*

Hence, combining Lemma 9 and Theorem 2, we have,

Theorem 4. *The* $\exists$*-Presburger-eventual problem is decidable for reversal-bounded multicounter machines with a free counter.*

Since the $\exists$-Presburger-eventual problem is equivalent to the negation of the $\forall$-Presburger-always problem, we have,

Theorem 5. *The* $\forall$*-Presburger-always problem is decidable for reversal-bounded multicounter machines with a free counter.*

The Presburger safety analysis problem is slightly different from the $\forall$-Presburger-always problem: the former looks at (finite) paths, while the latter looks at ω-paths.

4 Undecidable Results

In this section, we point out that both the $\exists$-Presburger-always problem and the $\exists$-Presburger-almost-always problem are undecidable for 0-reversal-bounded NCMs. Obviously, the undecidability remains when NCMFs are considered.

In [12], it is shown that the $\exists$-Presburger-always problem and the $\exists$-Presburger-almost-always problem are undecidable for discrete timed automata. The following techniques are used in that paper:

- A deterministic two-counter machine can be simulated by a generalized discrete timed automaton that allows tests in the form of linear constraints,
- The generalized discrete timed automaton can be simulated by a discrete timed automaton under a Presburger path restriction P [12] (i.e., each intermediate configuration of the discrete timed automaton must be in P),

- The halting problem (i.e., whether a control state is reachable, which is undecidable) for deterministic two-counter machines can be reduced to the $\exists$-Presburger-always problem for discrete timed automata,
- The finiteness problem (which is undecidable) for deterministic two-counter machines can be reduced to the $\exists$-Presburger-almost-always problem for discrete timed automata.

If in the items above, "discrete timed automaton" is replaced by "0-reversal-bounded multicounter machine", the techniques are still applicable. The reason is that, as shown below, any deterministic two-counter machine can be simulated by a deterministic generalized 0-reversal-bounded multicounter machine that allows tests in the form of linear constraints on counters.

Lemma 10. *Any deterministic two-counter machine M can be simulated by a deterministic 0-reversal-bounded multicounter machine M' that allows tests in the form of $y - z\#c$, where y and z are counters, and c is an integer [18].*

Analogous to the proofs in [12], we have,

Theorem 6. *The $\exists$-Presburger-always problem and the $\exists$-Presburger-almost-always problem are undecidable for 0-reversal-bounded multicounter machines. The undecidability remains when reversal-bounded multicounter machines with a free counter are considered.*

Considering the negations of the two problems, we have,

Theorem 7. *The $\forall$-Presburger-eventual problem and the $\forall$-Presburger-i.o. problem are undecidable for 0-reversal-bounded multicounter machines. The undecidability remains when reversal-bounded multicounter machines with a free counter are considered.*

5 Conclusions

In this paper, we investigated a number of Presburger liveness problems for NCMFs. We showed that

- The $\exists$-Presburger-i.o. problem and the $\exists$-Presburger-eventual problem are both decidable. So are their duals, the $\forall$-Presburger-almost-always problem and the $\forall$-Presburger-always problem.
- The $\forall$-Presburger-i.o. problem and the $\forall$-Presburger-eventual problem are both undecidable. So are their duals, the $\exists$-Presburger-almost-always problem and the $\exists$-Presburger-always problem.

These results can be used to formulate a weak form of Presburger linear temporal logic and develop its model-checking theories for NCMFs. We believe the techniques developed in [12] and in this paper can be naturally combined to study the same set of liveness problems on an extended form of discrete timed automata containing, besides clocks, a number of reversal-bounded counters and a free counter. We conjecture that the $\exists$-Presburger-i.o. problem is also decidable for (discrete timed) pushdown automata when the counts on individual stack symbols are part of the Presburger property being verified [8].

As for applications of NCMFs, "reversal-bounded counters" may appear unnatural, and applying the decidable results presented in this paper in model-checking may seem remote. However, the model of NCMFs does have applications in verification/debugging infinite state systems as we discuss below.

- Many infinite state systems can be modeled as multicounter machines. These machines, usually having Turing computing power, can be approximated by NCMFs by restricting all but one counter to be reversal-bounded. This approximation technique provides a way to debug Presburger safety properties for, for instance, arithmetic programs (for a number of conservative approximation techniques for real-time systems see [9–11]). On the other hand, the technique also shows a way to verify an $\exists$-Presburger i.o. problem for a multicounter machine if the same problem is true on the resulting NCMF.
- A non-decreasing counter is also a reversal-bounded counter with zero reversal bound. This kind of counters has a lot of applications. For instance, it can be used to count time elapse, the number of external events, the number of a particular branch taken by a nondeterministic program (this is important, when fairness is taken into account), etc. For example, consider a finite-state transition system T. Associate a name 'a' from a finite alphabet to each transition in T (a, in the *reactive* system T, can be treated as the input signal triggering the transition). At any moment in an execution of T, $\#_a$ is used to count the number of transitions labeled by a that have been executed. Each $\#_a$ can be considered as a 0-reversal-bounded counter, since $\#_a$ is nondecreasing along any execution path. To make the system more complex, on some transitions, the triggering conditions also contain a test that compares $\#_b - \#_c$ against an integer constant, for some fixed labels b and c [1]. Essentially T can be treated as a NCMF: those counts of $\#_a$'s are reversal-bounded counters and $\#_b - \#_c$ is the free counter. The results in this paper show that the following statement can be automatically verified:

  There is an execution of T such that $\#_a + 2\#_b - 5\#_c > 0$ holds for infinitely many times.

  This result can be used to argue whether a fairness condition on the event label counts of T is realistic.

The decision procedure for the $\exists$-Presburger i.o. problem seems hard to implement. However, by closely looking at the proofs, the hard part is how to (practically) calculate the binary reachability of an NCMF. Once this is done, testing the existence of the ω-chain in Lemma 7 and Lemma 8 is equivalent to checking a Presburger predicate (i.e., $Q^{s,\boldsymbol{\theta}}$ in the lemmas) in a particular format (the Omega Library [22] can be used to do the checking). Calculating the binary reachability of an NCMF needs some software engineering thoughts. We are currently conducting a prototype tool implementation.

Thanks go to anonymous reviewers for many useful suggestions.

[1] It is important that b and c are fixed. If we allow comparisons on the counts of four labels (i.e., besides the test on $\#_b - \#_c$, we have a test on $\#_d - \#_e$), then T is Turing powerful [18].

References

1. R. Alur and D. Dill, *"The theory of timed automata," TCS*, 126(2):183-236, 1994
2. P. Abdulla and B. Jonsson, *"Verifying programs with unreliable channels," Information and Computation*, 127(2): 91-101, 1996
3. A. Bouajjani, J. Esparza, and O. Maler. *"Reachability analysis of pushdown automata: application to model-Checking," CONCUR'97*, **LNCS** 1243, pp. 135-150
4. G. Cece and A. Finkel, *"Programs with Quasi-Stable Channels are Effectively Recognizable," CAV'97*, **LNCS** 1254, pp. 304-315
5. H. Comon and Y. Jurski. *"Multiple counters automata, safety analysis and Presburger arithmetic," CAV'98*, **LNCS** 1427, pp. 268-279
6. H. Comon and Y. Jurski, *"Timed automata and the theory of real numbers," CONCUR'99*, **LNCS** 1664, pp. 242-257
7. Z. Dang, *"Binary reachability analysis of timed pushdown automata with dense clocks," CAV'01*, **LNCS** 2102, pp. 506-517
8. Z. Dang, O. H. Ibarra, T. Bultan, R. A. Kemmerer and J. Su, *"Binary Reachability Analysis of Discrete Pushdown Timed Automata," CAV'00*, **LNCS** 1855, pp. 69-84
9. Z. Dang, O. H. Ibarra and R. A. Kemmerer, *"Decidable Approximations on Generalized and Parameterized Discrete Timed Automata," COCOON'01*, **LNCS** 2108, pp. 529-539
10. Z. Dang and R. A. Kemmerer, *"Using the ASTRAL model checker to analyze Mobile IP," Proceedings of the Twenty-first International Conference on Software Engineering (ICSE'99)*, pp. 132-141, IEEE Press, 1999
11. Z. Dang and R. A. Kemmerer, *"Three approximation techniques for ASTRAL symbolic model checking of infinite state real-time systems," Proceedings of the Twenty-second International Conference on Software Engineering (ICSE'00)*, pp. 345-354, IEEE Press, 2000
12. Z. Dang, P. San Pietro, and R. A. Kemmerer, *"On Presburger Liveness of Discrete Timed Automata," STACS'01*, **LNCS** 2010, pp. 132-143
13. A. Finkel and G. Sutre. *"Decidability of Reachability Problems for Classes of Two Counter Automata," STACS'00*, **LNCS** 1770, pp. 346-357
14. A. Finkel, B. Willems, and P. Wolper. *"A direct symbolic approach to model checking pushdown systems," INFINITY'97*
15. O. H. Ibarra, *"Reversal-bounded multicounter machines and their decision problems," J. ACM*, **25** (1978) 116-133
16. O. H. Ibarra, *"Reachability and safety in queue systems with counters and pushdown stack," Proceedings of the International Conference on Implementation and Application of Automata*, pp. 120-129, 2000
17. O. H. Ibarra, Z. Dang, and P. San Pietro, *"Verification in Loosely Synchronous Queue-Connected Discrete Timed Automata,"* submitted. 2001
18. O. H. Ibarra, J. Su, T. Bultan, Z. Dang, and R. A. Kemmerer, *"Counter Machines: Decidable Properties and Applications to Verification Problems,", MFCS'00*, **LNCS 1893**, pp. 426-435
19. G. Kreisel and J. L. Krevine, *"Elements of Mathematical Logic,"* North-Holland, 1967
20. K. L. McMillan. *"Symbolic model-checking - an approach to the state explosion problem,"* PhD thesis, Department of Computer Science, Carnegie Mellon University, 1992
21. W. Peng and S. Purushothaman. *"Analysis of a Class of Communicating Finite State Machines," Acta Informatica*, 29(6/7): 499-522, 1992
22. W. Pugh, *"The Omega test: a fast and practical integer programming algorithm for dependence analysis," Communications of the ACM*, 35(8): 102-114, 1992