Unité Mixte de Recherche 5104 CNRS - INPG - UJF
Centre Equation
2, avenue de VIGNATE
F-38610 GIERES
tel : +33 456 52 03 40
fax : +33 456 52 03 50
http://www-verimag.imag.fr

Flat Parametric Counter Automata

Marius Bozga, Radu Iosif and Yassine Lakhnech

Report n^o TR-2005-15

March 21, 2006

Flat Parametric Counter Automata

Marius Bozga, Radu Iosif and Yassine Lakhnech

March 21, 2006

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].

Keywords: counter automata, diophantine systems

Reviewers:

Notes:

How to cite this report:

@techreport { ,
title = { Flat Parametric Counter Automata},
authors = { Marius Bozga, Radu Iosif and Yassine Lakhnech},
institution = { Verimag Technical Report },
number = {TR-2005-15},
year = { },
note = { }
}

1 Introduction

Flat counter automata [5], [6], [3] 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 [23] 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 applied this framework to a more general class of flat counter automata, in which, besides integer constants, parameters are also allowed to occur in transitions. The reachability problem in the latter case amounts to checking satisfiability of *Diophantine systems* [16].

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.

Last, we study the relation between flat counter automata and another important class of computational devices, the 2-way reversal bounded counter machines [13]. Interesting enough, by distinguishing between deterministic and non-deterministic, 1 counter reversals and k counter reversals, we can mimic the hierarchy of flat counter automata, using 2-way counter machines this time, in strong (dual) relation with the same arithmetic theories used in the study of flat counter automata: Presburger arithmetic, existential theory of addition and divisibility, and parametric Diophantine systems.

1.1 Related Work

Work on the decidability of reachability problems for counter automata starts with the negative result of Minsky [18] regarding two counter machines. The two most studied restrictions of this model are the *reversal bounded* 2-way counter machines [13] 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 [10], using a result from the theory of reversal-bounded counter automata, and by Y. Matyiasevich [17]. 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 $\mathbf{x}' = \{y' \mid y \in \mathbf{x}\}$. In what follows we will abusively use the name of a variable to denote its value also. For any $y \in \mathbf{x}$, let

$\zeta(y) = 1$ if $y \neq 0$ and $\zeta(y) = 0$ if $y = 0$. $\zeta(\mathbf{x})$ denotes the tuple $\langle \zeta(x_1), \ldots, \zeta(x_k) \rangle$, for a chosen order of the elements in $\mathbf{x}$. Let Σ be a finite alphabet, i.e. a set of symbols. A *2-way counter machine* over Σ is a tuple $M = \langle \mathbf{x}, Q, \delta, q_0, F \rangle$, where Q is the set of *control states*, $q_0 \in Q$ the *initial state*, $F \subseteq Q$ the set of final states, and $\delta : Q \times \Sigma \cup \{\#, \&\} \times \{0,1\}^k \longrightarrow \mathcal{P}(Q \times \{-1,0,1\}^{k+1})$ is the *transition mapping*. The input of the machine is a finite tape τ containing a word of the form $\#w\&$, where $\#, \& \notin \Sigma$ are the left and right end of tape markers, and $w \in \Sigma^*$. By τ_i we indicate the symbol at position i on the tape. A configuration $\langle q, i, \mathbf{x} \rangle$ is an element of the set $Q \times \mathbb{N} \times \mathbb{Z}^k$, where q is the current control state, $1 \leq i \leq |w| + 2$ the current position of the input (read only) head, and $\mathbf{x}$ the current values of the counters[1]. A *configuration* $\langle q', j, \mathbf{x}' \rangle$ is said to be the successor of $\langle q, i, \mathbf{x} \rangle$, denoted by $\langle q, i, \mathbf{x} \rangle \rightarrow \langle q', j, \mathbf{x}' \rangle$ if and only if there exists $\langle q', d, \mathbf{a} \rangle \in \delta(q, \tau_i, \zeta(\mathbf{x}))$ such that $j = i + d$ and $\mathbf{x}' = \mathbf{x} + \mathbf{a}$. As usual, we require a special behavior in the presence of the end of tape markers # and &, preventing the input head to fall off the tape. A *run* of the machine is a sequence of configurations $c_0, c_1, c_2 \ldots c_N$ such that $c_0 = \langle q_0, \mathbf{0} \rangle$ and $c_i \rightarrow c_{i+1}$ for $0 \leq i < N$. The run is said to be *accepting* if the control state of the last configuration is an element of F. An input string w, i.e. $\tau = \#w\&$, is *accepted* if the machine has at least one accepting run on it. The set of all accepted strings is the *language* of M, denoted by $\mathcal{L}(M)$.

Let $\mathrm{CM}(k, r, l)$ denote the class of all 2-way counter machines with k counters, and the restriction that, in every accepting run, each counter alternates from increasing to decreasing mode at most r times, and the input head changes direction at most l times. These machines are called (r,l)*-reversal bounded*. Further, let $\mathrm{CM}(k, r, l, n)$ be the class of (r,l)-reversal bounded machines restricted to work only on input tapes of the form $\#u_1^{i_1} \ldots u_n^{i_n}\&$, for some $u_k \in \Sigma$ and $i_k \in \mathbb{N}$, $1 \leq k \leq n$. Obviously, $\mathrm{CM}(k, r, l, n) \subseteq CM(k, r, l)$. By $\mathrm{DCM}(k, r, l, n)$ we denote the subclass of *deterministic* machines from $\mathrm{CM}(k, r, l, n)$. It is well-known that the emptiness, infiniteness and disjointness problems for the class $\mathrm{CM}(k, r, l, n)$ are decidable, and moreover, the universe, containment and equivalence problems for the class of $\mathrm{DCM}(k, r, l, n)$ are also decidable [13]. In the following, we may lift the restriction on either the number of counter reversals, direction changes, or input letters by writing ∞ instead of r, l, n, respectively.

In this paper we investigate a different class of counter machines, defined as follows. A relation $R(\mathbf{x}, \mathbf{x}')$ that can be written as a finite conjunction:

$$\bigwedge x_i - x_j \leq a_{ij} \wedge \bigwedge x'_l - x_m \leq b_{lm} \wedge \bigwedge x_n - x'_p \leq c_{np} \wedge \bigwedge x'_q - x'_r \leq d_{qr}$$

for some $1 \leq i, j, l, m, n, p, q \leq k$, and $a_{ij}, b_{lm}, c_{np}, d_{qr}$ either integer constants or parameters ranging over $\mathbb{Z}$, is said to be an *affine relation*. Let $\mathbf{z}$ denote the set of parameters of R. Notice that any affine relation R between $\mathbf{x}$ and $\mathbf{x}'$, with parameters $\mathbf{z}$, can be defined by a counter machine $M_R \in \mathrm{CM}(k + \|z\|, 1, 0, 1)$, in the following sense: $\models R(\mathbf{x}, \mathbf{x}', \mathbf{z})$ if and only if M_R, started in a configuration $\langle q_0, \mathbf{xz} \rangle$, has an accepting run ending in $\langle q_f, \mathbf{x}'\mathbf{z} \rangle$. In other words, the values of the parameters do not change during the computation. We further denote the existence of this run by writing $\langle q_0, \mathbf{xz} \rangle \xrightarrow{R} \langle q_f, \mathbf{x}'\mathbf{z} \rangle$. A *counter automaton* (CA) is a counter machine $M \in \mathrm{CM}(k, \infty, 0, 1)$, in which the transition relation is of the form $\bigcup_i \xrightarrow{R_i}$, and R_i are affine relations. Thus, a CA is a one-way counter machine working on a 1-letter alphabet. Notice that a CA is not r-reversal bounded, even if we restrict the control to only one state and a self-loop as in, e.g. $q \xrightarrow{-1 \leq x - x' \leq 1} q$.

[1] In the classical literature [13], the counters are assumed to take only positive values, however this is not a restriction, since a machine with integer counters can be simulated by a machine working only on positive counters, by encoding the k-tuple of signs in the control state.

A control state r is said to be the *successor* of a state q if and only if there exists configurations $\langle q,\mathbf{x}\rangle \rightarrow \langle r,\mathbf{x}'\rangle$, for some $\mathbf{x},\mathbf{x}' \in \mathbb{Z}^k$. A *control path* is a sequence of 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. The interested reader can also refer to [14] for an alternative, yet equivalent definition of flatness.

The goal of this paper is to investigate flat counter automata with respect to their emptiness problem. Since there are no ε-transitions, this problem translates into a reachability problem: is there any final control state that is reachable? An important role is played by the set of values $\mathcal{V}(M)$, since the 1-letter language of a CA is empty if and only if its set of values is. As we show in the following, the latter 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. Clearly we have $\mathrm{FCA}(p,n) \subseteq \mathrm{FCA}(q,m)$, if $p \leq q$ and $n \leq m$.

It is well-known that the class of affine relations is closed under composition, defined as $(R_1 \circ R_2)(\mathbf{x},\mathbf{y}) = \exists \mathbf{z}\, R_1(\mathbf{x},\mathbf{z}) \wedge R_2(\mathbf{z},\mathbf{y})$. In other words, the existential quantifiers can be eliminated[2], the result being written as another affine relation, possibly by introducing fresh variables. As a consequence, we can assume without losing generality, that each control path $q_1 \xrightarrow{R_1} q_2 \ldots q_{n-1} \xrightarrow{R_{n-1}} q_n$ is equivalent to a transition $q_1 \xrightarrow{R_1 \circ \ldots \circ R_{n-1}} q_n$. Applying this transformation to the whole counter automaton, we obtain a *normalized* counter automaton. The class $\mathrm{FCA1A}(p,n)$ is the subclass of $\mathrm{FCA}(p,n)$ in which, the transition relation of each loop, in the normal form, is a formula of the form:

$$x'_i \leq x_j + p \;\wedge\; x_k \leq x'_i + q \;\wedge\; \bigwedge_{j \neq i} x'_j = x_j \wedge \phi(\mathbf{x}) \wedge \psi(\mathbf{x}')$$

where ϕ, ψ are affine formulae. In other words, at most one assignment is performed at the time.

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 [7]. The basic result has been discovered by A. Church [4], and the essential undecidability (undecidability of its every consistent extension) by B. Rosser [22]. To complete the picture, the existential fragment of the full arithmetic, i.e. *Hilbert's Tenth Problem* [9] was proved undecidable by Y. Matiyasevich [16]. On the positive side, the decidability of the arithmetic of natural numbers with *addition and successor function* $\langle \mathbb{Z},\geq,+,0,1\rangle$ has been shown by M. Presburger [21].

Let us first introduce the theories of Presburger arithmetic [21] 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

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

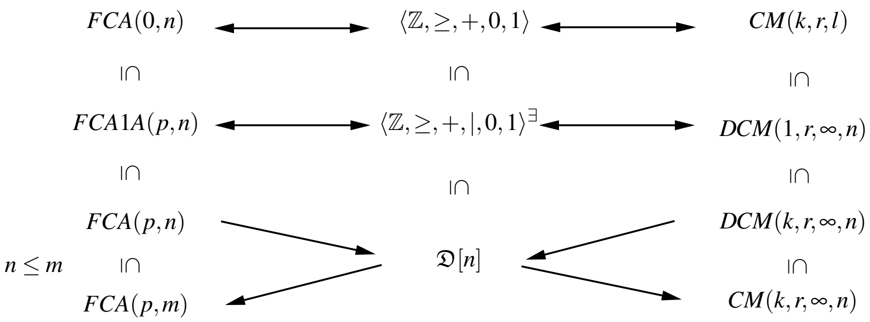

Figure 1: A Hierarchy of Flat Counter Automata, Arithmetic and Counter Machines

meaning of the function symbols $0, 1, +$ is the natural one. The theory $\langle \mathbb{Z}, \geq, +, 0, 1 \rangle$ is equivalent to the set of positive boolean combinations of relations of one of the following forms:

$$\sum_{i=1}^{n} a_i x_i + b \quad \geq \quad 0 \tag{1}$$

$$\sum_{i=1}^{n} a_i x_i + b \quad \equiv \quad 0 \mod d \tag{2}$$

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 $P(\mathbf{x}) = \sum_{i=1}^{m} a_i t_i(\mathbf{x}) + a_0$, where t_i are multiplicative terms of the 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:

$$\sum_{i=1}^{n} p_i(m) x_i + p_0(m) = 0 \tag{3}$$

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.

With this notation, Figure 1 shows the relations between various subclasses of flat counter automata, integer arithmetic and 2-way counter machines. The thick arrows show reductions between classes of counter machines and subtheories of arithmetic, with the following meaning: if C is a class of counter machines and T is an arithmetic theory, $C \longrightarrow T$ means that, for every machine $M \in C$ there exists an open formula $\varphi(\mathbf{x})$ in the language of T, such that $\mathcal{L}(M) \neq \emptyset$ if and only if $\models \exists \mathbf{x}\, \varphi(\mathbf{x})$. The direction $T \longrightarrow C$ is defined in a symmetrical way.

Let us start by explaining the reductions from the right-hand side of Figure 1. For $\langle \mathbb{Z}, \geq, +, 0, 1 \rangle \longleftrightarrow \mathrm{CM}(k,r,l)$, the right to left direction was proved in [13]. The other direction is proved by the following Lemma.

Lemma 1 $\langle \mathbb{Z}, \geq, +, 0, 1 \rangle \longrightarrow CM(k,r,l)$.

Proof: Let $\varphi(\mathbf{x})$, $\mathbf{x} = \{x_1, \ldots, x_n\}$ be a formula of $\langle \mathbb{Z}, \geq, +, 0, 1 \rangle$, i.e. a positive boolean combination of relations of either one of the forms (1) or (2). Let $\Sigma = \{u_1, \ldots, u_n, v_1, \ldots, v_n\}$. We shall build a machine $M \in \mathrm{CM}(k,r,l)$ that recognizes the following language:

$$L_\varphi = \{s_1^{x_1} \dots s_n^{x_n} \mid s_i \in \{u_i, v_i\} \text{ and } \models \varphi(\sigma(s_1)x_1, \dots, \sigma(s_n)x_n)\}$$

where $\sigma(s) = 1$ if $s \in \{u_1, \dots, u_n\}$ and $\sigma(s) = -1$ if $s \in \{v_1, \dots, v_n\}$. Since $\mathrm{CM}(k,r,l)$ is closed under the operations of union and intersection [13], it is sufficient to exhibit machines that recognize the languages corresponding to (1) and (2). Let $M \in \mathrm{CM}(1,n,1)$ be a machine such that:

- The expected input is an element of $(u_1^*|v_1^*)\dots(u_n^*|v_n^*)$. Any input symbol $s \in \{u_i, v_i\}$ must be followed by either itself, u_{i+1} or v_{i+1}, else M rejects.
- While reading a symbol u_i (v_i) M adds (subtracts) the coefficient a_i from the current value of the counter. At the end of the input, the b value is added to the counter.
- The control of M keeps track of the sign of the counter. There are two disjoint sets of control states Q_+ and Q_-. M moves from Q_+ to Q_- whenever the counter was 0 and a decrement action is performed, and from Q_- back to Q_+ whenever the counter becomes 0 again.
- For (1) M accepts if, at the end of the tape, the control is in a state from Q_+. For (2), if at the end of the tape, M is in a state from Q_+ (Q_-), the value d is repeatedly subtracted (added) from (to) the counter. If, at any time between two consecutive subtractions (additions) the value of the counter is 0, M accepts, otherwise M rejects as soon as the control goes from Q_+ to Q_- (Q_- to Q_+).

Notice that M will halt on any input. It is straightforward to check that the language of the composition of such machines is non empty if and only if the original formula is satisfiable. □

The reductions $\langle \mathbb{Z}, \geq, +, |, 0, 1\rangle^{\exists} \longleftrightarrow \mathrm{DCM}(1,r,\infty,n)$ are described in [8]. In the proofs of these reductions, it is essential that the counter machines are deterministic. The reduction $\mathfrak{D}[n] \longrightarrow \mathrm{CM}(k,r,\infty,n)$ is described in [10], for the case $n = 1$, the generalization of their proof for $n > 1$ being straightforward. The reduction $\mathrm{DCM}(k,r,\infty,n) \longrightarrow \mathfrak{D}[n]$ is given by Lemma 2. It is important to mention that, for $n = 1$ we have $\mathfrak{D}[1] \longleftrightarrow \mathrm{CM}(k,r,\infty,1) = \mathrm{DCM}(k,r,\infty,1)$, the proof of the latter equivalence being given in [11]. Since language emptiness for $\mathrm{CM}(k,r,\infty,1)$ is decidable [11], this entails the decidability of the satisfiability problem for the class $\mathfrak{D}[1]$, which is the main result of [10]. In our paper, we propose an alternative, direct proof for the decidability of $\mathfrak{D}[1]$, using a number theoretic argument.

Lemma 2 *$DCM(k,r,\infty,n) \longrightarrow \mathfrak{D}[n]$.*

Proof: We need to introduce a definition from [8], generalized to the case of $k \geq 1$. We say that a counter machine $M \in \mathrm{DCM}(k,r,\infty,n)$ is *canonical* if and only if the following hold:

1. M halts on all computations.
2. M changes the direction of the input head only at the tape markers (#, &).
3. M reverses its counters only at the left tape marker (#).

One can show that, for every $M \in \mathrm{DCM}(k,r,\infty,n)$ it is possible to effectively build a finite set of canonical machines $M_I \in \mathrm{DCM}(k,r,\infty,n)$, $1 \leq I \leq N$ for some $N \in \mathbb{N}$ depending only on M, such that $\mathcal{L}(M) = \emptyset$ if and only if $\mathcal{L}(M_I) = \emptyset$, for all $1 \leq I \leq N$. The first two conditions can be satisfied by modifying M to perform only full sweeps of the input, as described in [8]. Next, we simulate M using machines that work on inputs of the form:

$$\#(u_1,\langle l_1,0\rangle)^*(u_1,\langle l_1,1\rangle)(u_1,\langle l_1,2\rangle)^*(u_1,\langle l_2,0\rangle)^*(u_1,\langle l_2,1\rangle)(u_1,\langle l_2,2\rangle)^*\ldots$$
$$(u_n,\langle l_{k-1},0\rangle)^*(u_n,\langle l_{k-1},1\rangle)(u_n,\langle l_{k-1},2\rangle)^*(u_n,\langle l_k,0\rangle)^*(u_n,\langle l_k,1\rangle)(u_n,\langle l_k,2\rangle)^*\&$$

where $\{l_1,\ldots,l_k\}$ is a permutation of $\{1,\ldots,k\}$. We will have a different machine M_I for each such possible indexing. In order to simulate M, M_I treats symbols $(u_i,\langle l_j,l\rangle)$, $1 \le i \le n$, $1 \le l \le 3$ just as M treats u_i. If M_I attempts to reverse any counter other than x_{l_j} on a segment of the form $(u_i,\langle l_j,0\rangle)^*(u_i,\langle l_j,1\rangle)(u_i,\langle l_j,2\rangle)^*$, the input is rejected. Otherwise, if M_I attempts to reverse x_{l_j} on a symbol that is not $(u_i,\langle l_j,1\rangle)$, the input is rejected. In the last case, M_I remembers $(u_i,\langle l_j,1\rangle)$ in its finite control, moves the head until it encounters the left end marker # (possibly by reversing the direction once at the right end marker &), reverses x_{l_j} and continues until it restores the position of the input head.

Now for any canonical machine M_I, we will show the existence of a system $S_I \in \mathfrak{S}(m)$ with parameters $\mathbf{z} = \{z_1,\overline{z_1},\ldots,z_m,\overline{z_m}\}$, for some m, depending on M_I. In the following, we ignore the subscript I. Without loss of generality, assume that each counter reverses mode from non-decreasing to non-increasing at most once, and that M accepts when all counters have the value zero. Let the input tape be of the form $\#u_1^{y_1}\ldots u_n^{y_n}\&$. Each time M sweeps across $u_i^{y_i}$, $1 \le i \le n$, the j-th counter increases by $f_{ij} = a_{ij}y_i + b_{ij}$, $1 \le j \le k$, if M is in non-decreasing mode with respect to x_j and decreases by $g_{ij} = c_{ij}y_i + d_{ij}$, otherwise. The machine accepts if, for each counter there exists two values z_j and $\overline{z_j}$ such that $\sum_{i=1}^{n} z_j f_{ij} + \overline{z_j} g_{ij} = 0$. Intuitively, z_j ($\overline{z_j}$) represents the number of times M sweeps across the entire input being in the non-decreasing (non-increasing) mode, with respect to x_j. Moreover, it is required that $z_i + \overline{z_i} = z_j + \overline{z_j}$, for all $1 \le i < j \le k$. Altogether, these conditions form a system of Diophantine equations of the form (3). $\square$ The techniques used in the proof of the above Lemma are adapted from the proof of Theorem 1 in [8].

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 $\langle q_0, \mathbf{xz}\rangle$ 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 $A \in \mathrm{FCA}(p,n)$ can 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:

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

where $m_i \le n$, 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 2 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 $n \leq i \leq m$.

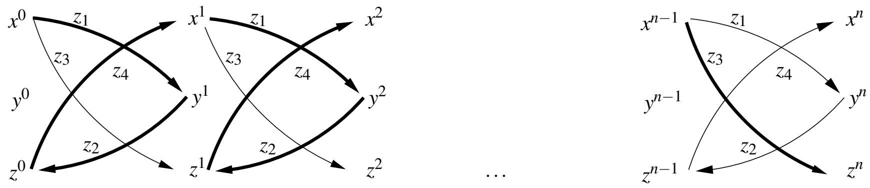

Figure 2: Constraint Graph for $x_1 - x_2' \leq z_1 \wedge x_2' - x_3 \leq z_2 \wedge x_3 - x_1' \leq z_3 \wedge x_1 - x_3' \leq z_4$

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:

$$\bigwedge_{x,y\in\mathbf{x}} x-y \le \min\{x^0 \to y^0\} \wedge x'-y' \le \min\{x^n \to y^n\} \wedge \\ x-y' \le \min\{x^0 \to y^n\} \wedge x'-y \le \min\{x^n \to y^0\} \tag{4}$$

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 $x-y \le \alpha$ are replaced by $x-t' \le \alpha \wedge t'-y \le 0$, and all constraints of the form $x'-y' \le \alpha$ are replaced by $x'-t \le \alpha \wedge t-y' \le 0$, 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 $\mathbf{x}^i \cup \mathbf{x}^{i+1}$, $0 \le i < m$. 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*. Figure 3 (b) shows the word encoding of the highlighted path between x^0_1 and x^n_3, from Figure 2.

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 $x-y \le \alpha$ 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 $\Sigma_\varphi^{e,o} = \Sigma_\varphi^e \cup \Sigma_\varphi^o$. Since, by the previous assumption, no $G \in \Sigma_\varphi^{e,o}$ contains edges of the form $x \xrightarrow{\alpha} y$ or $x' \xrightarrow{\alpha} y'$, the number of edges in all symbols of Σ_φ^e is even, while the number of edges in all symbols of Σ_φ^o 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 $w \in \Sigma_\varphi^{e,o*}$. Notice that $\omega(w) \in \mathbf{lin}\mathbb{Z}[\mathbf{z}]$, for any given $w \in \Sigma_\varphi^{e,o*}$, 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_φ^e for the former, and Σ_φ^o for the latter. Precisely, we have $A_\varphi^{e,o} = \langle Q, \delta \rangle$, where $Q = \{l, r, lr, rl, \bot\}^k$, and $\mathbf{q} \xrightarrow{G} \mathbf{q}'$ if the following conditions hold, for all $1 \le i \le k$:

- $q_i = l$ 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.
- $q'_i \in \{lr, \bot\}$ iff G has no edge involving x'_i.
- $q_i \in \{rl, \bot\}$ iff G has no edge involving x_i.
- G has at least one edge between $\mathbf{x}$ and $\mathbf{x}'$.

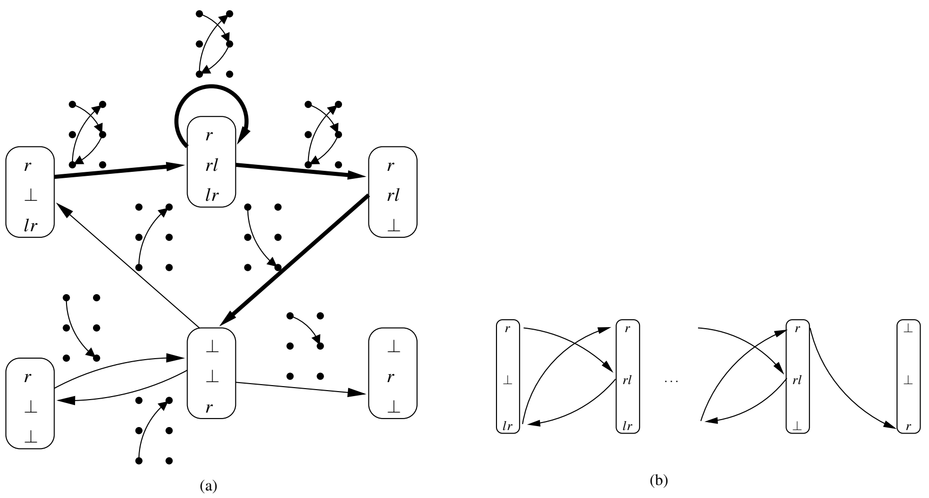

Figure 3: The Odd Automaton for $x_1 - x'_2 \le z_1 \wedge x'_2 - x_3 \le z_2 \wedge x_3 - x'_1 \le z_3 \wedge x_1 - x'_3 \le z_4$

The odd automaton for $\varphi = x_1 - x'_2 \le z_1 \wedge x'_2 - x_3 \le z_2 \wedge x_3 - x'_1 \le z_3 \wedge x_1 - x'_3 \le z_4$ is depicted in Figure 3 (a). An example of a run of this automaton is given in Figure 3 (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, $q_{i\,j} = lr$ 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 $q_{i\,j}$, and there is an edge from $q_{i\,j}$ to $q_{i+1\,h}$ 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 $q_{i+1\,h}$ to $q_{i\,j}$ are defined symmetrically. Each node in $G(\pi)$ is labeled by a symbol from $\{l, r, lr, rl, \perp\}$, and we write, e.g. $q_{i\,j} = l$, meaning that $q_{i\,j}$ is labeled with l. We denote by $\omega(\pi)$ the weight of the run π, defined as $\omega(\pi) = \omega(G(\pi))$.

Lemma 3 *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* $q_{i\,j}$, $1 \leq i \leq n$, $1 \leq j \leq k$, *from* $G(\pi)$, *has at most one predecessor and at most one successor.*

Proof: Suppose that $q_{i\,j}$ is a node in $G(\pi)$, and that $q_{i\,j}$ has two or more predecessors. We distinguish three cases: $i = 1$, $1 < i < n$, and $i = n$. For the case $i = 1$, $q_{1\,j}$ must have two or more incoming edges from $\mathbf{q}_2$, which is in contradiction with the third point in the definition of Σ^e_φ. The case $i = n$ is symmetrical. In the case $1 < i < n$ we have $\mathbf{q}_{i-1} \xrightarrow{G_{i-1}} \mathbf{q}_i \xrightarrow{G_i} \mathbf{q}_{i+1}$. If $q_{i\,j}$ has two incoming edges, it can only have one edge from $\mathbf{q}_{i-1}$, and another from $\mathbf{q}_{i+1}$. Now if G_i has one edge incoming to $q_{i\,j}$, $1 \leq j \leq k$ it must be that $q_{i\,j} \in \{r, rl\}$. On the other hand, if G_{i+1} has one edge incoming to $q_{i\,j}$, it must be that $q_{i\,j} \in \{l, lr\}$, and we obtain a contradiction. The proof for $q_{i\,j}$ having at most one outgoing edge is symmetrical. $\square$

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 4 *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.

Proof: 1. "$\longrightarrow$" Assume that A^e_{ij} has an accepting run $\pi : \mathbf{q}_0 \xrightarrow{G_1} \mathbf{q}_1 \xrightarrow{G_2} \ldots \mathbf{q}_{n-1} \xrightarrow{G_n} \mathbf{q}_n$, with $\mathbf{q}_0 \in Q_0$ and $\mathbf{q}_n \in F$, $n \leq m$. We need to build a path in G^∞_φ, from x^0_i to x^0_j, stretching between 0 and at most n. Note first that $G(\pi)$ is isomorphic with a subset of G^∞_φ. Our argument is the following: suppose that we have already built a path from q_{0i} to q_{ht}, for some $0 \leq h \leq m$, $1 \leq t \leq k$, then either $h = 0$ and $t = j$, case in which we are done, or else we can extend this path further. Since $G(\pi)$ is finite, we will eventually find either a path from q_{0i} to $q_{0\,j}$, or a cycle. But, in the last case, $G(\pi)$ must have a node with two incoming edges and at least one outgoing edge. For, otherwise q_{0i} would belong to a cycle, having an incoming edge from $\mathbf{q}_1$. But this contradicts with the fact that $q_{0i} = r$ and the only edge involving q_{0i} is an outgoing edge. According to Lemma 3, no node in $G(\pi)$ can have two incoming edges, thus we have reached a contradiction.

We are now left with proving that every node, other than q_{0j}, that is reachable from q_{0i}, has at least one successor. Obviously, this is the case for q_{0i}, since $q_{0i} = r$. For other nodes $q_{0j} \neq \bot$, $j \neq i$, we have $q_{0j} = lr$, and we are done. Any other node q_{h_t}, $1 \leq h \leq n$, $1 \leq t \leq k$ that is reachable from q_{0i} has at least one incoming edge. Hence it must be that $q_{h_t} \neq \bot$. If $q_{h_t} \in \{lr, rl\}$, we are done. Otherwise, if $q_{h_t} = l$, and since $\mathbf{q}_{h-1} \xrightarrow{G_h} \mathbf{q}_h$, then G_h has an edge $x'_t \xrightarrow{c} x_u$, for some $1 \leq u \leq k$, which becomes an outgoing edge of q_{h_t}. For the case $q_{h_t} = r$, we must distinguish between $h < n$ and $h = n$. In case $h < n$, we have $\mathbf{q}_h \xrightarrow{G_{h+1}} \mathbf{q}_{h+1}$ and we do a similar reasoning, as in the case $q_{h_t} = l$. Else, if $h = n$, we cannot have $q_{n_t} = r$, because that would contradict with the fact that $\mathbf{q}_n \in F = \{rl, \bot\}^k$.

"$\longleftarrow$" We show the existence of the run by induction on n. Note that one only needs to consider states and transitions that occur within the path, and verify that the transitions are valid. This check is trivial.

2. Let A^e_{ij} have an accepting run $\rho : \mathbf{q}_0 \xrightarrow{G_1} \mathbf{q}_1 \xrightarrow{G_2} \ldots \mathbf{q}_{n-1} \xrightarrow{G_n} \mathbf{q}_n$, with $\mathbf{q}_0 \in Q_0$ and $\mathbf{q}_n \in F$. By the first point, there exists path π from q_{0i} to q_{0j} in $G(\rho)$. Moreover, this path should be unique, since no node in the graph can have two different successors. We prove first that each node $q_{h_t} \neq \bot$, $1 \leq h \leq n$, $1 \leq t \leq k$, that is not on π, must belong to a cycle, which does not intersect with π. This is done along the same lines as the proof for existence of the path, at the previous point. First, each node $q_{h_t} \neq \bot$, $q_{h_t} \notin \pi$, must have a successor. Moreover, the successor must not be on π, or else one node from π would have two different predecessors. Hence, q_{h_t} belongs to an infinite path π', and $\pi \cap \pi' \neq \emptyset$. Now we need to show that π' is a cycle. But if this would not be the case, since π' is infinite, then at least one node on π' must have two different predecessors, which results in a contradiction with Lemma 3.

Since for every accepting run ρ of A^e_{ij} of length m, there exists a path π from q_{0i} to q_{0j}, stretching from 0 to at most m, and moreover, every edge not on π belongs to a cycle, we have that $\omega(\rho) = \omega(\pi) + \sum_{\gamma \text{ is a cycle in } \rho} \omega(\gamma)$. Since there are no cycles γ such that $\omega(\gamma) < 0$, we have that $\omega(\rho) \geq \omega(\pi)$. Dually, for each path π from q_{0i} to q_{0j}, one can build an accepting run ρ such that $\omega(\rho) = \omega(\rho)$. Suppose now that, for instance we had:

$$\begin{aligned} &\min\{\omega(\pi) \mid \pi \text{ is a path from } q_{0i} \text{ to } q_{0j} \text{ stretching from 0 to } n \leq m\} \\ &\neq\ \min\{\omega(\rho) \mid \rho \text{ is an accepting run of } A^e_{ij} \text{ of length } n \leq m\} \end{aligned}$$

Suppose that the left hand side is strictly greater than the right hand side. Then there exists an accepting run of A^e_{ij} of length $n \leq m$ which has smaller weight than any path from q_{0i} to q_{0j} stretching from 0 to some $n' \leq m$. But this is in contradiction with the fact that for each run of length n, there exists a path stretching from 0 to $n' \leq n$ of smaller weight. Else, if the right hand side is strictly greater than the left hand side, then there exists a path from q_{0i} to q_{0j}, stretching from 0 to some $n \leq m$ of weight smaller than that of any accepting run of A^e_{ij} of length $n' \leq m$. But this is in contradiction with the existence of a run of length exactly n, and of weight equal to the weight of the path. $\square$

Lemma 5 *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.*

Proof: "$\longrightarrow$" Suppose that A^e_i has an accepting run $\rho : \mathbf{q}_0 \xrightarrow{G_1} \mathbf{q}_1 \xrightarrow{G_2} \ldots \mathbf{q}_{n-1} \xrightarrow{G_n} \mathbf{q}_n$, with $\mathbf{q}_0 \in Q_0$ and $\mathbf{q}_n \in F$, such that $\omega(\rho) < 0$. Then, by the first point of Lemma 4, there exists a cycle π in $G(\rho)$, such that q_{0i} is on that cycle. Also, by the proof of the second point of Lemma 4, we have that $\omega(\rho) = \omega(\pi) + \sum_{\gamma \text{ is a cycle in } \rho} \omega(\gamma) < 0$. Then either $\omega(\pi) < 0$ or $G(\rho)$ has another cycle $\gamma \neq \pi$ whose weight is negative. Since $G(\rho)$ is isomorphic with a subset of G^∞_φ, we are done.

"$\longleftarrow$" Suppose that G^{∞}_{φ} has a cycle of negative weight, stretching between n and m, for some $n < m$. Note that all subgraphs of G^{∞}_{φ}, that consist only of nodes $\mathbf{x}^i$ and $\mathbf{x}^{i+1}$ (together with the edges between them), are isomorphic. Hence there exists a cycle of negative weight, stretching between n and m if and only if there exists a cycle of negative weight stretching between 0 and $m-n$. Now one can build a run of A^e_i that has exactly the same weight as the latter cycle. □

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:

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

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

Lemma 6 *For any $1 \le i, j \le k$, 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.*

Proof: This proof is done along the same lines as the proof of Lemma 4. "$\longrightarrow$ If ρ is an accepting run of A^o_{ij} of length m, then there exists a path π from q_{0_i} to q_{0_j} in $G(\rho)$, and moreover, since $G(\rho)$ does not have cycles of negative weight, $\omega(\rho) \ge \omega(\pi)$. "$\longleftarrow$" If G^{∞}_{φ} has a path between x^0_i and x^m_j, then there exists an accepting run ρ of A^o_{ij}, of length m, such that $G(\rho)$ has a path π from q_{0_i} to q_{m_j}, and no other edges, except for the ones in π. Hence $\omega(\rho) = \omega(\pi)$. The equality of minimal weights follows in the same way as in the proof of Lemma 4. □

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 $\min\{x^i \to y^j\}$, 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 $q \to r$ a linear expression $\omega(q, r) \in \mathbf{lin}\mathbb{Z}[\mathbf{z}]$. If δ has no transition $q \to r$, 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 $q \to r$ 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:

$$\phi_A(l, w) \triangleq \exists \mathbf{x} \bigvee_{q_f \in \mathcal{F}} \varphi_{q_f}(\mathbf{x}) \ \wedge \sum_{q,r \in Q} x_{qr} = l \ \wedge \sum_{q,r \in Q} x_{qr}\omega(q, r) = w \tag{5}$$

where $\varphi_{q_f}(\mathbf{x})$ expresses the necessary and sufficient conditions in order for $\mathbf{x}$ to define a 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. For self-containment reasons, we give the definition of φ_{q_f} below.

$$\varphi_{q_f}(\mathbf{x}) \triangleq \begin{cases} \varphi^1_{q_0}(\mathbf{x}) \wedge \varphi^2_{q_f}(\mathbf{x}) \wedge \varphi^3_{q_0 q_f}(\mathbf{x}) \wedge \psi(\mathbf{x}) & \text{if } q_f \ne q_0 \\ \varphi^4(\mathbf{x}) \wedge \psi(\mathbf{x}) & \text{otherwise} \end{cases}$$

where

$$\varphi_q^1(\mathbf{x}) \;\triangleq\; 1 + \sum_{p\in Q} x_{pq} = \sum_{r\in Q} x_{qr} \tag{6}$$

$$\varphi_q^2(\mathbf{x}) \;\triangleq\; \sum_{p\in Q} x_{pq} = \sum_{r\in Q} x_{qr} + 1 \tag{7}$$

$$\varphi_{qq'}^3(\mathbf{x}) \;\triangleq\; \bigwedge_{s\in Q\setminus\{q,q'\}} \sum_{p\in Q} x_{ps} = \sum_{r\in Q} x_{sr} \tag{8}$$

$$\varphi^4(\mathbf{x}) \;\triangleq\; \bigwedge_{s\in Q} \sum_{p\in Q} x_{ps} = \sum_{r\in Q} x_{sr} \tag{9}$$

and $\psi(\mathbf{x})$ is detailed next. Intuitively, the first three formulae above are the flow equations for the initial state (6), the final state of the run (7), and any state, other than the initial and the final, that may occur on the run (8). The case of (possibly empty) circular runs (i.e., $q_0 = q_f$) needs only one flow equation (9).

The final condition $\psi(\mathbf{x})$ is that a path must be connected. Notice that the above flow equations can be satisfied by two strongly connected components of A with no transition relating them. Let $\mathcal{R}_A(q)$ be the set of all runs accepted by a state $q \in Q$, *with no repeated transitions*. Since Q is finite, this set is also finite. With these considerations, the connectivity condition can be given as a prefix closure, where $\alpha\cdot\beta$ denotes the concatenation of paths α and β:

$$\psi(\mathbf{x}) \triangleq \bigwedge_{q\in Q} \bigvee_{r\in Q} x_{qr} > 0 \;\longrightarrow\; \bigvee_{\rho\cdot pq\in\mathcal{R}_A(q)} x_{pq} > 0$$

If $\mathbf{m} \in \mathbb{N}^{\|\mathbf{x}\|}$ is an interpretation of $\mathbf{x}$, we refer as a $\mathbf{m}$-path to a path $s_0, s_1, \ldots, s_n$, where $s_i \in Q$, such that each transition $s_i \to s_{i+1}$ is taken *exactly* $m_{s_i s_{i+1}}$ times. We may as well refer to an $\mathbf{m}$-cycle, $\mathbf{m}$-scc (strongly connected component) or, $\mathbf{m}$-run, with the obvious meanings. The following result is needed to prove that our conditions are sufficient.

Lemma 7 *If $\models \varphi_{q_f}(\mathbf{m})$ for some $q_f \in \mathcal{F}$, then for any $\mathbf{m}$-scc we have that q_f is reachable from any state of the scc by an $\mathbf{m}$-path.*

Proof: For any state $q \in Q$, let $\theta_m(q) = \sum_{r\in Q} m_{qr} - \sum_{p\in Q} m_{pq}$. Since $\models \varphi_{q_f}(\mathbf{m})$ for some interpretation $\mathbf{m}$, we have that $\theta_m(q) = 0$ for any $q \in Q\setminus\{q_0, q_f\}$, and either $\theta_m(q_0) = 1$ and $\theta_m(q_f) = -1$, if $q_0 \neq q_f$, or $\theta_m(q_0) = \theta_m(q_f) = 0$, otherwise. Let $C = \{s_1, s_2, \ldots, s_n\}$ be an $\mathbf{m}$-scc. Define $\theta_m(C) = \sum_{i=1}^n \theta_m(s_i)$. By induction on n, it can be shown that $\theta(C) = \sum_{q\in C, r\in Q\setminus C} m_{qr} - \sum_{p\in Q\setminus C, q\in C} m_{pq}$. If C does not contain q_f, then either $\theta(C) = 1$, if $q_0 \in C$ or $\theta(C) = 0$, otherwise.

Let $\delta_m(q_0, C)$ be either zero, if $q_0 \in C$, or the length of the shortest $\mathbf{m}$-path from q_0 to a state in C, otherwise. Since $\models \psi(\mathbf{m})$ is the case, then such a path is guaranteed to exist.

Suppose now that there exists an $\mathbf{m}$-scc C from which q_f is not reachable by any $\mathbf{m}$-path, and choose C such that $\delta_m(q_0, C)$ is maximal. We need to consider two cases, either:

1. $q_0 \in C$, in which case $\sum_{q\in C, r\in Q\setminus C} m_{qr} = 1 + \sum_{p\in Q\setminus C, q\in C} m_{pq} > 0$, or

2. $q_0 \notin C$, in which case there must be a state $q \in C$ that has at least one predecessor not in C on the $\mathbf{m}$-path from q_0 to q. Hence $\sum_{q\in C, r\in Q\setminus C} m_{qr} = \sum_{p\in Q\setminus C, q\in C} m_{pq} > 0$.

In both cases there must exist at least one state $q' \in C$ that has a successor $r' \notin C$. Then it must be the case that $r' \in C'$ for some other $\mathbf{m}$-scc C'. Since q_f is not reachable from $q' \in C$, it must not be reachable from $r' \in C'$, either. Then either C is reachable from $r' \notin C$, which contradicts the maximality of C, or C is not reachable from r', which contradicts the maximality of $\delta(q_0,C) < \delta(q_0,C')$. This completes our proof. □

We are now ready to prove that the formula defined in the previous correctly characterizes all runs accepted by A:

Lemma 8 *For all $n \in \mathbb{N}$, $\gamma \in \mathbb{Z}$, $\models \phi_A(n,\gamma)$ if and only if A has an accepting run of length n and weight γ.*

Proof: We need to prove that, for all $n \in \mathbb{N}$ and $\gamma \in \mathbb{Z}$, $\models \phi_A(n,\gamma)$ if and only if A has a run ρ of length n and weight γ, from q_0 to some $q_f \in \mathcal{F}$. For the "if" part, if ρ is an accepting run of length n and weight γ, let $\mathbf{m}$ be the vector of occurrences of each transition within ρ and check $\models \varphi(\mathbf{m})$, which is trivial.

To prove the "only if" part, let $\mathbf{m}$ be the witness for $\varphi(\mathbf{x})$ i.e., $\models \varphi(\mathbf{m})$. We shall build an accepting $\mathbf{m}$-run of A, by induction on $M = \sum_{q,r\in Q} m_{qr}$. The base case is $M = 0$, which implies $y = 0$, hence the only run to be considered is the empty run. Let us prove that this is also an accepting run i.e. $q_0 \in \mathcal{F}$. Assuming the contrary we have $q_0 \neq q_f$ for all $q_f \in \mathcal{F}$. But $\models \varphi_{q_f}(\mathbf{m})$, for some $q_f \in \mathcal{F}$ must be the case, hence, also $\models \varphi^1_{q_0}(\mathbf{m})$, which is a contradiction, since we have assumed that $M = 0$.

For the inductive step $M > 1$, assume that for all $M' < M$, where $M' = \sum_{q,r\in Q} m'_{qr}$, if $\models \varphi_{q_f}(\mathbf{m}')$ for some $q_f \in \mathcal{F}$, then A has an $\mathbf{m}$-run from q_0 to q_f. By the hypothesis, there exists a final state $q_f \in \mathcal{F}$ such that $\models \varphi_{q_f}(\mathbf{m})$. The idea is to exhibit the presence of an $\mathbf{m}$-scc whose transitions can be eliminated, obtaining as result $\mathbf{m}'$. Since $M' = \sum_{q,r\in Q} \mathbf{m}'_{qr} < M$, if we actually show that $\models \varphi_{q_f}(\mathbf{m}')$, then the inductive hypothesis applies. In this case, there exists a $\mathbf{m}'$-run that ends in q_f. The desired $\mathbf{m}$-run is obtained by appending the scc back to the $\mathbf{m}'$-run. Since $M > 0$ there exists a transition $s \longrightarrow t$ such that $m_{st} > 0$. Because $\models \psi(vecm)$, there exists an $\mathbf{m}$-path ρ from q_0 to s. We only need to show now that q_f is reachable from t by an $\mathbf{m}$-path ρ'. For this is the case, we have an accepting run $\rho \cdot \rho'$. Next, there are three cases to be considered:

- for any transition $q \longrightarrow r$, if $q \longrightarrow r \in \rho \cdot \rho'$ then $m_{qr} = 1$ and $m_{qr} = 0$, otherwise. Then $\rho \cdot \rho'$ is the desired path and we are done.
- for any transition $q \longrightarrow r$, if $q \longrightarrow r \in \rho \cdot \rho'$ then $m_{qr} = 1$ and for some $q' \longrightarrow r' \notin \rho \cdot \rho'$ we have $m_{q'r'} > 0$. Then, by $\models \psi(\mathbf{m})$, there must be an $\mathbf{m}$-path π from q_0 to q'. Let r_0 be the last common state of π and $\rho \cdot \rho'$ i.e., $q_0 \dots r_0$ is the maximal common subpath of π and $\rho \cdot \rho'$, such that $r_0 \longrightarrow s_1 \in \pi$ and $r_0 \longrightarrow r_1 \in \rho \cdot \rho'$ for two distinct states s_1, r_1, with $m_{r_0 s_1} > 0$ and $m_{r_0 r_1} > 0$. In case $r_0 = q_0$, we have $1 + \sum_{p\in Q} pq_0 = \sum_{r\in Q} q_0 r > 1$, hence $m_{p_0 q_0} > 0$ for some $p_0 \in Q$. But,since $\models \psi(\mathbf{m})$, p_0 must be reachable from q_0 by an $\mathbf{m}$-path, hence p_0, q_0 belong to the same $\mathbf{m}$-scc C. We define $\mathbf{m}'$ as follows:

$$m'_{st} = \begin{cases} m_{st} - 1 & \text{if } m_{st} > 0 \text{ and } s,t \in C \\ m_{st} & \text{otherwise} \end{cases} \tag{10}$$

It is easy to check that $\models \varphi_q(\mathbf{m}')$, hence the induction hypothesis applies and we are done. The remaining case is $r_0 \neq q_0$ i.e., the paths π and $\rho \cdot \rho'$ have a non-trivial common prefix. We shall now iterate the following reasoning, for $i = 1, 2, \dots$, taking two cases at each step:

1. if $r_i = q_f$ then there exists an $\mathbf{m}$-path π' from r_0 to q_f. Let S be the set of transitions whose source states are reachable from a state in $\pi \cdot \pi'$. We define $\mathbf{m}'$ as follows:

$$m'_{st} = \begin{cases} m_{st} - 1 & \text{if } m_{st} > 0 \text{ and } s,t \in S \\ m_{st} & \text{otherwise} \end{cases} \tag{11}$$

   It is easy to check that $\models \varphi_q(\mathbf{m}')$, hence the induction hypothesis applies and we are done.

2. else, $\sum_{p \in Q} m_{pr_i} = \sum_{q \in Q} m_{r_i q} > 0$, thus r_i has a successor r_{i+1} with $m_{r_i r_{i+1}} > 0$. If $r_{i+1} = r_j$ for some $1 \leq j \leq i$, then all states $r_j, r_{j+1}, \ldots, r_i, r_{i+1}$ belong to the same $\mathbf{m}$-scc C, and we define $\mathbf{m}'$ as in (10), following the same argument. Otherwise, repeat step 1, taking $i+1$ instead of i.

- for some transition $q \longrightarrow r \in \rho \cdot \rho'$ we have $m_{qr} > 1$. Again, we distinguish two cases, based on whether $r = q_0$ or not. In the case $r = q_0$, we have already discovered a non-trivial $\mathbf{m}$-scc C containing q, r and apply the definition (10). Otherwise, $\sum_{s \in Q} m_{rs} > 0$, thus there exists a successor s_0 of r with $m_{rs_0} > 0$. Now we can apply the same argument from the previous point.

We are left with proving the fact that q_f is reachable from t by a $\mathbf{m}$-path ρ'. To do so, we apply essentially the same argument as in the second point above. If $t = q_0$ then s, t belong to the same non-trivial $\mathbf{m}$-scc C, any by Lemma 7, q_f must be reachable from C. Otherwise, t has a successor t_0 such that $m_{tt_0} > 0$. Continuing in this way, we discover a sequence $t_0, t_1, \ldots$ which either contains q_0, or eventually loops. In both cases, all states from the sequence belong to the same $\mathbf{m}$-scc, and Lemma 7 applies. □

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 9 *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.*

Proof: We apply the following transformation to each disjunct from the definition (5), i.e. for each $q_f \in \mathcal{F}$. Let $\mathbf{x} = \{x_1, \ldots, x_m\}$ be a renaming of the existentially quantified variables, and if x_i, $1 \leq i \leq m$ is the renaming of x_{qr}, then let ω_i, denote the term $\omega(q,r)$. Since the subformula $\varphi_{q_f}(\mathbf{x}) \wedge \sum_{q,r \in Q} x_{qr} = y$ is an open Presburger formula, it is either false or equivalent to a finite disjunction of formulae of the following:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_m \\ y \end{pmatrix} = \begin{pmatrix} a_{01} \\ \vdots \\ a_{0m} \\ b_0 \end{pmatrix} + \begin{pmatrix} a_{11} \\ \vdots \\ a_{1m} \\ b_1 \end{pmatrix} \lambda_1 + \ldots + \begin{pmatrix} a_{k1} \\ \vdots \\ a_{km} \\ b_k \end{pmatrix} \lambda_k$$

for some new existentially quantified variables $\lambda_1, \ldots, \lambda_k$, with $a_{ij}, b_i \in \mathbb{Z}$, $1 \leq i \leq k$, $1 \leq j \leq m$. Since $z = \sum_{q,r \in Q} x_{qr}\omega(q,r)$, we obtain, for each disjunct of the original formula:

$$\begin{pmatrix} y \\ z \end{pmatrix} = \begin{pmatrix} b_0 \\ \sum_{j=1}^m a_{0j}\omega_j \end{pmatrix} + \begin{pmatrix} b_1 \\ \sum_{j=1}^m a_{1j}\omega_j \end{pmatrix} \lambda_1 + \ldots + \begin{pmatrix} b_k \\ \sum_{j=1}^m a_{kj}\omega_j \end{pmatrix} \lambda_k$$

Since $y > 0$, it must be that $b_i > 0$, for all $0 \le i \le n$. Otherwise, if some $b_i < 0$ we can obtain a negative value for y by increasing λ_i sufficiently. On the other hand if some $b_i = 0$, there would be an infinite number of weights z corresponding to the same path length y, resulting in a contradiction. Let $\kappa_i = \bigwedge_{1\le l\le k} b_l \sum_{j=1}^m a_{ij}\omega_j \le b_i \sum_{j=1}^m a_{lj}\omega_j$, with free variables from the set of parameters from φ. We perform a case split, considering the i-th case for a choice of parameter values that satisfy κ_i. Notice that $\models \bigvee_{1\le i\le k} \kappa_i$. If $\models \kappa_i$, the minimal value z can take, in the above formula, for a given y, is encoded by the following:

$$\begin{pmatrix} y \\ z \end{pmatrix} = \begin{pmatrix} b_0 \\ \sum_{j=1}^m a_{0j}\omega_j \end{pmatrix} + \sum_{1\le l\le k}^{l\ne i} \begin{pmatrix} b_l \\ \sum_{j=1}^m a_{lj}\omega_j \end{pmatrix} r_l + \begin{pmatrix} b_i \\ \sum_{j=1}^m a_{ij}\omega_j \end{pmatrix} (\lambda_i + \sum_{1\le l\le k}^{l\ne i} q_l b_l)$$

where q_l and r_l are the quotient and the remainder of λ_l divided by b_i, for all $l \in \{1,\ldots,i-1,i+1,\ldots,k\}$. This is because b_i can be subtracted from any λ_l, $l \ne i$, at most q_l times, by adding at the same time $q_l b_l$ to λ_i, and without modifying the value of y. Since $0 \le r_l < b_i$, we perform another case split and replace r_l by constants in the formula above. Moreover, we introduce a fresh variable m, define $m = \lambda_i + \sum_{1\le l\le k}^{l\ne i} q_l b_l$, and make the substitution accordingly, in the formula above.

Notice however that the above expresses the minimum for only one disjunct of the semilinear transform of $\varphi_{q_f}(\mathbf{x}) \wedge \sum_{q,r\in Q} x_{qr} = y$ considered for only one disjunct from the definition (5). We have to extend the construction to the case of more than one disjuncts. Let us consider the case of two disjuncts, call them D_1 and D_2, the generalization being rather straightforward. For each D_i, $i = 1,2$ we have a formula of the above form, defining the minimal z:

$$D_i : \begin{pmatrix} y \\ z_i \end{pmatrix} = \begin{pmatrix} b_i \\ \beta_i \end{pmatrix} + \begin{pmatrix} c_i \\ \gamma_i \end{pmatrix} m, \quad i = 1,2$$

Our goal is to define the following set:

$$\begin{aligned} D &= \{\min(z_1,z_2) \mid \exists y\ (y,z_1) \in D_1 \ \wedge\ (y,z_2) \in D_2\} \\ &= \{z \mid \exists y\ (y,z) \in D_1 \ \wedge\ \forall z'\ (y,z') \notin D_2\} \\ &\quad \cup \{z \mid \exists y\ (y,z) \in D_2 \ \wedge\ \forall z'\ (y,z') \notin D_1\} \\ &\quad \cup \{z \mid \exists y\ (y,z) \in D_1 \cap D_2 \ \wedge\ z = \min\{z' \mid (y,z') \in D_1 \cap D_2\}\} \end{aligned}$$

The first two sets can be defined directly by adjoining Presburger conditions on m. Let us take for example $\{z \mid (y,z) \in D_1 \ \wedge\ \forall z\ (y,z) \notin D_2\}$, which can be defined by:

$$\exists m\ z = \beta_1 + \gamma_1 m \ \wedge\ \forall m'\ b_1 + c_1 m \ne b_2 + c_2 m'$$

Notice that the above formula can be turned into an equivalent formula of $\mathfrak{D}[m]$, by putting $\forall m'\ b_1 + c_1 m \ne b_2 + c_2 m'$ into the semilinear form. To represent the latter set from the definition of D, we have two symmetrical cases, as follows:

$$b_1 + c_1 m_1 = b_2 + c_2 m_2 \wedge \beta_1 + \gamma_1 m_1 \sim_i \beta_2 + \gamma_2 m_2 \wedge z = \beta_i + \gamma_i m_i$$

where $\sim_1$ is $\le$, and $\sim_2$ is $\ge$. Notice that each case reduces to a formula of $\mathfrak{D}[m]$, with $m = m_1$ (m_2), by expressing m_2 (m_1) as a linear function of m_1 (m_2). $\square$

Intuitively, the parameter m occurring in the formula $\phi_A \in \mathfrak{D}[m]$ 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 $\mathrm{FCA}(p,1)$.

However, for an arbitrary number of loops, one needs the full expressivity of Diophantine systems, in order to encode the reachability problem. In the light of Hilbert's Tenth Problem [9], the following Lemma entails undecidability of the reachability problem for parametric FCA with unrestricted number of loops.

Lemma 10 *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 $\langle q_0, \mathbf{0z} \rangle \to \ldots \to \langle q, \mathbf{yz} \rangle$*

Proof: The system $S(\mathbf{x})$ is a set of equations of the form $P(\mathbf{x}) = 0$, with $P \in \mathbb{Z}[\mathbf{x}]$. We transform each such equation in a system $T(\mathbf{y})$, by introducing new variables, as follows. Start with $\mathbf{y} = \mathbf{x}$ and $T = \emptyset$. Then iterate the following steps:

- choose one subterm t of the form $y_i \circ y_j$, $\circ \in \{+, \cdot\}$ and two variables $z, z' \notin \mathbf{y}$,
- $S \leftarrow S[z/t]$, $T \leftarrow T \cup \{y_i \circ z = z',\ y_j = z\}$, and $\mathbf{y} \leftarrow \mathbf{y} \cup \{z, z'\}$.

until a fixpoint is reached. It is easy to check that, for all $\mathbf{x} \in \mathbb{Z}$, $\models S(\mathbf{x})$ if and only if there exist integer values $\mathbf{y} \setminus \mathbf{x}$ such that $\models T(\mathbf{y})$. For a suitable indexing of the set $\mathbf{y} = \{y_1, y_2, \ldots\}$, T has only equations of the form (1) $y_i \cdot y_j = y_k$, (2) $y_i + y_j = y_k$ where $i < j < k$.

Now we build a parametric FCA $A = \langle \{x_1, x_2\}, \mathbf{y}, Q, \delta, q_0 \rangle$ with two working counters, and the set of parameters same as the set of the variables of $T(\mathbf{y})$. Note that we have $\mathbf{x} \subseteq \mathbf{y}$, from the construction of T. For every equation of the form (1) we have a control loop $q_1 \xrightarrow{\varphi_1} q_2$, $q_2 \xrightarrow{\varphi_2} q_2$ and $q_2 \xrightarrow{\varphi_3} q_3$, where:

- the entry relation is $\varphi_1 : x_1' = y_i \ \wedge\ x_2' = 0$
- the loop relation is $\varphi_2 : x_1' = x_1 - 1 \ \wedge\ x_2' = x_2 + y_j \ \wedge\ x_2 > 0$
- the exit relation is $\varphi_3 : x_1 = 0 \wedge x_2 = y_k$

For equations of type (2) we introduce a similar loop, the only exception being the loop relation, which is $\varphi_2 : x_1' = x_1 - 1 \ \wedge\ x_2' = x_2 + 1 \ \wedge\ x_2 > 0$ in this case. A is flat by construction, and let q be the last state of type q_3, in the loop construction above. It is easy to check now that $T(\mathbf{y})$ has a solution if and only if A has a run ending in $\langle q, \mathbf{xy} \rangle$. $\square$

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 $D \geq 4 \wedge V \geq 2 \vee D \geq 2 \wedge V \geq 9$ [19]. 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 [10], using a property of reversal bounded counter machines. Another proof has been suggested to us by Y. Matiyasevich [17], using a more involved case analysis. Our proof is based on a result of L. Pottier [20], quoted by Theorem 1.

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.[3] 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 [20]:

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 $A(m_0)$.*

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 $x_i \leq m_0^{(K+3)r+1}$.*

Proof: We have $a_{ij}(m_0) \leq Cm_0^K + Cm_0^{K-1} + \ldots + C = C\frac{m_0^{K+1}-1}{m_0-1} \leq m_0^{K+1}$, and therefore $\sum_{i,j} a_{ij} \leq nr \cdot m_0^{K+1} \leq m_0^{K+3}$. Since $0 < r_0 \leq r$, we have $(n - r_0)\left(\frac{\sum_{i,j} a_{ij}}{r_0}\right)^{r_0} \leq n\left(\frac{\sum_{i,j} a_{ij}}{r_0}\right)^{r} \leq n\left(\frac{m_0^{K+3}}{r_0}\right)^{r} \leq n(m_0^{K+3})^r \leq m_0^{(k+3)r+1}$. By Theorem 1, we obtain the result. $\square$ 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

[3] 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 $m, x_1, \ldots, x_n$.

have:

$$
\begin{aligned}
(f)_m = (d)_m + (e)_m &\iff \bigvee_{\mathbf{r}\in\{0\}\times\{0,1\}^{k-1}\times\{0\}} \bigwedge_{i=0}^{M} \delta_i + \varepsilon_i + r_i = \phi_i + m r_{i+1} \\
(e)_m = c(d)_m &\iff \bigvee_{\mathbf{r}\in\{0\}\times\{0,\ldots,c-1\}^{k-1}\times\{0\}} \bigwedge_{i=0}^{M} c\delta_i + r_i = \varepsilon_i + m r_{i+1} \\
(e)_m = m(d)_m &\iff \delta_M = \phi_0 = 0 \wedge \bigwedge_{i=0}^{M-1} \delta_i = \phi_{i+1}
\end{aligned}
$$

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 $A(m)\mathbf{x} = \mathbf{0}$.

Example Consider the equation: $1 \cdot x_1 + m \cdot x_2 = m^2 + 2$. By Corollary 1 we should have considered the case $m \geq 6$, however the following is true even for $m \geq 3$: $(1)_m \cdot x_1 + (10)_m \cdot x_2 = (102)_m$. We look for solutions of the form $x_1 = (a_2 a_1 a_0) m$ and $x_2 = (b_1 b_0)_m$, and therefore, our equation is equivalent to: $(a_2 a_1 a_0)_m + (b_1 b_0 0)_m = (102)_m$. This is reduced to the following two systems:

$$
\left\{ \begin{array}{rcl} a_0 &=& 2 \\ a_1 + b_0 &=& 0 \\ a_2 + b_1 &=& 1 \end{array} \right.
\qquad\qquad
\left\{ \begin{array}{rcl} a_0 &=& 2 \\ a_1 + b_0 &=& m \\ a_2 + b_1 + 1 &=& 1 \end{array} \right.
$$

from which we get the set of all solutions (x_1, x_2): $\{((102)_m, (0)_m), ((2)_m, (10)_m)\} \cup \{((c\ 2)_m, (m - c\ 0)_m) \mid 1 < c < m\}$ $\square$

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.*

Proof: Let $A(m)\mathbf{x} = B(m)$ (1) be the original (non-homogeneous) system, where $\mathbf{x} = \langle x_1, \ldots, x_n \rangle$, $\mathbf{x}' = \langle x_1, \ldots, x_n, x_{n+1} \rangle$, and $A'(m)\mathbf{x}' = 0$ (2) be the homogeneous system $A(m)\mathbf{x} = B(m) x_{n+1}$. Also let S and S' be the sets of non-trivial solutions of the systems (1) and (2). It is sufficient to show the following: $S \neq \emptyset$ iff S' has a minimal element with x_{n+1}. Since the latter is decidable (by adding the condition $x_{n+1} = 1$ to the Presburger systems derived using the m base representation), we obtain the result.

"$\Leftarrow$" Any solution of (2) with $x_{n+1} = 1$ is a solution of (1).

"$\Rightarrow$" Let $\mathbf{x_0'} = \min\{\mathbf{x}' \text{ solution of (2)} \mid x_{n+1} = 1\}$ Obviously, $\mathbf{x_0'} \in S'$. Suppose that $\mathbf{x_0'}$ is not a minimal element of S', i.e. there exists some $\mathbf{x}'' \in S'$ such that $\mathbf{x}'' \leq \mathbf{x_0'}$, and $x_j'' > 0$ for some $1 \leq j \leq n+1$. But $\mathbf{x}'' \leq \mathbf{x_0'}$ implies $x'_{0n+1} = 0$, and $x_i'' \leq x'_{0i}$, for all $1 \leq i \leq n$. Therefore $x_j'' > 0$, for some $1 \leq j \leq n$, and $\mathbf{x_0'} - \mathbf{x}'' \in S'$. But $\mathbf{x_0'} - \mathbf{x}'' < \mathbf{x_0'}$, contradicting the choice of $\mathbf{x_0'}$. So, $\mathbf{x_0'}$ is a minimal element of S'. $\square$ 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 13, which entails the undecidability of the reachability problem for $\mathrm{FCA}(p,n)$ with $p > 0$ parameters, and sufficiently many control loops.

6 From Integer Arithmetic to FCA

This section is dedicated to the reductions between classes of FCA and the theories $\langle \mathbb{Z}, \geq, +, 0, 1\rangle$, $\langle \mathbb{Z}, \geq, +, |, 0, 1\rangle^{\exists}$ and $\mathfrak{D}[n]$. We distinguish the FCA according to the number of parameters, and the form of the transition relations. In general, we reduce a class C of FCA to an arithmetic theory T, by defining, for each automaton $M \in C$, its set of values $\mathcal{V}(M)$ in T. The dual direction is handled symmetrically.

The first class, denoted by FCA$(0,n)$, consists of counter automata with no parameters. The direction FCA$(0,n) \longrightarrow \langle \mathbb{Z}, \geq, +, 0, 1\rangle$ is a direct consequence of the fact that, for any counter automaton $M \in$ FCA$(0,n)$, the set $\mathcal{V}(M)$ is definable in Presburger arithmetic, as was proved earlier. The direction $\langle \mathbb{Z}, \geq, +, 0, 1\rangle \longrightarrow$ FCA$(0,n)$, is handled by the following Lemma:

Lemma 11 *For any formula $\varphi(\mathbf{x})$ in the language of $\langle \mathbb{Z}, \geq, +, 0, 1\rangle$, there exists an automaton $M \in$ FCA$(0,n)$ such that $\mathcal{V}(M) = \{\mathbf{v} \in \mathbb{Z}^{\|\mathbf{x}\|} \mid \models \varphi(\mathbf{v})\}$.*

Proof: If $\models \varphi(\mathbf{x}) \leftrightarrow \bot$, the machine M corresponding to φ has a final state that is unreachable, i.e. $\mathcal{V}(M) = \emptyset$. Otherwise, φ can be effectively written in the equivalent semilinear form, as a finite disjunction of formulae of the form $\mathbf{x} = \mathbf{a_0} + \sum_{i=1}^{n} \mathbf{a_i}\lambda_i$, where $\mathbf{a_i} \in \mathbb{Z}^{\|\mathbf{x}\|}$, $0 \leq i \leq n$ and $\lambda_1, \ldots, \lambda_n$ are fresh variables. The automaton corresponding to φ is composed of disjoint linear flat counter automata, one for each disjunct in the semilinear form of φ, and defined as follows. All LFCA have in common only the initial state. Then, for each term $\mathbf{a_0}$, we have a transition from the initial state to the first state of the LFCA, which is also a 2-branching state, and the transition relation is $\mathbf{x}' = \mathbf{x} + \mathbf{a_0}$. Finally, for any term of the form $\mathbf{a_i}\lambda_i$, the LFCA has a self-loop with a transition relation $\mathbf{x}' = \mathbf{x} + \mathbf{a_i}$. All loops are linked by transitions of the form $\mathbf{x} = \mathbf{x}'$. $\square$

Remark In fact one can also show that the classes FCA$(0,n)$ and CM(k,r,l) are directly inter-reducible, i.e. without the intermediate of Presburger arithmetic. The direction CM$(k,r,l) \longrightarrow$ FCA$(0,n)$ has been proved in [15]. For the dual direction FCA$(0,n) \longrightarrow$ CM(k,r,l), we can see the even/odd automata as a one-way 2-counter machines, in which one (unrestricted) counter sums up the weight of a path, and the other (0-bounded) counter increases at each step, in order to measure the length of the path. These machines have been shown to be equivalent to the r-bounded counter machines, in [12]. $\square$

The second class, denoted by FCA1A(p,n), is obtained by restricting the transition relations on the loops to formulae of the form $x'_i \leq x_j + p \wedge x_k \leq x'_i + q \wedge \bigwedge_{j \neq i} x'_j = x_j \wedge \phi(\mathbf{x}) \wedge \psi(\mathbf{x}')$ where ϕ, ψ are affine formulae. The reductions FCA1A$(p,n) \longleftrightarrow \langle \mathbb{Z}, \geq, +, |, 0, 1\rangle^{\exists}$ are handled by the following Lemma:

Lemma 12 *For any formula $\varphi(\mathbf{x})$ in the language of $\langle \mathbb{Z}, \geq, +, |, 0, 1\rangle^{\exists}$, there exists an automaton $M \in$ FCA1A(p,n) such that $\mathcal{V}(M) = \{\mathbf{v} \in \mathbb{Z}^{\|\mathbf{x}\|} \mid \models \varphi(\mathbf{v})\}$. Dually, for any automaton $M \in$ FCA1A(p,n) there exists a formula $\varphi(\mathbf{x})$ in the language of $\langle \mathbb{Z}, \geq, +, |, 0, 1\rangle^{\exists}$, such that $\mathcal{V}(M) = \{\mathbf{v} \in \mathbb{Z}^{\|\mathbf{x}\|} \mid \models \varphi(\mathbf{v})\}$.*

Proof: "$\longrightarrow$" We show how to translate a relation of the form $f(\mathbf{x}) \mid g(\mathbf{x})$, where f and g are linear functions on $\mathbf{x}$. First, the values of the functions are computed using two separate counters, i.e. $y = f(\mathbf{x})$ and $z = g(\mathbf{x})$. Notice that this can be done using a flat control structure, with only one assignment per loop. Then the automaton guesses the value of y using a parameter p, by testing $y = p$. In order to ensure that $p|z$, the automaton uses another loop with the transition relation whose only assignment is $z' = z - p$, and an exit transition with condition $z = 0$, that leads to the accepting state.

"$\Longleftarrow$" Notice that the constraint graph corresponding to the loop relation consists of horizontal edges of weight zero, corresponding to the constraints $x'_j = x_j$, vertical edges generated by the constraints in $\phi(\mathbf{x}) \wedge \psi(\mathbf{x}')$, and at most one oblique edge for $x'_i \sim x_j + p$. As a consequence, the execution graph corresponding to n unfoldings of the loop will have at most one path connecting the nodes x^0_j and x^n_i, of weight $(p+c)n$, for some constant $c \in \mathbb{Z}$, depending on the relation. The existence of such a path entails an input-output relation of the form $\exists n\, x'_i \sim x_j + (p+c)n \wedge \bigwedge_{j \neq i} x'_j = x_j \wedge \phi(\mathbf{x}) \wedge \psi(\mathbf{x}')$ independently, for each loop of M. However, each such relation can be expressed in the language of $\langle \mathbb{Z}, \geq, +, |, 0, 1 \rangle^{\exists}$, e.g. $\exists n\, x'_i \leq x_j + (p+c)n \iff \exists y\, y \geq 0 \wedge p + c | x'_i + y - x_j$. $\Box$

The reduction $\mathrm{FCA}(p,n) \longrightarrow \mathfrak{D}[n]$ is a direct consequence of the fact that, for any $M \in \mathrm{FCA}(p,n)$, that consists of only one self-loop, the set $\mathcal{V}(M)$ is defined by a formula of $\mathfrak{D}[1]$. The reduction $\mathfrak{D}[n] \longrightarrow \mathrm{FCA}(p,m)$, for $m \geq n$, is proved in the following Lemma:

Lemma 13 *For any formula $\varphi(\mathbf{x})$ in the language of $\mathfrak{D}[n]$, there exists an automaton $M \in FCA(p,m)$, for some $m \geq n$ such that $\mathcal{V}(M) = \{\mathbf{v} \in \mathbb{Z}^{\|\mathbf{x}\|} \mid\ \models \varphi(\mathbf{v})\}$.*

Proof: By the definition of $\mathfrak{D}[n]$, φ is a finite disjunction of parametric linear Diophantine systems, consisting of equations of the form (3). Notice that each such equation can be reduced to a system in which all polynomials p_i, q_i are of degree one, by introducing new variables. For instance, if $x_{1,2}$ are variables and $z_{1,2}$ are parameters, the equation $x_1 = z_1^2 z_2 \cdot x_2$ is equivalent to the system:

$$\begin{cases} x_1 &= z_1 \cdot y_1 \\ y_1 &= z_1 \cdot y_2 \\ y_3 &= z_2 \cdot x_2 \end{cases}$$

where y_1, y_2, y_3 are fresh variables. We can assume w.l.o.g. that $\varphi(\mathbf{x})$ is in this form. In order to build an automaton $M \in \mathrm{FCA}(p,m)$ such that $\mathcal{V}(M) = \{\mathbf{v} \in \mathbb{Z}^{\|\mathbf{x}\|} \mid\ \models \varphi(\mathbf{v})\}$, it is sufficient to encode the relations of the form (1) $x_1 = z \cdot x_2$ and (2) $x_1 = x_2 + x_3$. Each such relation will be encoded by a loop, using counters $x_{1,2,3}$ and an extra counter y. For (1) we initialize $x'_1 = 0 \wedge y' = x_2$. The transition relation of the loop is $x'_1 = x'_1 + z \wedge y' = y' - 1 \wedge y > 0$, and the exit condition is $y = 0$. For (2) we initialize $x'_1 = x_2 \wedge y' = x_3$. The transition relation of the loop is $x'_1 = x_1 + 1 \wedge y' = y - 1 \wedge y > 0$ and the exit condition is $y = 0$. Notice that the number of loops needed for M is greater or equal than the number of parameters in φ. $\Box$

7 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.

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. 1

[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. 1

[3] B. Boigelot. On iterating linear transformations over recognizable sets of integers. *TCS*, 309(2):413–468, 2003. 1, 1.1

[4] Alonzo Church. An unsolvable problem of elementary number theory. *American Journal of Mathematics*, 58:345 – 363, 1936. 3

[5] Hubert Comon and Yan Jurski. Multiple Counters Automata, Safety Analysis and Presburger Arithmetic. In *Proc. CAV*, volume 1427 of *LNCS*, pages 268 – 279. Springer, 1998. (document), 1, 1.1, 4.3, 7

[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. 1, 1.1

[7] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38:173 – 198, 1931. 3

[8] E. M. Gurari and O. H. Ibarra. Two-way counter machines and diophantine equations. *Journal of the Association for Computing Machinery*, 29(3):863–873, July 1982. 3, 3, 3

[9] David 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. (document), 3, 4.3

[10] O. H. Ibarra and Z. Dang. On the solvability of a class of diophantine equations and applications. Submitted, 2005. 1.1, 3, 5

[11] O. H. Ibarra, T. Jiang, N. Tran, and H. Wang. New decidability results concerning two-way counter machines. *SIAM J. Comput.*, 24(1):123–137, February 1995. 3

[12] O. H. Ibarra, J. Su, Z. Dang, T. Bultan, and R. Kemmerer. Counter machines and verification problems. *TCS*, 289:165 – 189, 2002. 6

[13] Oscar H. Ibarra. Reversal-bounded multicounter machines and their decision problems. *Journal of the Association for Computing Machinery*, 25(1):116 – 133, January 1978. 1, 1.1, 2, 1, 3, 3

[14] J. Leroux and G. Sutre. On flatness for 2-dimensional vector addition systems with states. In *Proc. CONCUR*, volume 3170 of *LNCS*, pages 402–416. Springer, 2004. 2

[15] J. Leroux and G. Sutre. Flat counter automata almost everywhere! In *Proc. ATVA*, volume 3707 of *LNCS*, pages 489–503. Springer, 2005. 6

[16] Yuri Matiyasevich. Enumerable sets are diophantine. *Journal of Sovietic Mathematics*, 11:354 – 358, 1970. 1, 3

[17] Yuri Matiyasevich. Personal communication, 2005. 1.1, 5

[18] M. Minsky. *Computation: Finite and Infinite Machines*. Prentice-Hall, 1967. 1.1

[19] T. Pheidas and K. Zahidi. Undecidability of existential theories of rings and fields: A survey. *Contemporary Mathematics*, 270:49–106, 2000. 5

[20] Loïc Pottier. Solutions minimales des systemes diophantiens lineaires: bornes et algorithmes. Technical Report 1292, INRIA Sophia Antipolis, 1990. 5

[21] Mojzesz Presburger. Über die Vollstandigkeit eines gewissen Systems der Arithmetik. *Comptes rendus du I Congrés des Pays Slaves*, Warsaw 1929. 3

[22] B. Rosser. Extensions of some theorems of Gödel and Church. *The Journal of Symbolic Logic*, 1:87 – 91, 1936. 3

[23] 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. 1