Dense Counter Machines and Verification Problems

Gaoyan Xie[1], 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, USA
[2] Department of Computer Science
University of California
Santa Barbara, CA 93106, USA
[3] Dipartimento di Elettronica e Informazione
Politecnico di Milano, Italia

Abstract. We generalize the traditional definition of a multicounter machine (where the counters, which can only assume nonnegative integer values, can be incremented/decremented by 1 and tested for zero) by allowing the machine the additional ability to increment/decrement each counter C_i by a nondeterministically chosen fractional amount δ_i between 0 and 1 (δ_i may be different at each step). Further at each step, the δ_i's of some counters can be linearly related in that they can be integral multiples of the same fractional δ (e.g., $\delta_1 = 3\delta$, $\delta_3 = 6\delta$). We show that, under some restrictions on counter behavior, the binary reachability set of such a machine is definable in the additive theory of the reals and integers. There are applications of this result in verification, and we give an example in the paper. We also extend the notion of "semilinear language" to "dense semilinear language" and show its connection to a restricted class of dense multicounter automata.

1 Introduction

Dense counters are necessary in modeling many control systems and real-time applications. Their importance has already been noticed in model-checking. One of the focuses during the past ten years is the study of hybrid automata [2,13] where dense counters follow some complex continuous flow, typically characterized by differential equations, and interact with bounded discrete control variables. Decidable results on reachability has been obtained for many forms of hybrid automata (e.g., timed automata [3], multirate automata [2,18], initialized rectangular automata [19]). On the other hand, linear hybrid automata in general are undecidable for reachability [19]. In fact, the undecidability remains even for timed automata augmented with one stop watch [19].

Another focus approaches dense counters in a different way. Ultimately, in the view of an external observer, the evolution of a system containing dense counters in $\mathbf{X}$ can

* Corresponding author (`zdang@eecs.wsu.edu`).

** The research of Oscar H. Ibarra has been supported in part by NSF Grants IIS-0101134 and CCR02-08595.

*** Supported in part by MIUR grants FIRB RBAU01MCAC, COFIN 2001015271, CNR Strategico 1999-Società dell'Informazione -SP4.

be characterized by a formula $T(s, \mathbf{X}, s', \mathbf{X}')$, whose meaning is roughly: the system transits from control state s to s' while changing the counters from $\mathbf{X}$ to $\mathbf{X}'$. In other words, T characterizes a one-step transition of the system, called a dense counter system. A fundamental question is then: what kinds of T would make the transitive closure T^* computable? Many model-checking queries (e.g., reachability) relies on the answer. Some results studying special forms of T and its (restricted) transitive closure can be found in e.g., [6,7,20,5,12].

Recently, it has been shown that some fundamental results in automata theory (such as [14,15,8]) on some restricted discrete counter machines are quite useful in studying various model-checking problems for infinite state systems containing discrete counters (e.g., [9,11] etc.). Following this line, we believe that developing a fundamental theory (which does not exist) in the view of automata theory for these machines but with dense counters should be equally useful for studying dense counter systems. This automata-theoretic approach is different from those taken in [6,20,5,12] mentioned earlier. As a starting point, in this paper we will develop a preliminary automata theory for dense counter machines.

We define a dense counter machine $\mathcal{M}$ as a finite state machine augmented with a number of dense counters. The counters can assume nonnegative real values. At each step, each counter C_i can be incremented/decremented by 0, 1 or a nondeterministically chosen fractional amount δ_i between 0 and 1 (δ_i may be different at each step). We will see that without loss of generality, we can assume that at a single step, for all i, the δ_i's are of the same amount δ (but still the δ may be different between steps). This δ-increment/decrement is the essential difference between dense and discrete counters. The machine $\mathcal{M}$ can also test a counter against 0 ($= 0?, > 0?$). Since counters are assumed nonnegative, $\mathcal{M}$ crashes if a counter falls below 0. (Note that since the counters can be tested against 0, the system can actually check if it will crash and if so enter a distinguished state. So the assumption of "crashing" can be made w.l.o.g.) Given two designated states s_{init} and s_{final} in $\mathcal{M}$, we study the possibility of computing the transitive closure "$\rightsquigarrow$", called the binary reachability, of $\mathcal{M}$:

$$\mathbf{X} \rightsquigarrow \mathbf{X}' \text{ iff } \mathbf{X} \text{ at } s_{\text{init}} \text{ reaches } \mathbf{X}' \text{ at } s_{\text{final}} \text{ in } \mathcal{M}.$$

On the negative side, even the state reachability problem (whether s_{init} reaches s_{final}, or equivalently, whether $\rightsquigarrow$ is empty) is in general undecidable. This is because a two (discrete) counter machine can be simulated by $\mathcal{M}$ in which no δ-increments/decrements are made. But, what if $\mathcal{M}$ only performs δ-increments/decrements (along with tests against 0)? In this case, the undecidability remains even when there are only four dense counters. Interestingly, still in this case, the state reachability problem becomes decidable when there are two counters. The case for three counters is open.

On the positive side, we will show some restricted versions of $\mathcal{M}$ whose binary reachability is definable in the additive theory of the reals and integers. The theory is decidable, for instance, by the Büchi-automata based decision procedure presented in [4] and a quantifier elimination technique in [21]. This will allow us to automatically verify some safety properties for the restricted $\mathcal{M}$: Are there $\mathbf{X}$ and $\mathbf{X}'$ such that $I(\mathbf{X}, \mathbf{X}') \wedge \mathbf{X} \rightsquigarrow \mathbf{X}'$? where I is definable in the additive theory of the reals and integers (e.g., $x_1 + x'_1 - 3x_2 > 4 \wedge x_3 - x'_2$ *is an integer* $\wedge x'_2 - x_1 < 7$). Furthermore, some liveness properties (e.g., infinitely ofteness [11]) can also be automatically verified:

Are there $\mathbf{X}^0, \cdots, \mathbf{X}^n, \cdots$ such that $\mathbf{X}^0 \leadsto \mathbf{X}^1 \leadsto \cdots \leadsto \mathbf{X}^n \leadsto \cdots$, $I(\mathbf{X}_0)$ holds, and, there are infinitely many n for which $P(\mathbf{X}_n)$ holds?

where I and P are definable in the additive theory of the reals and integers.

In this paper, we first consider a restricted version of $\mathcal{M}$ in which all the dense counters are monotonic (i.e., never decreasing). Then we consider the case when all the dense counters are reversal-bounded (the alternations between nondecreasing and nonincreasing are bounded by a fixed integer, for each counter). The concept of "reversal-boundedness" is borrowed from its counterpart for discrete counters [14]. It is not too difficult to prove that in these cases $\leadsto$ is definable in the additive theory of the reals and integers. The proof becomes more difficult when $\mathcal{M}$ is further augmented with an unrestricted dense counter (called a free counter). In the rather complex proof, we use a "shifting" technique to simplify the behavior of the free counter.

The proofs can be easily generalized to the cases when counters in $\mathcal{M}$ are of multirate. That is, a nonnegative integer rate vector $(r_1, \cdots, r_k)$ is now associated with a counter instruction such that, for each counter x_i ($1 \le i \le k$), an increment/decrement by 1 now corresponds to an increment/decrement by r_i; an increment/decrement by δ now corresponds to an increment/decrement by $r_i \cdot \delta$. Also note that, in an instruction, the δ need not necessarily be the same for each counter. For instance, one may have an instruction by associating δ_1 with x_1, x_2 and δ_2 with x_4, x_5 as follows:

```
s: if $x_1 > 0$ then for some $0 < \delta_1, \delta_2 < 1$,
        $x_1' = x_1 + 3 \cdot \delta_1,\ x_2' = x_2 - 4 \cdot \delta_1,\ x_3' = x_3 + 5 \cdot 1,$
        $x_4' = x_4 - 6 \cdot \delta_2,\ x_5' = x_5 - 7 \cdot \delta_2,$
goto $s'$.
```

The automata-theoretic approach taken in this paper is new and the decidable results for the transitive closure computations on the counter systems are incomparable to previously known results (e.g., [6,20,5,12]). The models, e.g., the reversal-bounded dense counter machines with a free counter, are incomparable with some restricted and decidable models for hybrid systems (e.g., timed automata [3], initialized rectangle automata [19], etc). In the future, we plan to use the results in this paper as a fundamental tool to reason about a broader class of dense counter systems. For instance, we may study a subclass of timed automata whose accumulated delays [1] are decidable over a formula of the additive theory of reals and integers. Our models are convenient in modeling accumulated delays which are simply monotonic dense counters. We can also use the model to specify some interesting systems with multiple dense/discrete counters.

Consider, e.g., the following version of the traditional producer-consumer system. A system may *produce*, *consume* or be *idle*. When in state $produce$, a resource is produced, which may be stored and later consumed while in state $consume$. The system may alternate between production and consumption states, but it may not produce and consume at the same time. Production may be stored, and used up much later (or not used at all). The novelty is that the resource may be a real number, representing for instance the available amount of a physical quantity (e.g., fuel, water or time).

This system may be easily modeled by a finite state machine with a free purely-dense counter, where the resource is added when produced or subtracted when consumed. Since the free counter may never decrease below zero (e.g., it can tested against 0), the system clearly implements the physical constraint that consumption must never exceed production. Using a dense-counter, there is an underlying assumption that a continuous variable, such as our resource, changes in discrete steps only; however, this is acceptable in many cases where a variable actually changes continuously, since the increments/decrements may be arbitrarily small.

We note that decidable versions of timed or hybrid automata do not appear to be able to specify the producer-consumer example above (even though we cannot rule out that some other decidable model can). In timed automata, when the resource is interpreted as time, the amount of production (respectively, consumption) is equivalent to the “total accumulated time spent while in state $produce$ (respectively, $consume$)". Implementing the constraint $production - consumption \geq 0$ is then tantamount to implementing a stop watch, which is known to lead to undecidability of the model. In hybrid automata, a continuous variable for $production - consumption$ must have different flow rates in state $produce$ (nonnegative) and in state $consume$ (nonpositive). A rate change, at least for the decidable class of initialized rectangular automata, forces the variable to be reinitialized to a predefined value after a state change: the value a variable had in state $produce$ is lost in state $consume$. Adding more variables does not appear to solve the problem, either, since no variable comparison is possible.

The dense-counter model of the example can be easily adapted to more complex situations. For instance, suppose that a constraint on the system is that total production is at most twice the amount of consumption. This can be described by adding two reversal-bounded dense counters, namely p, c, to store the total production (p) and twice the total consumption (c). For the sake of clarity, a nondeterministic version of the producer-consumer model $\mathcal{M}$ is shown in Figure 1, in which counter *count* denotes the difference between the total production and the total consumption. Each arc has a boolean guard and may specify an increment or decrement that is a multiple of a δ, $0 < \delta < 1$, for each counter *count*, p, c. Recall that δ may be different at eah step. If no variation is specified, then the counter stays. When in the (initial) state *idle*, $\mathcal{M}$ may

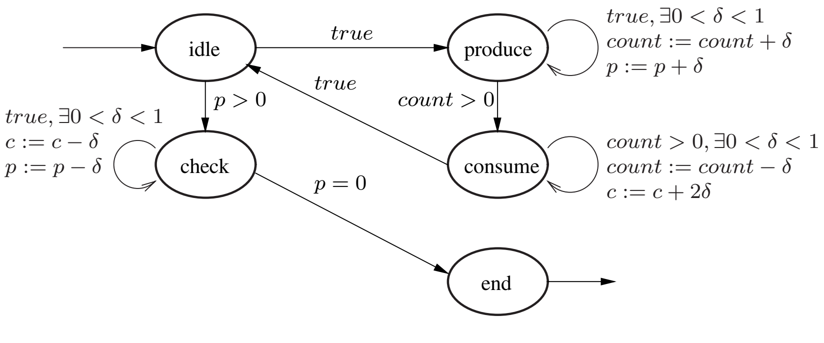
idle
produce
check
consume
end
$true$
$true$
$p > 0$
$count > 0$
$p = 0$
$true, \exists 0 < \delta < 1$
$count := count + \delta$
$p := p + \delta$
$true, \exists 0 < \delta < 1$
$c := c - \delta$
$p := p - \delta$
$count > 0, \exists 0 < \delta < 1$
$count := count - \delta$
$c := c + 2\delta$

Fig. 1. A producer-consumer system $\mathcal{M}$.

start producing or, nondeterministically, may go into the checking state if $p > 0$. While producing (in state *produce*), counter p is increased together with *count* (hence, of the same amount). Eventually consumption starts: counter c is increased in state *consume* of the double amount used to decrease $count$. Then $\mathcal{M}$ may go back to the *idle* state. Notice that $count$ may never go below 0, otherwise $\mathcal{M}$ crashes (alternatively, $count$ could be tested against 0, but crashing is ruled out since it leads anyway to a nonaccepting path).

When finished producing and consuming, $\mathcal{M}$ goes into state *check*, where it decrements both p and c until p goes to 0. At this time, it moves to the final state *end*. Hence, if the value of c is not greater or equal to p, $\mathcal{M}$ crashes. Nondeterminism allows the automaton to guess a sequence of decrements δ that leads to $p = 0$ and hence to the final state *end*. To verify that the system really produces at most twice than it consumes, it is enough to check whether $\mathcal{M}$ may reach state *end*. Similar linear bounds, such as "total production should not exceed consumption more than 5 per cent", can be dealt with analogously.

A more sophisticated verification capability is given by the fact that the binary reachability $\leadsto^{\mathcal{M}}$ is not only computable but may be represented with a formula in the additive theory of reals and integers (hence, decidable). For instance, consider the property that the system may be implemented with finite storage (i.e., *count* is bounded). This can be expressed by the following decidable formula:

$$\exists y > 0\ \forall s \forall \mathbf{X}\ \big((idle, \mathbf{0}) \leadsto^{\mathcal{M}} (s, X)\ \Rightarrow\ \mathbf{X}(count) \leq y\big)$$

whose meaning is that there is a bound $y > 0$ such that, starting in $idle$ state with all counters equal to 0, $\mathcal{M}$ can only reach configurations $(s, \mathbf{X})$ where the value of $count$ in $\mathbf{X}$, $\mathbf{X}(count)$, is not greater than y.

In the simple case of Figure 1, the property is obviously violated since for instance production in state *produce* may go on unbounded without consumption.

Due to space limitation, proofs are omitted in the paper. The full version of the paper is accessible at `www.eecs.wsu.edu/~zdang`.

2 Preliminaries

A dense counter is a nonnegative real variable. A dense multicounter machine $\mathcal{M}$ is a finite state machine augmented with a number of dense counters. On a move from one state to another, $\mathcal{M}$ can add an amount of $0, +1, -1, +\delta$, or $-\delta$ for some nondeterministically chosen δ, with $0 < \delta < 1$. On a move, $\mathcal{M}$ can also test a counter against 0 while leaving all the counters unchanged. Formally, we have the following definitions. A dense counter changes according to one of the following five *modes*: stay, unit increment, unit decrement, fractional increment, fractional decrement. We use $\mathbf{X}$ to denote a vector of values for dense counters $x_1, \cdots, x_k$. In the sequel, we shall use $\mathbf{X}(x_i)$ to denote the component for x_i in $\mathbf{X}$. A *mode vector* is a k-tuple of modes. There are 5^k different mode vectors. Given a mode vector $\mathbf{m} = (m_1, \cdots, m_k)$ and an amount $0 < \delta < 1$, we define

$$R_{\mathbf{m},\delta}(\mathbf{X}, \mathbf{X}')$$

as follows: $R_{\mathbf{m},\delta}(\mathbf{X}, \mathbf{X}')$ iff for each $1 \leq i \leq k$, $\mathbf{X}(x_i) \geq 0$ and $\mathbf{X}'(x_i) \geq 0$, and each of the followings holds:

- if m_i is stay, then $\mathbf{X}'(x_i) = \mathbf{X}(x_i)$;
- if m_i is unit increment, then $\mathbf{X}'(x_i) = \mathbf{X}(x_i) + 1$;

- if m_i is unit decrement, then $\mathbf{X}'(x_i) = \mathbf{X}(x_i) - 1$;
- if m_i is fractional increment, then $\mathbf{X}'(x_i) = \mathbf{X}(x_i) + \delta$;
- if m_i is fractional decrement, then $\mathbf{X}'(x_i) = \mathbf{X}(x_i) - \delta$.

We use

$$R_{\mathbf{m}}(\mathbf{X}, \mathbf{X}')$$

to characterize the relationship between the old values $\mathbf{X}$ and the new values $\mathbf{X}'$ under the mode vector; i.e., $R_{\mathbf{m}}(\mathbf{X}, \mathbf{X}')$ is true iff there exists some $0 < \delta < 1$ such that $R_{\mathbf{m},\delta}(\mathbf{X}, \mathbf{X}')$ holds. Notice that when $\mathbf{m}$ does not contain any mode of fractional increment/decrement, the amount δ is irrelevant.

Formally, a *(nondeterministic) dense counter machine* $\mathcal{M}$ is tuple

$$\langle S, \{x_1, \cdots, x_k\}, s_{\text{init}}, s_{\text{final}}, T \rangle, \tag{1}$$

where S is a finite set of *(control) states* where s_{init} and s_{final} are the initial and the final states. $x_1, \cdots, x_k$ are dense counters. T is a set of transitions. Each transition is a triple $(s, \mathbf{m}, s')$ of a source state s, a mode vector $\mathbf{m}$, and a destination state s'. A configuration of $\mathcal{M}$ is a pair $(s, \mathbf{X})$ of a state and (nonnegative) dense counter values. We write

$$(s, \mathbf{X}) \xrightarrow{\mathbf{m}} (s', \mathbf{X}'),$$

called a move of $\mathcal{M}$, if $(s, \mathbf{m}, s') \in T$ and $R_{\mathbf{m}}(\mathbf{X}, \mathbf{X}')$. As usual, $(s, \mathbf{X})$ *reaches* $(s', \mathbf{X}')$, written $(s, \mathbf{X}) \rightsquigarrow (s', \mathbf{X}')$, if there are states $s_0 = s, s_1, \cdots s_n = s'$, mode vectors $\mathbf{m}_1, \cdots, \mathbf{m}_n$, counter values $\mathbf{X}^0 = \mathbf{X}, \mathbf{X}^1, \cdots, \mathbf{X}^n = \mathbf{X}'$, for some n, such that

$$(s_0, \mathbf{X}^0) \overset{\mathbf{m}_1}{\to} (s_1, \mathbf{X}^1) \cdots \overset{\mathbf{m}_n}{\to} (s_n, \mathbf{X}^n). \tag{2}$$

The set of all pairs $(\mathbf{X}, \mathbf{X}')$ satisfying $(s_{\text{init}}, \mathbf{X}) \rightsquigarrow (s_{\text{final}}, \mathbf{X}')$ is called the *binary reachability* of $\mathcal{M}$. $\mathcal{M}$ can be thought of as a transducer, which is able to generate $\mathbf{X}'$ from $\mathbf{X}$ whenever $(\mathbf{X}, \mathbf{X}')$ is in the binary reachability.

Before proceeding further, some more definitions are needed. $\mathcal{M}$ is *monotonic* (resp. *purely dense*, *purely discrete*) if, in every transition $(s, \mathbf{m}, s')$ in T, the mode vector $\mathbf{m}$ does not contain any mode of unit/fractional decrement (resp. unit increment/decrement, fractional increment/decrement). Let r be a nonnegative integer. A sequence of modes is *r-reversal-bounded* if, on the sequence, the mode changes from a unit/fractional increment (followed by 0 or more stay modes) to a unit/fractional decrement and vice versa for at most r number of times. On an execution in (2) from s to s', counter x_i is *r-reversal-bounded* if the sequence of modes for x_i is r-reversal-bounded. Counter x_i is *reversal-bounded* in $\mathcal{M}$ if there is an r such that, on every execution from s_{init} to s_{final}, x_i is r-reversal-bounded. $\mathcal{M}$ is a reversal-bounded dense multicounter machine if every counter in $\mathcal{M}$ is reversal-bounded. $\mathcal{M}$ is a reversal-bounded dense multicounter machine with a free counter if all but one counters in $\mathcal{M}$ are reversal-bounded. The notion of reversal-boundedness is generalized from the same notion for discrete counters [14]. Also notice that a dense counter in $\mathcal{M}$ can be effectively restricted to be reversal-bounded, since one may use additional control states to remember each reversal and not to go over the bound. A discrete multicounter machine is a dense multicounter machine that is purely discrete and whose counters start from nonnegative integer values. Similarly, one can define a monotonic discrete multicounter machine, a reversal-bounded discrete multicounter machine, and a reversal-bounded discrete multicounter machine with a free discrete counter (NCMF).

Let m and n be positive integers. Consider a formula

$$\sum_{1 \le i \le m} a_i x_i + \sum_{1 \le j \le n} b_j y_j \sim c,$$

where each x_i is a nonnegative real variable, each y_j is a nonnegative integer variable, each a_i, each b_j and c are integers, $1 \le i \le m, 1 \le j \le n$, and $\sim$ is $=, >$, or $\equiv_d$ for some integer $d > 0$. The formula is a *mixed linear constraint* if $\sim$ is $=$ or $>$. The formula is called a *dense linear constraint* if $\sim$ is $=$ or $>$ and each $b_j = 0, 1 \le j \le n$. The formula is called a *discrete linear constraint* if $\sim$ is $>$ or $=$, and each $a_i = 0, 1 \le i \le m$. The formula is called a *discrete mod constraint*, if each $a_i = 0, 1 \le i \le m$, and $\sim$ is $\equiv_d$ for some integer $d > 0$.

A formula is *definable in the additive theory of reals and integers (resp. reals, integers)* if it is the result of applying quantification ($\exists$) and Boolean operations ($\neg$ and $\wedge$) over mixed linear constraints (resp. dense linear constraints, discrete linear constraints); the formula is called a *mixed formula (resp. dense formula, Presburger formula)*. It is decidable whether a mixed formula is satisfiable (see [21] for a quantifier elimination procedure for mixed formulas).

Theorem 1. *The satisfiability of mixed formulas (and hence of dense formulas and Presburger formulas) is decidable.*

A set of nonnegative real/integer tuples is definable by a mixed formula with free variables: a tuple is in the set iff the tuple satisfies the formula. Similarly, a set of nonnegative real (resp. integer) tuples is definable by a dense (resp. Presburger) formula if a tuple is in the set iff the tuple satisfies the formula. One may have already noticed that, for the purpose of this paper, our definition of mixed/Presburger/dense formulas is on nonnegative variables.

Consider a mixed formula $R(x_1, \cdots, x_n, y_1, \cdots, y_m)$. By separating each dense variable x_i into a discrete variable $\lceil x_i \rceil$ for the integral part and a dense variable $\lfloor x_i \rfloor$ for the fractional part, $R(x_1, \cdots, x_n, y_1, \cdots, y_m)$ can always be written into the following form (after quantifier elimination), for some l: $R_1 \vee \cdots \vee R_l$, where each R_i is in the form of

$$\exists z_1, \cdots, z_n, t_1, \cdots, t_n.\ x_1 = z_1 + t_1 \wedge \cdots \wedge x_n = z_n + t_n \wedge$$

$$P(z_1, \cdots, z_n, y_1, \cdots, y_m) \wedge Q(t_1, \cdots, t_n), \tag{3}$$

where $z_1, \cdots, z_n$ are (nonnegative) discrete variables, and $t_1, \cdots, t_n$ are dense variables (defined on the interval $[0, 1)$). This representation can be easily obtained from [21]. In the representation, P is a conjunction of discrete linear constraints and discrete mod constraints and Q is a conjunction of dense linear constraints. For the given R, we define $J(N, X_1, \cdots, X_n, Y_1, \cdots, Y_m)$ if there are $x_1^i, \cdots, x_n^i, y_1^i, \cdots, y_m^i$, for all $1 \le i \le N$, such that for all $1 \le i \le N$, $R(x_1^i, \cdots, x_n^i, y_1^i, \cdots, y_m^i)$ and

$$X_1 = \sum_{1 \le i \le N} x_1^i, \cdots, X_n = \sum_{1 \le i \le N} x_n^i, Y_1 = \sum_{1 \le i \le N} y_1^i, \cdots, Y_m = \sum_{1 \le i \le N} y_m^i.$$

Notice that all the above variables are nonnegative.

Lemma 1. *$J(N, X_1, \cdots, X_n, Y_1, \cdots, Y_m)$ is definable by a mixed formula.*

Let $R_1, \cdots, R_k$ be mixed formulas over n dense variables and m discrete variables. $\mathcal{M}$ is a monotonic multicounter machine with discrete counters $y_1, \cdots, y_m$ and dense counters $x_1, \cdots, x_n$. All the counters start from 0. $\mathcal{M}$ moves from its initial state and ends with its final state. On a move from one state to another, $\mathcal{M}$ increments its counters $(x_1, \cdots, x_n, y_1, \cdots, y_m)$ by any amount $(\delta_1, \cdots, \delta_n, d_1, \cdots, d_m)$ satisfying $R_i(\delta_1, \cdots, \delta_n, d_1, \cdots, d_m)$ – here we say R_i is picked. The choice of i is given in the description of $\mathcal{M}$ and only depends on the source and destination state of the move. We define $R(X_1, \cdots, X_n, Y_1, \cdots, Y_m)$ iff $(X_1, \cdots, X_n, Y_1, \cdots, Y_m)$ are the counter values when $\mathcal{M}$ reaches the final state.

Theorem 2. *$R(X_1, \cdots, X_n, Y_1, \cdots, Y_m)$ is definable by a mixed formula.*

The following results [9] are also needed in the paper.

Theorem 3. *The binary reachability for a reversal-bounded discrete multicounter machine with a free counter is Presburger. Therefore, the same result also holds for a monotonic discrete multicounter machine and a reversal-bounded discrete multicounter machine.*

3 Decidability Results

In this section, we show a decidable characterization for various restricted versions of dense multicounter machines. The following two results can be shown using Theorem 2.

Theorem 4. *The binary reachability of a monotonic dense multicounter machine is definable by a mixed formula.*

Theorem 5. *The binary reachability of a reversal-bounded dense multicounter machine is definable by a mixed formula.*

Now, we consider a dense multicounter machine $\mathcal{M}$ with k reversal-bounded counters $x_1, \cdots, x_k$ and a free counter x_0, in which s_{init} and s_{final} are two designated states. We further assume that $\mathcal{M}$ satisfies the following conditions:

– (Cond1) On any execution sequence in $\mathcal{M}$ from s_{init} to s_{final}, the reversal bounded counters are nondecreasing (i.e., never reverse),
– (Cond2) On any execution sequence in $\mathcal{M}$ from s_{init} to s_{final}, each move will change the free counter x_0 by a fractional decrement, a fractional increment, a unit decrement, or a unit increment (i.e., the free counter can not stay),
– (Cond3) On any execution sequence in $\mathcal{M}$ from s_{init} to s_{final}, the initial and ending values of the free counter are both 0, and in between, the free counter remains positive (> 0).

We first show a binary reachability characterization of $\mathcal{M}$ under the three conditions. The proof of the result is rather complex. It uses a technique of shifting the free counter values so that the free counter behavior is simplified.

Lemma 2. *The binary reachability of reversal-bounded dense multicounter machines with a free counter, satisfying the above three conditions, is definable by a mixed formula.*

In fact, the three conditions in Lemma 2 can be completely removed, using Theorem 2 and Lemma 2.

Theorem 6. *The binary reachability of reversal-bounded dense multicounter machines with a free counter is definable by a mixed formula.*

Now we generalize $\mathcal{M}$ to have *multirate* dense counters. The counters are *multirate* if a move in $\mathcal{M}$, in addition to the mode vector $\mathbf{m}$, is further associated with a k-ary positive integer vector $\mathbf{r} = (r_1, \cdots, r_k)$. The vector $\mathbf{r}$ is called a rate vector. The move can bring counter values from $\mathbf{X}$ to $\mathbf{X}'$ whenever $R_{\mathbf{m}}(\mathbf{X}, \mathbf{X}'')$, where $\mathbf{X}''$ is defined as follows, for each $1 \le i \le k$,

$$\mathbf{X}''(x_i) = \frac{\mathbf{X}'(x_i) - \mathbf{X}(x_i)}{r_i}.$$

For instance, suppose $k = 2$ and $\mathbf{m}$ is (fractional increment, fractional decrement). Let $\mathbf{r} = (4, 5)$. Then the effect of the move is to increment x_1 by 4δ and decrement x_2 by 5δ, for some $0 < \delta < 1$.

One can show that Theorem 6 (and hence Theorem 4 and Theorem 5) still holds even when the dense counters are multirate, using the following ideas. Let $\mathcal{M}$ be a reversal-bounded dense multicounter machine with a free counter. Let $x_0, x_1, \cdots, x_k$ be all the counters in $\mathcal{M}$ (x_0 is the free counter). Suppose that the reversal-bounded counters $x_1, \cdots, x_k$ are monotonic (the technique can be easily generalized). We now construct another $\mathcal{M}'$ to simulate $\mathcal{M}$ as follows. In $\mathcal{M}'$, each x_i, $1 \le i \le k$, is replaced with many monotonic counters, namely, $y^i_{\mathbf{m}}$, for all mode vectors $\mathbf{m}$. When $\mathcal{M}$ performs an instruction with mode vector $\mathbf{m}$ and a rate vector $(r_0, r_1 \cdots, r_k)$, $\mathcal{M}'$ performs the same instruction, repeated for r_0 times, on counters $(x_0, y^1_{\mathbf{m}}, \cdots, y^k_{\mathbf{m}})$ with mode vector $\mathbf{m}$ but with rate $(1, \cdots, 1)$ (i.e., single rate instead of multirate). Let $1 \le i \le k$. What is the relationship between x_i in $\mathcal{M}$ and all the $y^i_{\mathbf{m}}$ in $\mathcal{M}'$? We use δ^i to denote the net change to counter x_i after $\mathcal{M}$ performs the instruction. We use $\delta^i_{\mathbf{m}}$ to denote the net change to counter $y^i_{\mathbf{m}}$ after $\mathcal{M}'$ performs the simulated instructions. Clearly,

$$\delta^i = \frac{r_i}{r_0} \cdot \delta^i_{\mathbf{m}}.$$

Similarly, we use Δ_i to denote the net change to counter x_i on a path of $\mathcal{M}$, and use $\Delta^i_{\mathbf{m}}$ to denote the net change to counter $y^i_{\mathbf{m}}$ on the simulated path of $\mathcal{M}'$. One can show

$$\Delta_i = \frac{r_i}{r_0} \cdot \sum_{\mathbf{m}} \Delta^i_{\mathbf{m}}.$$

Since $\mathcal{M}'$ preserves the free counter x_0, and counters in $\mathcal{M}'$ is with single rate, from Theorem 6, we can show,

Theorem 7. *The binary reachability of multirate reversal-bounded dense multicounter machines (with a free counter) is definable by a mixed formula.*

So far, we have only focused on dense multicounter machines with at most one free counter. Now consider $\mathcal{M}$ with multiple free counters. Suppose that all the counters start from 0 in $\mathcal{M}$. The *state reachability problem* for $\mathcal{M}$ is: is there an execution path in $\mathcal{M}$ from the initial state to the final state? Obviously, if $\mathcal{M}$ contains two counters, the problem is undecidable. This is because, when the two dense counters only implement discrete increments/decrements, $\mathcal{M}$ is a Minsky machine [17] (a two (discrete) counter machine). A more interesting case is when $\mathcal{M}$ contains *purely dense* free counters only; i.e., the counters do not perform any discrete increments/decrements. The following theorem states that the state reachability problem is undecidable even when $\mathcal{M}$ has only four purely dense free counters.

Theorem 8. *The state reachability problem for purely dense multicounter machines is undecidable. The undecidability remains even when there are only four purely dense free counters.*

Turning now to the case when $\mathcal{M}$ has only two purely dense free counters, we have the following decidable result. The case when there are three counters is open.

Theorem 9. *The state reachability problem for machines with only two purely dense free counters is decidable.*

4 Safety/Liveness Verification

From the binary reachability characterizations given in the previous section, one can establish decidable results on various verification problems for a reversal-bounded dense multicounter machine $\mathcal{M}$ with a free counter, even when counters in $\mathcal{M}$ are of multirate.

The *binary reachability problem* for $\mathcal{M}$ is defined as follows: Given a mixed formula $I(\mathbf{X}, \mathbf{X}')$, are there $\mathbf{X}$ and $\mathbf{X}'$ such that $I(\mathbf{X}, \mathbf{X}')$ holds and $(s_{\text{init}}, \mathbf{X})$ reaches $(s_{\text{final}}, \mathbf{X}')$ in $\mathcal{M}$? An example of the problem is as follows:

> Is there $(x_1, x_2, x_3, x_1', x_2', x_3')$ satisfying "$x_1' - 2x_1 + x_2$ *is an integer* $\wedge x_3' + x_2' > x_3 + x_2 + x_1 + 1$" and $(s_{\text{init}}, x_1, x_2, x_3)$ reaches $(s_{\text{final}}, x_1', x_2', x_3')$ in $\mathcal{M}$?

Using Theorem 1 and Theorem 6, one can show that the binary reachability problem is decidable.

Additionally, one can also consider the *mixed i.o. (infinitely often) problem* for $\mathcal{M}$ as follows. Given two mixed formulas I and P, the problem is to decide whether there is an infinite execution path of $\mathcal{M}$

$$(s^0, \mathbf{X}^0) \to (s^1, \mathbf{X}^1) \to \cdots \to (s^n, \mathbf{X}^n) \to \cdots$$

such that $s^0 = s_{\text{init}}, I(\mathbf{X}_0)$ holds, and there are infinitely $n_1 < n_2 < \cdots$ such that $P(X^{n_i})$ holds for all i. An example of the problem is as follows: Is there an infinite run of $\mathcal{M}$ such that

$$x_3 > x_2 + x_1 - 1 \wedge 2x_2 - x_1 \textit{ is an integer}$$

is satisfied for infinitely many times? The problem can be used to formalize some fairness properties along an ω execution path of a transition system (see also [11]). Because of

Theorem 6, $\mathcal{M}$ is a mixed linear system in the sense of [10]. From the main theorem in [10], one can conclude that the mixed i.o. problem is decidable.

A dense monotonic counter machine with a free counter (with multirate counters) can be used to model a dense counter system with counter instructions in the following form

$$\exists 0 < \delta < 1.\, x_0' = x_0 + r_0 \cdot t_0 \wedge x_1' = x_1 + r_1 \cdot t_1 \wedge \cdots \wedge x_k' = x_k + r_k \cdot t_k,$$

where, $r_0, \cdots, r_k$ are positive integers (rates), x_0 is the free counter, and $x_1, \cdots, x_k$ are the monotonic counters. We use the primed variables to indicate the new values. The term t_0 for the free counter x_0 is one of $0, \delta, -\delta, 1, -1$. The term t_i, $1 \leq i \leq k$, for monotonic counter x_i is one of $0, \delta, 1$. In addition, the counters can be tested against 0. Though the machine models are intended to be a fundamental tool to reason about a broader class of dense counter systems, using Theorem 6, one can also use the model to specify some interesting systems with multiple dense/discrete counters (e.g., the consumer/producer system in Section 1).

5 Discussions

It is a natural idea to transform a dense counter machine $\mathcal{M}$ into a dense counter automaton (i.e., acceptor) $\mathcal{A}$ in which a one-way input tape is provided. In contrast to a traditional word automaton, a dense word is provided on the input tape. We elaborate on this as follows. A *block* B is a pair (c, δ), where $c \in C$ is the color of the block and $0 \leq \delta \leq 1$ is called the block's *length*. There are only finitely many possible colors in C. Let $Blocks$ be the set of all blocks on colors in C and $Blocks^*$ be the free monoid generated by the infinite set $Blocks$. Hence, there exists an associative operation (called concatenation) of blocks with an identity ϵ. The Kleene closures * and $^+$ are defined as usual using concatenation. A *dense word* is an element of $Blocks^*$ and a *dense language* is a subset of $Blocks^*$. Given a dense word w as input, $\mathcal{A}$ reads the blocks in w one by one. On reading a block, $\mathcal{A}$ updates its control state and the counters in the same way as $\mathcal{M}$ does, except that $\mathcal{A}$ knows the color of the block, can distinguish whether the length of the block is 0, 1, or strictly greater than 0 and strictly less than 1. $\mathcal{A}$ can increment/decrement some of the counters by 0, 1, or the length of the block. In this way, one can similarly define dense monotonic counter automata, dense reversal-bounded counter automata, and dense reversal-bounded counter automata with a free counter.

For a dense word w, we use $\#_c(w)$ (resp. $l_c(w)$) to denote the total number (resp. length) of blocks with color c in w. We use $Parikh(w)$ to denote the tuple of counts $\#_c(w)$ and $l_c(w)$ for each $c \in C$; i.e.,

$$Parikh(w) = (\#_{c_1}(w), \cdots, \#_{c_n}(w), l_{c_1}(w), \cdots, l_{c_n}(w)).$$

For a dense language L, we use $Parikh(L)$, the Parikh map of L, to denote the set of all $Parikh(w)$ for $w \in L$. A dense language L is a *mixed semilinear* dense language if $Parikh(L)$ is definable by a mixed formula F over n integer variables and n dense variables: For all $x_1, \cdots, x_n \in \mathbf{N}$ and for all $y_1, \cdots, y_n \in \mathbf{R}$,

$$(x_1, \cdots, x_n, y_1, \cdots, y_n) \in Parikh(L)$$

iff $F(x_1, \cdots, x_n, y_1, \cdots, y_n)$ holds. The above definition of a Parikh map for a dense language can be seen as a natural extension of the concept of Parikh maps for discrete languages. Indeed, one can treat a discrete language $\mathcal{L}$ as a special dense language $L_{\mathcal{L}}$, where a symbol in C is understood as a unit block. One can easily verify that $\mathcal{L}$ is a semilinear discrete language iff $L_{\mathcal{L}}$ is a mixed semilinear dense language. So, over discrete languages, our definition of “mixed semilinearity" coincides with the traditional “semilinearity" definition.

It is straightforward to verify the following theorem, using the results in Section 3.

Theorem 10. *Dense languages accepted by dense reversal-bounded counter automata with a free counter are mixed semilinear languages. Hence, the emptiness and infiniteness problems for these automata are decidable.*

One can define a deterministic dense reversal-bounded counter automaton in the usual way, with the additional requirement that the transition the automaton makes on an input block (c, δ) with $0 < \delta < 1$ should be the same if the block is replaced by any (c, δ') with $0 < \delta' < 1$.

The following corollaries are easily verified:

Corollary 1. *Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be dense reversal-bounded counter automata.*

1. *We can effectively construct dense reversal-bounded counter automata $\mathcal{A}$ and $\mathcal{A}'$ accepting $L(\mathcal{A}_1) \cap L(\mathcal{A}_2)$ and $L(\mathcal{A}_1) \cup L(\mathcal{A}_2)$, respectively.*
2. *IF $\mathcal{A}_1$ is deterministic, we can effectively construct a deterministic dense reversal-bounded counter automaton accepting the complement of $L(\mathcal{A}_1)$.*

If one of $\mathcal{A}_1$ or $\mathcal{A}_2$ (but not both) has a free counter, then $\mathcal{A}$ and $\mathcal{A}'$ will also have a free counter. It follows that the class of languages accepted by deterministic dense reversal-bounded counter automata is closed under the boolean operations.

Corollary 2. *The emptiness, infiniteness, and disjointness problems for dense reversal-bounded counter automata are decidable. The containment and equivalence problems for deterministic dense reversal-bounded counter automata are decidable.*

Notice that the universe problem for dense reversal-bounded counter automata is undecidable, since the undecidability holds even for discrete counters [14]. Obviously, from Theorem 10, when the automata (even with a free counter) are deterministic, the universe problem is decidable.

References

1. R. Alur, C. Courcoubetis, and T. A. Henzinger. Computing accumulated delays in real-time systems. *Formal Methods in System Design: An International Journal*, 11(2):137–155, August 1997.
2. R. Alur, C. Courcoubetis, T. A. Henzinger, and P. Ho. Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems. In *Hybrid Systems*, pages 209–229, 1992.

3. R. Alur and D. L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, April 1994.
4. B. Boigelot, S. Rassart, and P. Wolper. On the expressiveness of real and integer arithmetic automata. In *ICALP'98*, volume 1443 of *LNCS* , pages 152–163. Springer, 1998.
5. B. Boigelot and P. Wolper. Symbolic verification with periodic sets. In *CAV'94*, volume 818 of *LNCS*, pages 55–67. Springer, 1994.
6. H. Comon and Y. Jurski. Multiple counters automata, safety analysis and Presburger arithmetic. In *CAV'98*, volume 1427 of *LNCS*, pages 268–279. Springer, 1998.
7. H. Comon and Y. Jurski. Timed automata and the theory of real numbers. In *CONCUR'99*, volume 1664 of *LNCS*, pages 242–257. Springer, 1999.
8. Z. Dang, O. H. Ibarra, and Z. Sun. On the emptiness problems for two-way nondeterministic finite automata with one reversal-bounded counter. In *ISAAC'02*, volume 2518 of *LNCS*, pages 103–114. Springer, 2002.
9. Zhe Dang, O. H. Ibarra, T. Bultan, R. A. Kemmerer, and J. Su. Binary reachability analysis of discrete pushdown timed automata. In *CAV'00*, volume 1855 of *LNCS*, pages 69–84. Springer, 2000.
10. Zhe Dang and Oscar H. Ibarra. On the existence of ω-chains for transitive mixed linear relations and its applications. *International Journal of Foundations of Computer Science*, 13(6):911–936, 2002.
11. Zhe Dang, P. San Pietro, and R. A. Kemmerer. On Presburger Liveness of Discrete Timed Automata. In *STACS'01*, volume 2010 of *LNCS*, pages 132–143. Springer, 2001.
12. L. Fribourg and H. Olsen. A decompositional approach for computing least fixed-points of Datalog programs with Z-counters. *Constraints*, 2(3/4):305–335, 1997.
13. T. A. Henzinger, P.-H. Ho, and H. Wong-Toi. HYTECH: A Model Checker for Hybrid Systems. In *CAV'97*, volume 1254 of *LNCS*, pages 460–463. Springer, 1997.
14. O. H. Ibarra. Reversal-bounded multicounter machines and their decision problems. *Journal of the ACM*, 25(1):116–133, January 1978.
15. O. H. Ibarra, T. Jiang, N. Tran, and H. Wang. New decidability results concerning two-way counter machines. *SIAM J. Comput.*, 24:123–137, 1995.
16. K. Larsen, G. Behrmann, Ed Brinksma, A. Fehnker, T. Hune, P. Pettersson, and J. Romijn. As cheap as possible: Efficient cost-optimal reachability for priced timed automata. In *CAV'01*, volume 2102 of *LNCS*, pages 493–505. Springer, 2001.
17. M. Minsky. Recursive unsolvability of Post's problem of Tag and other topics in the theory of Turing machines. *Ann. of Math.*, 74:437–455, 1961.
18. X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. An approach to the description and analysis of hybrid systems. In *Hybrid Systems*, pages 149–178, 1992.
19. A. Puri P. Kopke, T. Henzinger and P. Varaiya. What's decidable about hybrid automata? *27th Annual ACM Symposium on Theory of Computing (STOC)*, pages 372–382, 1995.
20. P. Z. Revesz. A closed form for datalog queries with integer order. *Proc. Intl. Conf. on Database Theory (ICDT'90), volume 470 of LNCS*, pages 187–201. Springer, 1990.
21. V. Weispfenning. Mixed real-integer linear quantifier elimination. *Proc. Intl. Symp. on Symbolic and Algebraic Computation*, pages 129–136, Vancouver, B.C., Canada, July 29-31, 1999.