Flat Parametric Counter Automata

Marius Bozga, Radu Iosif, Yassine Lakhnech

Flat Parametric Counter Automata

Marius Bozga[1], Radu Iosif[1], and Yassine Lakhnech[1]

VERIMAG, 2 Avenue de Vignate, 38610 Gières, France
bozga,iosif,lakhnech@imag.fr

Abstract. In this paper we study the reachability problem for parametric flat counter automata, in relation with the satisfiability problem of three fragments of integer arithmetic. The equivalence between non-parametric flat counter automata and Presburger arithmetic has been established previously by Comon and Jurski [5]. We simplify their proof by introducing finite state automata defined over alphabets of a special kind of graphs (zigzags). This framework allows one to express also the reachability problem for parametric automata with one control loop as the existence of solutions of a *1-parametric linear Diophantine systems*. The latter problem is shown to be decidable, using a number-theoretic argument. Finally, the general reachability problem for parametric flat counter automata with more than one loops is shown to be undecidable, by reduction from Hilbert's Tenth Problem [9].

1 Introduction

Flat counter automata [5, 6, 3, 4] have been extensively studied, as an important class of infinite-state systems, for which the reachability problem is decidable. The results obtained so far have been used in a number of successful verification tools, like FAST [2], LASH [18] or TREX [1].

Comon and Jurski show in [5] that the reachability problem for a flat counter automaton can be expressed in Presburger arithmetic, given that the automata have transition guards that are conjunctions of relations of the form $x - y \leq c$, where x and y denote either the current or the future (primed) values of the counters, and c is an integer constant. To our knowledge, their result concerns the most general class of flat counter automata, considered so far.

The contributions of the present paper are many fold. First, we give an alternative, easier, proof of the result of [5], using finite state automata defined over alphabets of graphs (zigzags). Second, we consider a more general class of flat counter automata, in which, besides integer constants, parameters are also allowed to occur in transitions. This class is useful in modeling open programs, whose behavior is parameterized by some input values, e.g. procedures in a larger program. The reachability problem in the latter class of automata amounts to checking satisfiability of *Diophantine systems* [12].

Third, we give an effective decision procedure for the following problem: given a linear system with unknowns $x_1, \ldots, x_n$, the coefficients being polynomials of any degree in m, is there a constant $c \in \mathbb{N}$, such that the system resulting from substituting m with c has a positive solution? This result gives an effective algorithm to decide reachability for parametric counter automata with one control loop, whereas in the case of more than one control loop, the reachability problem for such systems is undecidable.

1.1 Related Work

Work on the decidability of reachability problems for counter automata starts with the negative result of Minsky [14] regarding two counter machines. The two most studied restrictions of this model are the *reversal bounded* 2-way counter machines [10] and the *flat counter automata* [5, 6, 3]. The class of flat counter automata that is closest to the one considered in this paper is the one studied by Comon and Jurski [5], where the transition relations are conjunctions of inequalities of the form $x - y \leq c$, with $c \in \mathbb{Z}$. Their result is that the set of reachable configurations for such automata is definable in Presburger arithmetic. Our result considers parametric transition relations of the form $x - y \leq f(\mathbf{z})$, and defines the set of reachable configurations as solutions of a linear Diophantine system with one parameter. Decision procedures for this class of systems have been independently found by O. Ibarra and Z. Dang in [11], using a result from the theory of reversal-bounded counter automata, and by Y. Matiyasevich [13]. The latter result uses a similar number theoretic argument, but the proof is based on a more involved case analysis.

2 Preliminaries

Let $\mathbf{x} = \{x_1, \ldots, x_k\}$ be a finite set of variables (counters) ranging over $\mathbb{Z}$, and $\mathbf{x}' = \{y' \mid y \in \mathbf{x}\}$ be the corresponding set of primed variables. For any counter y, we denote by y' its value at the next computational step. In what follows we will abusively use the name of a variable to denote its value also. The (compulsory) occurrence of a set of variables $\mathbf{x}$ in a logical formula φ is denoted as $\varphi(\mathbf{x})$. By $\langle \mathbb{Z}[\mathbf{x}], +, \cdot \rangle$ we denote the ring of polynomials, and by $\langle \mathbf{lin}\mathbb{Z}[\mathbf{x}], + \rangle$ the monoid of linear polynomials, with variables $\mathbf{x}$ and integer coefficients. For a closed formula φ, we write $\models \varphi$ meaning that it is valid, i.e. equivalent to true.

Let $\mathbf{z} = \{z_1, \ldots, z_l\}$ be a set of *parameter* variables, disjoint from $\mathbf{x}$. A relation $\varphi(\mathbf{x}, \mathbf{x}', \mathbf{z})$ that can be written as a finite conjunction of the form:

$$\bigwedge x_i - x_j \leq \alpha_{ij} \wedge \bigwedge x'_m - x_n \leq \beta_{mn} \wedge \bigwedge x_p - x'_q \leq \gamma_{pq} \wedge \bigwedge x'_r - x'_s \leq \delta_{rs}$$

with $1 \leq i, j, m, n, p, q, r, s \leq k$, and $\alpha_{ij}, \beta_{mn}, \gamma_{pq}, \delta_{rs} \in \mathbf{lin}\mathbb{Z}[\mathbf{z}]$, is said to be an *affine relation*. Note the formal difference between variables ($\mathbf{x}$) and parameters ($\mathbf{z}$) in φ: variables are bound to occur both unprimed and primed, whereas parameters can only occur unprimed in formulae.

A *parametric counter automaton* is a tuple $A = \langle \mathbf{x}, \mathbf{z}, Q, \delta, q_0 \rangle$, where $\mathbf{x}$ is the set of working counters, $\mathbf{z}$ is the set of parameters, Q is the set of *control states*, $q_0 \in Q$ is the *initial state*, and δ is the set of *transitions* of the form: $q \xrightarrow{\varphi(\mathbf{x}, \mathbf{x}', \mathbf{z})} q'$, where φ is an affine relation. A *configuration* of A is a tuple $c = \langle q, \mathbf{xz} \rangle$ consisting of a control state, and a set of integer values for the counters and parameters. A *run* of the automaton is a sequence of configurations, $c_0, c_1, c_2, \ldots, c_n$, $c_i = \langle q_i, \mathbf{x_i z} \rangle$, such that $\mathbf{x_0} = \mathbf{0}$, i.e. the counters are initially set to zero, and $q_i \xrightarrow{\varphi(\mathbf{x_i}, \mathbf{x_{i+1}}, \mathbf{z})} q_{i+1}$, for all $0 \leq i < n$. Note that the values of the parameters are not modified throughout the run. A control state q is said to be *reachable* in A if and only if A has a run ending in a configuration $\langle q, \mathbf{xz} \rangle$.

A control state r is said to be the *successor* of a state q if and only if there exists configurations $\langle q, \mathbf{x}\mathbf{z}\rangle \rightarrow \langle r, \mathbf{x}'\mathbf{z}\rangle$, for some $\mathbf{x}, \mathbf{x}' \in \mathbb{Z}^k$, $\mathbf{z} \in \mathbb{Z}^l$. A *control path* is a sequence of control states $q_1, q_2, \ldots, q_n$ such that, for all $0 \leq i < n$, q_{i+1} is a successor of q_i. The path is said to be non-trivial if $n > 0$. A *cycle* is a non-trivial control path starting and ending with the same state. A counter automaton is said to be *flat* (FCA) if and only if each control state belongs to at most one cycle. A control state with two or more successors (in the sense mentioned above) is said to be a *branching* state. A branching state with exactly two successors is said to be a *2-branching* state. A FCA is said to be *linear* (LFCA) if and only if the only branching states are 2-branching, and every cycle contains at most one such state. Notice that every FCA can be effectively turned into a finite union of LFCA, the only branching state that is not 2-branching, being the initial state.

It is well-known that the class of affine relations is closed under composition, defined as $(\varphi_1 \circ \varphi_2)(\mathbf{x}, \mathbf{x}', \mathbf{z}) = \exists \mathbf{y}\ \varphi_1(\mathbf{x}, \mathbf{y}, \mathbf{z}) \ \wedge \ \varphi_2(\mathbf{y}, \mathbf{x}', \mathbf{z})$. In other words, the existential quantifiers can be eliminated[1], the result being written as another affine relation. As a consequence, we can assume without losing generality, that each control path $q_1 \xrightarrow{\varphi_1} q_2 \ldots q_{n-1} \xrightarrow{\varphi_{n-1}} q_n$, with no incoming edges, is equivalent to a transition $q_1 \xrightarrow{\varphi_1 \circ \ldots \circ \varphi_{n-1}} q_n$. By applying this transformation to the whole counter automaton, we obtain a counter automaton in *normal form*.

Given a counter automaton $A = \langle \mathbf{x}, \mathbf{z}, Q, \delta, q_0 \rangle$ and a control state $q \in Q$, the *reachability problem* asks whether q is reachable in A. As we show in the following, this problem can be defined in various subfragments of the arithmetic of integer numbers. Moreover, we can show equivalence of these logical theories with different subclasses of flat counter automata. The latter are obtained by restricting the number of parameters and loops on a control path. We denote by $\mathrm{FCA}(p, n)$ the class of flat counter automata with at most p parameters that occur in the transition relations, and with at most n cycles on each linear component.

3 The Arithmetic of Integers

The undecidability of first-order arithmetic of integers $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ occurs as a consequence of Gödel's Incompleteness Theorem [8]. Moreover, the existential fragment, i.e. *Hilbert's Tenth Problem* [9] was proved undecidable by Y. Matiyasevich [12]. On the positive side, the decidability of the arithmetic of integer numbers with *addition and successor function* $\langle \mathbb{Z}, \geq, +, 0, 1 \rangle$ has been shown by M. Presburger [17].

Let us first introduce the theories of Presburger arithmetic [17] and parametric linear Diophantine systems. Presburger arithmetic $\langle \mathbb{Z}, \geq, +, 0, 1 \rangle$ is the theory of first-order logic of addition and successor function ($S(x) = x + 1$). The interpretation of logical variables is the set of integers $\mathbb{Z}$, and the meaning of the function symbols $0, 1, +$ is the natural one.

A *Diophantine equation* is a formula of the form $P(\mathbf{x}) = 0$, where $P \in \mathbb{Z}[\mathbf{x}]$ is a polynomial of the form $P(\mathbf{x}) = \sum_{i=1}^{m} a_i t_i(\mathbf{x}) + a_0$, and t_i are multiplicative terms of the

[1] By e.g. the Fourrier-Motzkin procedure.

form $\Pi_{l=1}^{k} x_l^{i_l}$, with $i_1, \ldots, i_l \in \mathbb{N}$. The equation is said to be *linear with parameter* x_j, $1 \leq j \leq k$, if for every multiplicative term of the form above, we have $\sum_{l \in \{1 \ldots k\}}^{l \neq j} i_l \leq 1$. In other words, the only variable that can occur at a power greater than one is x_j, and moreover, all multiplicative terms contain at most one variable, other than x_j. Note that any Diophantine linear equation with parameter m can be equivalently written as:

$$\sum_{i=1}^{n} p_i(m) x_i + p_0(m) = 0 \tag{1}$$

where $p_i \in \mathbb{Z}[m]$, $0 \leq i \leq n$ are polynomials of arbitrary degree in m. In the following, we denote by $\mathfrak{D}[m]$ the set of positive boolean combinations of linear Diophantine equations with one parameter, namely m.

In this paper we show that the following problems are inter-reducible:

- the reachability for the class $\mathrm{FCA}(0,n)$ (flat counter automata without parameters with any number of loops) and satisfiability of Presburger arithmetic, and
- the reachability for the class $\mathrm{FCA}(p,1)$ (flat counter automata with any number of parameters and one loop) and satisfiability of $\mathfrak{D}[m]$.

Notice that the notion of *parameter* changes its meaning, depending on whether we are referring to counter automata, or Diophantine systems.

For the first point, it is already known that, given an arbitrary open Presburger formula $\varphi(\mathbf{x})$, one can build a flat counter automaton that generates exactly the values $\mathbf{x} \in \mathbb{Z}$ satisfying φ. This is a direct consequence of the fact that the set of such values is semilinear [7].

To complete the picture, we show the undecidability of the reachability problem for the class $\mathrm{FCA}(p,n)$ with unrestricted number of parameters (p) and loops (n), by reduction from Hilbert's Tenth Problem [9].

4 From FCA to Integer Arithmetic

In this section we develop the framework used to define the reachability problem of a FCA as a formula of either Presburger arithmetic, or $\mathfrak{D}[m]$. Given a FCA $A = \langle \mathbf{x}, \mathbf{z}, Q, \delta, q_0 \rangle$, and a state $q \in Q$, the idea is to build an arithmetic formula $\nu_{A,q}(\mathbf{x}, \mathbf{x}', \mathbf{z})$ such that, for every $\mathbf{x}, \mathbf{x}' \in \mathbb{Z}^k$, $\mathbf{z} \in \mathbb{Z}^l$, there is a run in A from $\langle q_0, \mathbf{x}\mathbf{z} \rangle$ to $\langle q, \mathbf{x}'\mathbf{z} \rangle$ if and only if $\models \nu_{A,q}(\mathbf{x}, \mathbf{x}', \mathbf{z})$. The reachability problem for A and q reduces then to checking the validity of the formula $\exists \mathbf{x} \exists \mathbf{z} \,.\, \nu_{A,q}(\mathbf{0}, \mathbf{x}, \mathbf{z})$.

In order to define $\nu_{A,q}$, we first observe that each $A \in \mathrm{FCA}(p,n)$ is a union of disjoint linear flat counter automata, each being composed of a sequence of cycles, connected by non-trivial control paths. Without loss of generality, we will assume that A is in normal form, i.e. each control path with no incoming edges and no branching has been reduced to one transition, by composing the transition relations along the way. It follows that $\nu_{A,q}(\mathbf{x}, \mathbf{x}', \mathbf{z})$ is of the following form:

$$\exists \mathbf{y_{1 \ldots n}} \exists \mathbf{y'_{1 \ldots n}} \bigvee_i \eta_{i1}(\mathbf{x}, \mathbf{y_1}, \mathbf{z}) \wedge \bigwedge_{1 \leq j < m_i} \left[\xi_{ij}(\mathbf{y_j}, \mathbf{y'_j}, \mathbf{z}) \wedge \eta_{ij}(\mathbf{y'_j}, \mathbf{y_{j+1}}, \mathbf{z}) \right] \wedge \mathbf{x}' = \mathbf{y_{m_i}}$$

where $m_i \leq n$, η_{ij} are the affine relations corresponding to the transitions between cycles, and ξ_{ij} represent the transitive closures of the cycle relations, in the following sense: if $q \xrightarrow{\varphi(\mathbf{x},\mathbf{x}',\mathbf{z})} q$ is a cycle, then the transitive closure of φ is the relation between the input and output values of the counters, after *any* number of iterations through the cycle. Since η_{ij} are affine relations, it follows that $\nu_{A,q}$ is a formula in the language of $\langle \mathbb{Z}, \geq, +, 0, 1 \rangle$, if ξ_{ij} belong to the same language. Moreover, for $m_i = 1$, $\nu_{A,q}$ is a formula of $\mathfrak{D}[m]$ if ξ_{ij} are. It is therefore sufficient to analyze the definability of $\nu_{A,q}$ when A has only one transition of the form $q \xrightarrow{\varphi(\mathbf{x},\mathbf{x}',\mathbf{z})} q$. In the following developments, we will silently assume that this is indeed the case.

4.1 Constraint Graph Execution Model

In general, an affine relation $\varphi(\mathbf{x},\mathbf{x}',\mathbf{z})$ can be represented as a directed weighted graph whose set of vertices is the set of variables $\mathbf{x} \cup \mathbf{x}'$, and there is an edge with weight α from x to y if and only if there is an explicit constraint $x - y \leq \alpha$ in φ, where $\alpha \in \mathbf{lin}\mathbb{Z}[\mathbf{z}]$. An n-step execution of $q \xrightarrow{\varphi(\mathbf{x},\mathbf{x}',\mathbf{z})} q$ is represented by a *constraint graph* G^n_φ, defined as the minimal graph whose set of vertices is $\bigcup_{i=0}^{n} \mathbf{x}^i$, where $\mathbf{x}^i = \{y^i \mid y \in \mathbf{x}\}$ and, for all $0 \leq i < n$, there is an edge labeled α:

- from x^i to y^i, if there is a constraint $x - y \leq \alpha$ in φ.
- from x^{i+1} to y^{i+1}, if there is a constraint $x' - y' \leq \alpha$ in φ.
- from x^i to y^{i+1}, if there is a constraint $x - y' \leq \alpha$ in φ.
- from x^{i+1} to y^i, if there is a constraint $x' - y \leq \alpha$ in φ.

For example, Figure 1 shows the constraint graph for the transition relation $\varphi : x_1 - x'_2 \leq z_1 \wedge x'_2 - x_3 \leq z_2 \wedge x_3 - x'_1 \leq z_3 \wedge x_1 - x'_3 \leq z_4$. Intuitively, the nodes $\mathbf{x}^i$ in the execution graph represent the possible values of the counters after i steps of execution. Define $G^\infty_\varphi = \bigcup_{n>0} G^n_\varphi$. We say that a path in G^∞_φ *stretches between n and m*, for some $n \leq m$, if the path contains at least one node from $\mathbf{x}^i$, for each $n \leq i \leq m$.

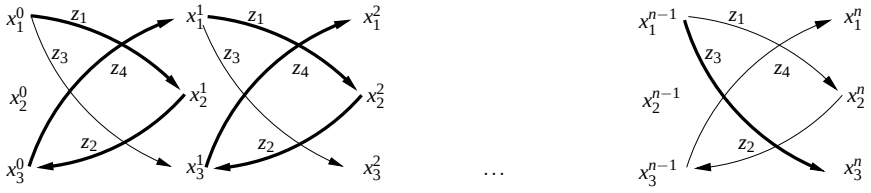

Fig. 1. Constraint Graph for $x_1 - x'_2 \leq z_1 \wedge x'_2 - x_3 \leq z_2 \wedge x_3 - x'_1 \leq z_3 \wedge x_1 - x'_3 \leq z_4$

If $\pi : x^i \xrightarrow{\alpha_1} \ldots \xrightarrow{\alpha_m} y^j$, $0 \leq i, j, \leq n$ is a path in G^n_φ, let $\omega(\pi)$ denote the sum of all labels along the path, i.e. $\omega(\pi) = \sum_{k=1}^{m} \alpha_k$. Notice that $\omega(\pi) \in \mathbf{lin}\mathbb{Z}[\mathbf{z}]$, for any constant $m \in \mathbb{N}$. Clearly, we have $x^i - y^j \leq \omega(\pi)$. We define $\min\{x^i \to y^j\} = \min\{\omega(\pi) \mid \pi :$

$x^i \xrightarrow{\alpha_1} \ldots \xrightarrow{\alpha_m} y^j\}$. By convention, if there are no paths in G^n_φ, between x^i and y^j, we take $\min\{x^i \to y^j\} = \infty$. On the other hand, if the set of paths between x^i and x^j doesn't have a minimal element, we take $\min\{x^i \to y^j\} = -\infty$. Notice that this can only be the case if G^n_φ has a cycle labeled only with constants, whose sum is less than zero. With the latter notation, we have $x^i - y^j \leq \min\{x^i \to y^j\}$. Moreover, this is the strongest relation involving the values of x and y at the execution times i and j, respectively. Notice that the satisfiability of any constraint between x^i and y^j entails the absence of negative cycles from G^n_φ. The relation between the input and output values of the counters, after n steps is:

$$\bigwedge_{x,y\in\mathbf{x}} x - y \leq \min\{x^0 \to y^0\} \wedge x' - y' \leq \min\{x^n \to y^n\} \wedge$$
$$x - y' \leq \min\{x^0 \to y^n\} \wedge x' - y \leq \min\{x^n \to y^0\} \quad (2)$$

The next step is to define the functions $\min\{x^i \to y^j\}$, $i, j \in \{0, n\}$ using the arithmetic of integers. These functions are definable in $\langle \mathbb{Z}, \geq, +, 0, 1\rangle$, if φ has no parameters, and in $\mathfrak{D}[m]$, otherwise. The reduction method, based on weighted finite automata, is the same in both cases, and will be presented in the rest of this section.

4.2 The Even and Odd Automata

In the following, we work with a simplified (yet equivalent) form of the transition relation $\varphi(\mathbf{x}, \mathbf{x}', \mathbf{z})$. Namely, all constraints of the form $x - y \leq \alpha$ are replaced by $x - t' \leq \alpha \wedge t' - y \leq 0$, and all constraints of the form $x' - y' \leq \alpha$ are replaced by $x' - t \leq \alpha \wedge t - y' \leq 0$, by introducing fresh variables $t \notin \mathbf{x}$. In other words, we can assume without loss of generality that the constraint graph corresponding to φ is *bipartite*, i.e. it does only contain edges from $\mathbf{x}$ and $\mathbf{x}'$ and viceversa.

As previously mentioned, the presence of any cycle of negative weight within G^n_φ indicates that the constraints represented by G^n_φ are not satisfiable, i.e. the automaton has no run of length n or greater. On the other hand, a path that has a cycle of positive weight is not minimal, as one can obtain a path of smaller weight by eliminating the cycle. So, in principle, we need one tool for recognizing cycles of negative weight, and another one for recognizing acyclic paths within G^∞_φ. Both tools will be finite state automata with weighted transitions, defined on two different alphabets.

Intuitively, a word w of length n represents a path π between, say, x^0 and x^n, with $x, y \in \mathbf{x}$, as follows: the w_i symbol represents *simultaneously* all edges of π that involve only nodes from $\mathbf{x}^i \cup \mathbf{x}^{i+1}$, $0 \leq i < m$. Note that, for a path from x^0 to y^n, coded by a word w, the number of times the w_i symbol is traversed by the path is odd, whereas for a path from x^0 to y^0, or from x^n to y^n, this number is even. Hence the names of *even* and *odd automata*.

Given an affine relation $\varphi(\mathbf{x}, \mathbf{x}', \mathbf{z})$, the *even alphabet* of φ, denoted as Σ^e_φ, is the set of all graphs satisfying the following conditions, for each $G \in \Sigma^e_\varphi$:

1. the set of nodes of G is $\mathbf{x} \cup \mathbf{x}'$,

2. for any $x, y \in \mathbf{x} \cup \mathbf{x}'$, there is an edge with label α from x to y, only if the constraint $x - y \leq \alpha$ occurs in φ.
3. the in-degree and out-degree of each node are at most one.
4. the number of edges from $\mathbf{x}$ to $\mathbf{x}'$ equals the number of edges from $\mathbf{x}'$ to $\mathbf{x}$.

The *odd alphabet* of φ, denoted by Σ^o_φ, is defined in the same way, with the exception of the last condition:

4. the difference between the number of edges from $\mathbf{x}$ to $\mathbf{x}'$ and the number of edges from $\mathbf{x}'$ to $\mathbf{x}$ is either 1 or -1.

Let $\Sigma^{e,o}_\varphi = \Sigma^e_\varphi \cup \Sigma^o_\varphi$. Since, by the previous assumption, no $G \in \Sigma^{e,o}_\varphi$ contains edges of the form $x \xrightarrow{\alpha} y$ or $x' \xrightarrow{\alpha} y'$, the number of edges in all symbols of Σ^e_φ is even, while the number of edges in all symbols of Σ^o_φ is odd. The label of G, is the sum of the weights that occur on its edges. Clearly the weight of a path through G^∞_φ is the weight of the word it is represented by. We denote by $\omega(w)$ the weight of a word $w \in \Sigma^{e,o*}_\varphi$. Notice that $\omega(w) \in \mathbf{lin}\mathbb{Z}[\mathbf{z}]$, for any given $w \in \Sigma^{e,o*}_\varphi$, where $\mathbf{z}$ is the set of parameters of φ.

Given the set of counters $\mathbf{x} = \{x_1, \ldots, x_k\}$, the even and odd automata share the same transition table, except for the alphabet, which is Σ^e_φ for the former, and Σ^o_φ for the latter. Precisely, we have $A^{e,o}_\varphi = \langle Q, \delta \rangle$, where $Q = \{l, r, lr, rl, \perp\}^k$, and $\mathbf{q} \xrightarrow{G} \mathbf{q}'$ if the following conditions hold, for all $1 \leq i \leq k$:

- $q_i = l$ iff G has one edge whose destination is x_i, and no other edge involving x_i.
- $q'_i = l$ iff G has one edge whose source is x'_i, and no other edge involving x_i.
- $q_i = r$ iff G has one edge whose source is x_i, and no other edge involving x_i.
- $q'_i = r$ iff G has one edge whose destination is x'_i, and no other edge involving x_i.
- $q_i = lr$ iff G has exactly two edges involving x_i, one having x_i as source, and another as destination.
- $q'_i = rl$ iff G has exactly two edges involving x'_i, one having x'_i as source, and another as destination.
- $q'_i \in \{lr, \perp\}$ iff G has no edge involving x'_i.
- $q_i \in \{rl, \perp\}$ iff G has no edge involving x_i.
- G has at least one edge between $\mathbf{x}$ and $\mathbf{x}'$.

The odd automaton for $\varphi = x_1 - x'_2 \leq z_1 \wedge x'_2 - x_3 \leq z_2 \wedge x_3 - x'_1 \leq z_3 \wedge x_1 - x'_3 \leq z_4$ is depicted in Figure 2 (a). An example of a run of this automaton is given in Figure 2 (b). Intuitively, $q_{ij} = l$ means that the node x^i_j of G^∞_φ is traversed from right to left by a path, and no other path comes across this node. Also, $q_{ij} = lr$ means that there is a path coming into x^i_j from $\mathbf{x}^{i+1}$ (left), and leaving also towards $\mathbf{x}^{i+1}$ (right), while no other path comes across this node. The transitions of $A^{e,o}_\varphi$ capture the necessary (yet not sufficient) conditions for a word in $\Sigma^{e,o*}_\varphi$ to represent a path in G^∞_φ. Suppose that $A^{e,o}_\varphi$ has a run $\pi : \mathbf{q}_1 \xrightarrow{G_1} \mathbf{q}_2 \xrightarrow{G_2} \ldots \mathbf{q}_{n-1} \xrightarrow{G_{n-1}} \mathbf{q}_n$. By $G(\pi)$ we shall denote, in the following, the graph associated with the run, i.e. the graph whose nodes are q_{ij}, and there is an edge from q_{ij} to q_{i+1h} if and only if $\mathbf{q}_i \xrightarrow{G_i} \mathbf{q}_{i+1}$ and G_i has an edge from x_j to x'_h, for all $1 \leq i \leq n$, $1 \leq j, h \leq k$. The edges from q_{i+1h} to q_{ij} are defined symmetrically. Each

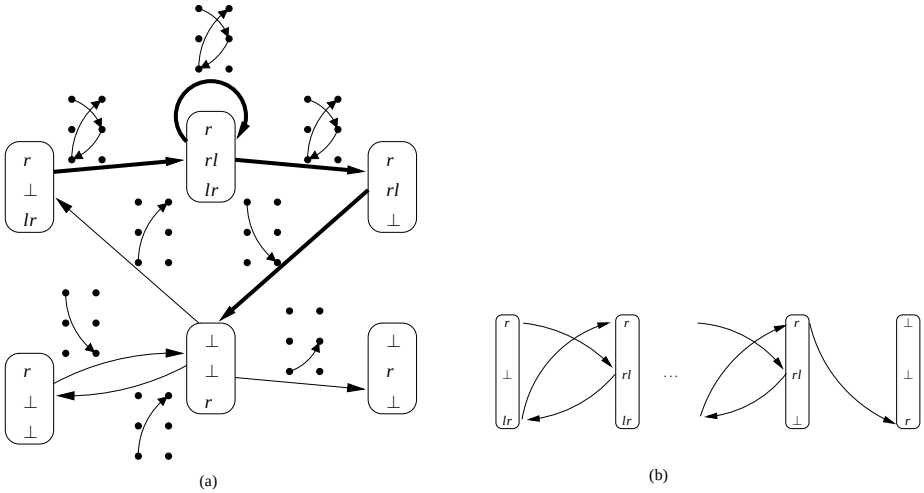

Fig. 2. The Odd Automaton for $x_1 - x'_2 \leq z_1 \wedge x'_2 - x_3 \leq z_2 \wedge x_3 - x'_1 \leq z_3 \wedge x_1 - x'_3 \leq z_4$

node in $G(\pi)$ is labeled by a symbol from $\{l, r, lr, rl, \perp\}$, and we write, e.g. $q_{ij} = l$, meaning that q_{ij} is labeled with l. We denote by $\omega(\pi)$ the weight of the run π, defined as $\omega(\pi) = \omega(G(\pi))$.

Lemma 1. *Let $\pi : \mathbf{q}_1 \xrightarrow{G_1} \mathbf{q}_2 \xrightarrow{G_2} \ldots \mathbf{q}_{n-1} \xrightarrow{G_{n-1}} \mathbf{q}_n$ be a run of $A^{e,o}_{\varphi}$. Then each node q_{ij}, $1 \leq i \leq n$, $1 \leq j \leq k$, from $G(\pi)$, has at most one predecessor and at most one successor.*

For some $1 \leq i, j \leq k$, let $A^e_{ij} = \langle A^{e,o}_{\varphi}, Q_0, F \rangle$ be the (non-deterministic) *even automaton*, defined over Σ^e_{φ}, where:

$$Q_0 = \begin{cases} \{q \mid q_i = r,\ q_j = l \text{ and } q_h \in \{lr, \perp\},\ 1 \leq h \leq k,\ h \notin \{i, j\}\} & \text{if } i \neq j \\ \{q \mid q_i = q_j = lr \text{ and } q_h \in \{lr, \perp\},\ 1 \leq h \leq k,\ h \neq i\} & \text{otherwise} \end{cases}$$

is the set of initial states, and $F = \{rl, \perp\}^k$. In the case when $i = j$, we denote A^e_{ij} by A^e_i.

Lemma 2. *For any $1 \leq i, j \leq k$, $i \neq j$, A^e_{ij} has an accepting run of length at most m if and only if there exists a path in G^{∞}_{φ}, from x^0_i to x^0_j, that stretches between 0 and some $n \leq m$. Moreover, if G^{∞}_{φ} does not have cycles of negative weight, the minimal weight among all paths from x^0_i to x^0_j, stretching from 0 to some $n \leq m$, equals the minimal weight among all accepting runs of length at most m.*

Lemma 3. *For any $1 \leq i \leq k$, A^e_i has an accepting run of negative weight if and only if there exists a cycle of negative weight in G^{∞}_{φ}.*

For some $1 \leq i, j \leq k$, let $A^o_{ij} = \langle A^{e,o}_{\varphi}, Q_0, F \rangle$ be the (non-deterministic) *odd automaton*, defined over Σ^o_{φ}, where:

$$Q_0 = \{q \mid q_i = r \text{ and } q_h \in \{lr, \perp\},\ 1 \leq h \leq k,\ h \neq i\}$$
$$F = \{q \mid q_j = r \text{ and } q_h \in \{rl, \perp\},\ 1 \leq h \leq k,\ h \neq j\}$$

An example of an odd automaton is given in Figure 2 (a). For $i = 1$ the initial states are $\langle r, \bot, lr \rangle$ and $\langle r, \bot, \bot \rangle$. For $j = 3$ the final state is $\langle \bot, \bot, r \rangle$. An accepting run of A^o_{13} is shown in Figure 2 (b).

Lemma 4. *For any $1 \leq i, j \leq k$, A^o_{ij} has an accepting run of length m if and only if there exists a path in G^∞_φ, from x^0_i to x^m_j. Moreover, if G^∞_φ does not have cycles of negative weight, then the minimal weight among all paths from x^0_i to x^m_j equals the minimal weight among all accepting runs of length m.*

4.3 Defining Minimal Accepting Runs

Given a finite automaton with linear weights on transitions, we consider the problem of defining the set of accepting runs of a given length and of minimal weight. This solves the previous problem of defining the functions $\min\{x^i \longrightarrow y^j\}$, in order to compute the input-output relation for an FCA.

Let $A = \langle Q, q_0, \delta, F \rangle$ be a given finite automaton, and $\omega : Q \times Q \longrightarrow \mathbf{lin}\mathbb{Z}[\mathbf{z}]$ be a weight function associating each transition $q \rightarrow r$ a linear expression $\omega(q,r) \in \mathbf{lin}\mathbb{Z}[\mathbf{z}]$. If δ has no transition $q \rightarrow r$, we take $\omega(q,r) = 0$. Now associate with any pair of states $q, r \in Q$ a variable x_{qr} and take $\mathbf{x}$ to be the set $\{x_{qr} \mid q, r \in Q\}$. Intuitively, x_{qr} is the number of times the transition $q \rightarrow r$ occurs within a run. Hence we take as an implicit condition the fact that all such x_{qr} range over positive integers. The formula characterizing an accepting run of length l and weight w is:

$$\phi_A(l,w) \stackrel{\Delta}{=} \exists \mathbf{x} \bigvee_{q_f \in \mathcal{F}} \varphi_{q_f}(\mathbf{x}) \wedge \sum_{q,r \in Q} x_{qr} = l \wedge \sum_{q,r \in Q} x_{qr}\omega(q,r) = w \qquad (3)$$

where $\varphi_{q_f}(\mathbf{x})$ expresses the necessary and sufficient conditions in order for $\mathbf{x}$ to correspond to a valid run of A ending with q_f. The definition of φ_{q_f} in Presburger arithmetic follows a method described in [5], which is based on the fact that the set of states Q of A is finite.

Notice that, if A does not have parameters, ϕ_A is already a formula in the language of $\langle \mathbb{Z}, \geq, +, 0, 1 \rangle$, hence we can already define the minimal weight m among all runs of length n by the following formula: $\phi_A(n,m) \wedge \forall z\, [z \leq m \rightarrow \neg\phi_A(n,z)]$. However, this is not the case when A has parameters, due to the multiplicative terms of the form $x_{qr}\omega(q,r)$ that occur within ϕ_A. However, it is possible to build from ϕ_A, a formula of $\mathfrak{D}[m]$ defining minimal runs.

Lemma 5. *Given a finite automaton $A = \langle Q, q_0, \delta, F \rangle$, and a weight function $\omega : Q \times Q \longrightarrow \mathbf{lin}\mathbb{Z}[\mathbf{z}]$ associating each transition a linear expression, it is possible build a formula $\psi_A(l,w,\mathbf{z}) \in \mathfrak{D}[m]$ such that, for any values $l \in \mathbb{N}$ and $w, \mathbf{z} \in \mathbb{Z}$, $\models \psi_A$ if and only if w is the weight of the minimal among all accepting runs of length l.*

Intuitively, the parameter m occurring in the formula $\psi_A \in \mathfrak{D}[m]$ above, represents the number of iterations of one control loop in the original parametric FCA. It is thus possible to define the reachability problem for single loop automata in $\mathfrak{D}[m]$. As we

show in Section 5, the problem concerning the existence of solutions for such systems is decidable, hence the decidability of the reachability problem for the class of FCA$(p,1)$.

However, for an arbitrary number of loops, one can reduce Hilbert's Tenth Problem to the reachability problem. In the light of [12] The following Lemma entails undecidability of the reachability problem for parametric FCA with unrestricted number of loops.

Lemma 6. *Given a Diophantine system $S(\mathbf{x})$, it is possible to build a parametric FCA $A = \langle \mathbf{y}, \mathbf{z}, Q, \delta, q_0 \rangle$ such that $\mathbf{x} \subseteq \mathbf{z}$, such that, for some control state $q \in Q$, and for all $\mathbf{x} \in \mathbb{Z}$, we have $\models S(\mathbf{x})$ if and only if there exists a run of A $\langle q_0, \mathbf{0z} \rangle \rightarrow \ldots \rightarrow \langle q, \mathbf{yz} \rangle$*

5 Solving Parametric Linear Diophantine Systems

In this section we give a proof for the decidability of the class of formulae $\mathfrak{D}[m]$. For a given system, let D denote the maximum degree of all equations, and V is the number of variables in the system. It is known that Diophantine systems become undecidable for $(D \geq 4 \wedge V \geq 2) \vee (D \geq 2 \wedge V \geq 9)$ [15]. For either $D = 1$ or $V = 1$ the systems are decidable. We are unaware of any previously published decidability results for the case $2 \leq D < 4 \wedge 2 \leq V < 9$. The problem considered here has been independently solved by O. Ibarra and Z. Dang in [11], using a property of reversal bounded counter machines. Another proof has been suggested to us by Y. Matiyasevich [13], using a more involved case analysis. Our proof is more concise, due to a result of L. Pottier [16].

Let us fix a linear Diophantine system with parameter m, i.e. a system of the form $\{\sum_{j=1}^{n} p_{ij}(m)x_j + q_i(m) = 0\}_{i=1}^{r}$, with $p_{ij}, q_i \in \mathbb{Z}[m]$. We are interested in the existence of a solution $m, x_1, \ldots, x_n$ in natural numbers, although this is not a restriction.[2] We denote by $A(m)$ the matrix $[p_{ij}(m)]$.

Let us consider first that the system is homogeneous, i.e. $q_i(m)$ is the zero polynomial, for all $1 \leq i \leq n$. The general case will be dealt with in the following, by adding a new variable x_{n+1}, replacing each occurrence of $q_i(m)$ by $q_i(m)x_{n+1}$, and looking only after solutions in which $x_{n+1} = 1$. Let $P(m)$ be the greatest common divisor of all $p_{ij}(m)$ with respect to (symbolic) polynomial division, i.e. obtained by applying Euclid's algorithm in $\mathbb{Z}[m]$. Since $P(m)$ is a polynomial in one variable, its set of roots is finite and effectively computable. If $P(m_0) = 0$ for some $m_0 \in \mathbb{Z}$, then $\langle m_0, x_1, \ldots, x_n \rangle$ is a solution of the system $A(m)\mathbf{x} = 0$, for any choice of $x_1, \ldots, x_n \in \mathbb{Z}$. Thus, we assume in the following that $P(m) \neq 0$, for all $m \in \mathbb{N}$, in other words that, for no value of m, $p_{ij}(m)$ will all become zero at the same time.

Next, we are interested in the minimal solutions of the system. For a given $m \in \mathbb{N}$, a solution $(x_1, \ldots, x_n)$ is said to be *minimal* if it is a least solution with respect to the pointwise ordering on $\mathbb{N}^n$: $(u_1, \ldots, u_n) \preceq (v_1, \ldots, v_n) \iff u_i \leq v_i$, $1 \leq i \leq n$. The following Theorem has been proved in [16]:

Theorem 1. *For a fixed $m_0 \in \mathbb{N}$, let $x_1, \ldots, x_n$ be any minimal solution of $A(m_0)\mathbf{x} = \mathbf{0}$. Then, for all $1 \leq i \leq n$, we have: $x_i \leq (n - r_0)\left(\frac{\sum_{i,j} a_{ij}(m_0)}{r_0}\right)^{r_0}$, where r_0 is the rank of $A(m_0)$.*

[2] The satisfiability problem for integers can be reduced to 2^{n+1} instances of the same problem on natural numbers, by performing a case split on the signs of $m, x_1, \ldots, x_n$.

Let $C > 0$ be the maximal absolute value of all coefficients of $a_{ij}(m)$, $1 \leq i \leq r$, $1 \leq j \leq n$, and $K \geq 0$ be the maximum degree of these polynomials. The following is a direct consequence of Theorem 1:

Corollary 1. *For a fixed $m_0 \geq \max(C,n,r)$, let $x_1,\ldots,x_n$ be any minimal solution of $A(m_0)\mathbf{x} = \mathbf{0}$. Then, for all $1 \leq i \leq n$, we have $x_i \leq m_0^{(K+3)r+1}$.*

Hence, one can enumerate all $0 \leq m < \max(C,n,r)$, and stop as soon as a solution of the linear Diophantine system $A(m)\mathbf{x} = \mathbf{0}$ has been found. Otherwise, for any $m \geq \max(C,n,r)$ the solution $x_1,\ldots,x_n$ can be represented in base m using at most $M = (K+3)r+1$ digits. Let $(x_i)_m = \sum_{j=0}^{M} \chi_{ij} m^j$, with $0 \leq \chi_{ij} < m$ be the polynomial representing x_i in base m. The entire system $A(m)\mathbf{x} = \mathbf{0}$ can be now represented in base m, as will be explained in the following.

First, we write the system as a set of equations of the form $P(m,x_1,\ldots,x_n) = Q(m,x_1,\ldots,x_n)$, with all coefficients of P and Q being positive. Since m was assumed to be greater that C, the maximal value of all coefficients c of the system, we have $(c)_m = c$. The operations of addition, multiplication by a constant $0 < c < m$, and multiplication by m, respectively, can be defined now using Presburger arithmetic. Let $(d)_m = \sum_{i=0}^{M} \delta_i m^i$, $(e)_m = \sum_{i=0}^{M} \varepsilon_i m^i$ and $(f)_m = \sum_{i=0}^{M} \phi_i m^i$, with $0 \leq \delta_i, \varepsilon_i, \phi_i < m$. We have:

$$(f)_m = (d)_m + (e)_m \iff \bigvee_{\mathbf{r} \in \{0\}\times\{0,1\}^{k-1}\times\{0\}} \bigwedge_{i=0}^{M} \delta_i + \varepsilon_i + r_i = \phi_i + m r_{i+1}$$

$$(e)_m = c(d)_m \iff \bigvee_{\mathbf{r} \in \{0\}\times\{0,\ldots,c-1\}^{k-1}\times\{0\}} \bigwedge_{i=0}^{M} c\delta_i + r_i = \varepsilon_i + m r_{i+1}$$

$$(e)_m = m(d)_m \iff \delta_M = \phi_0 = 0 \wedge \bigwedge_{i=0}^{M-1} \delta_i = \phi_{i+1}$$

The result of applying this transformation to the system $A(m)\mathbf{x} = \mathbf{0}$ is a formula $\Psi_A(m,\chi)$ in Presburger arithmetic, defining all minimal solutions of the original system $(x_i)_m = \sum_{j=0}^{M} \chi_{ij} m^j$, for $m \geq \max(C,n,r)$, with $\chi = \{\chi_{ij} \mid 1 \leq i \leq n,\ 1 \leq j \leq r\}$. The original system has a solution $(m,x_1,\ldots,x_n)$ if and only if, for some $m \in \mathbb{N}$, it has a minimal solution $(x_1^m,\ldots,x_n^m)$. Hence $\Psi_A(m,\chi)$ is satisfiable. Dually, if $\Psi_A(m,\chi)$ is satisfiable, we can construct a solution (not necessarily minimal) of $A(m)\mathbf{x} = \mathbf{0}$.

The non-homogeneous case is handled in the proof of the following:

Theorem 2. *The satisfiability problem for linear parametric Diophantine systems $\mathfrak{D}[m]$ is decidable.*

Theorem 2, together with the results of the previous section entail the main result:

Corollary 2. *The reachability problem for single loop parametric flat counter automata $FCA(p,1)$ is decidable.*

The strength of this result is highlighted by Lemma 6, which entails the undecidability of the reachability problem for $\mathrm{FCA}(p,n)$ with $p > 0$ parameters, and sufficiently many control loops.

6 Conclusions

We have studied a generalization of the flat counter automata considered by Comon and Jurski in [5], obtained by adding parameters to the transition relations. We reduce the reachability problem for these automata to either Presburger arithmetic, in the non-parametric case, and to linear Diophantine systems with one parameter, for single-loop automata with multiple parameters. The existence of solutions for the latter class of systems is shown to be decidable. This entails the decidability of the reachability problem for counter automata with parameters and one control loop, while in general, this problem is undecidable for flat automata with more than one control loop.

Acknowledgements: The authors wish to thank Yuri Matiyasevich and Oscar Ibarra for their enlightening suggestions leading to the proof of Theorem 2.

References

1. A. Annichini, A. Bouajjani, and M.Sighireanu. Trex: A tool for reachability analysis of complex systems. In *Proc.CAV*, volume 2102 of *LNCS*, pages 368 – 372. Springer, 2001.
2. S. Bardin, A. Finkel, J. Leroux, and L. Petrucci. Fast: Fast accelereation of symbolic transition systems. In *Proc. TACAS*, volume 2725 of *LNCS*. Springer, 2004.
3. B. Boigelot. On iterating linear transformations over recognizable sets of integers. *TCS*, 309(2):413–468, 2003.
4. H. Comon and V. Cortier. Flatness is not a weakness. In *Proc. CSL*, volume 1862 of *LNCS*, pages 262 – 276. Springer, 2000.
5. H. Comon and Y. Jurski. Multiple Counters Automata, Safety Analysis and Presburger Arithmetic. In *Proc. CAV*, volume 1427 of *LNCS*, pages 268 – 279. Springer, 1998.
6. A. Finkel and J. Leroux. How to compose presburger-accelerations: Applications to broadcast protocols. In *Proc. FST&TCS*, volume 2556 of *LNCS*, pages 145–156. Springer, 2002.
7. S. Ginsburg and E. H. Spanier. Semigroups, presburger formulas and languages. *Pacific Journal of Mathematics*, 16(2):285–296, 1966.
8. K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38:173 – 198, 1931.
9. D. Hilbert. Mathematische probleme. Vortrag, gehalten auf dem internationalen Mathematiker-Kongress zu Paris. In *Nachrichten von der Königliche Gesellschaft der Wissenschaften zu Göttingen*, pages 253–297, 1900.
10. O. H. Ibarra. Reversal-bounded multicounter machines and their decision problems. *Journal of the Association for Computing Machinery*, 25(1):116 – 133, January 1978.
11. O. H. Ibarra and Z. Dang. On the solvability of a class of diophantine equations and applications. Submitted, 2005.
12. Y. Matiyasevich. Enumerable sets are diophantine. *Journal of Sovietic Mathematics*, 11:354 – 358, 1970.
13. Y. Matiyasevich. Personal communication, 2005.
14. M. Minsky. *Computation: Finite and Infinite Machines*. Prentice-Hall, 1967.
15. T. Pheidas and K. Zahidi. Undecidability of existential theories of rings and fields: A survey. *Contemporary Mathematics*, 270:49–106, 2000.
16. L. Pottier. Solutions minimales des systemes diophantiens lineaires: bornes et algorithmes. Technical Report 1292, INRIA Sophia Antipolis, 1990.
17. M. Presburger. Über die Vollstandigkeit eines gewissen Systems der Arithmetik. *Comptes rendus du I Congrés des Pays Slaves*, Warsaw 1929.
18. P. Wolper and B. Boigelot. Verifying systems with infinite but regular state spaces. In *Proc. CAV*, volume 1427 of *LNCS*, pages 88–97. Springer, 1998.