Complete Linear Acceleration
for Convex Binary Relations

Jérôme Leroux
LaBRI (CNRS UMR 5800), MVTSI Team, Talence, France.
leroux@labri.fr

Abstract

The verification of an infinite state system often reduce to the computation of its reachability sets. For computing this set, a way consists in computing the exact effect of iterating loops of the systems, called meta-transitions. Sébastien Bardin and Alain Finkel shown in 2004 that up to our knowledge, all the algorithms computing meta-transitions compute in fact a richer structure called acceleration, as an intermediate step. In this paper, we prove that if the acceleration of a rational polyhedral closed convex binary relation is definable in the linear first order theory of the reals and the integers, then it is effectively computable as a linear extrapolation of two powers of the relation.

1 Introduction

The verification of a system can often be reduced to the computation of a precise enough over-approximation of its reachability set. In general, systems are infinite (they either manipulate unbounded variables: integers, clocks, reals, queue contents, and so on, or they are parameterized), and the computation of such an approximation is a difficult problem.

At least two large families of methods have been developed for performing this computation: (1) in the field of abstract interpretation, an over approximation of the reachability set is successively refined until a precise enough approximation is computed. This is for instance the case of predicate abstraction. (2) In the field of symbolic model checking, the system is approximated to a simple enough one (that remains infinite in general in order to keep for instance the important variables that cannot be abstracted into a finite domain) such that the exact computation of the reachability set is possible.

This paper contributes to the second approach (2) for the class of linear hybrid automata (LHA) [AHH96, BJ03]. Informally, a LHA is a finite graph extended with real variables that can exhibit both discrete and continuous behaviors. More formally, the semantics of a transition of a LHA is given as a rational polyhedral closed convex binary relation over real vectors.

As the class of LHA is expressive (for instance, any Minsky machine can be seen as a LHA), the price to pay is the undecidability of reachability properties, and we can only hope for "good" semi-algorithms, where "good" means that the semi-algorithm often terminates in practice even if no guaranty is provided in theory. Naturally, a semi-algorithm that just computes inductively the set of reachable states is not a "good one", because it converges only for very particular cases of LHA. In fact, such a semi-algorithm terminates if and only if any state is reachable by at least one path with a uniformly bounded maximal length. In order to overcome this limitation, this semi-algorithm can be enhanced by providing algorithms to perform meta-transitions corresponding to the computation of the exact effect of some loops of the LHA graph.

In this paper, we study this computation for the symbolic representation based on the linear first order logic of the reals and the integers FO $(\mathbb{R},\mathbb{Z},+,\leq)$. This logic is *powerful* and well adapted for systems that exhibit both *discrete* and *continuous* behaviors such as LHAs. In fact complex sets can be defined by formulas in this logic: linear sets, rational polyhedral closed convex sets, and combinations of these two sets. Moreover, this logic is *decidable*, which means that it can be used to compute solutions of linear equations, or even to compute some fix-points corresponding for instance to the reachability set of counter systems, LHA, timed automata (TA), and more generally systems manipulating either integer variables (counters, parameters, and so on) or real variables (clocks, approximation of floating point numbers).

As the binary relation corresponding to a loop of a LHA graph is a rational polyhedral closed convex binary relation, we have reduced our problem to the computation of a formula in FO $(\mathbb{R},\mathbb{Z},+,\leq)$ representing the reflexive and transitive closure $\mathcal{R}^*$ of a rational polyhedral closed convex binary relation $\mathcal{R}$. Several algorithms have been developed for this computation. In [CJ98], the reachability relation $\mathcal{R}^*$ corresponding to the reflexive and transitive closure of the one step reachability relation $\mathcal{R}$ of a timed automata is proved to be effectively definable in this logic. In [BJ03], an algorithm for binary relations $\mathcal{R}$ satisfying some algebraic conditions is provided. In [BLW04], following a regular model-checking approach, they show that an over-approximation of $\mathcal{R}^*$ can be computed using the RVA symbolic representation, an automata-based representation for a slight extension of FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$.

In this paper, we are interested in unifying these algorithms. Recently, Sébastien Bardin and Alain Finkel shown in [BF04] that up to our knowledge, all the algorithms computing exactly meta-transitions, compute in fact the richer set $\bigcup_{k\in\mathbb{N}} \mathcal{R}^k \times \{k\}$, called *acceleration* of $\mathcal{R}$ as an intermediate step, and next obtain $\mathcal{R}^*$ by eliminating the variable k.

Our contributions:

(1) We provide two semi-algorithms for computing a formula in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ defining the acceleration $\text{acc}(\mathcal{R})$ of a binary relation $\mathcal{R}$ definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$. Whereas the first one is very general but based on an enumerative approach, the second one is restricted to rational polyhedral closed convex binary relations but it is based on a linear extrapolation algorithm.

(2) We prove that these two semi-algorithms are complete: they terminate as soon as the acceleration $\text{acc}(\mathcal{R})$ is definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$. That means, if the acceleration of a binary relation definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ is definable in this logic, then it can be effectively computed thanks to (1).

(3) we show that the acceleration of a binary relation corresponding to a loop of a timed automata, and the acceleration of a binary relation satisfying the criteria given in [BJ03], are both definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$. Therefore formulas in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ defining $\text{acc}(\mathcal{R})$ and $\mathcal{R}^*$ can be effectively computed thanks to (1) and (2).

Plan: In section 2, we recall results about polyhedral closed convex sets and sets definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$. In the next section 3, we recall the flatenning framework that allow the computation of the reachability set of an initialized system thanks to acceleration. We also provide in this section a complete semi-algorithm that computes a formula in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ defining the acceleration of binary relation definable in this logic. In section 4, we provide the definition of linear hybrid automata (LHA), and recall that the semantics of a loop of a LHA corresponds to a rational polyhedral closed convex binary relation. Large classes of binary relations with an acceleration definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ are also provided in this section. Finally in section 5, for the restricted class of rational polyhedral closed convex binary relations, we provide a complete semi-algorithm for computing a formula in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ defining their acceleration thanks to a linear extrapolation algorithm.

2 Linear real spaces

In this section, we recall definitions and properties satisfied by the *linear real spaces*, used in this presentation. Some of this results can be easily derived from [Sch87].

2.1 Notations

Intersection, union, difference and symmetric difference of two sets A and B are written $A \cap B$, $A \cup B$, $A \backslash B$, and $A \Delta B = (A\backslash B) \cup (B\backslash A)$. The set of *functions* from a set X to a set Y, also called *sequences* of elements in Y indexed by X is written Y^X. A function $f \in Y^X$ is also denoted by $f : X \to Y$. For such a function and for any set A and B, we define $f(A) = \{f(a);\ a \in A \cap X\}$ and $f^{-1}(B) = \{x \in X;\ f(x) \in B\}$. We denote by $\mathbb{R}$, $\mathbb{R}_+$, $\mathbb{Q}$, $\mathbb{Q}_+$, $\mathbb{Z}$ and $\mathbb{N}$ respectively the set of real numbers, non-negative real numbers, rational numbers, non-negative rational numbers, integers, and non-negative integers. The class of subsets (resp. finite subsets) of a set A is denoted by $\mathcal{P}(A)$ (resp. $\mathcal{P}_f(A)$). The *cardinality* of a finite set X is written $|X| \in \mathbb{N}$. Given a real $x \in \mathbb{R}$, let us denote by $\lfloor x \rfloor$ the unique integer such that $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$, let us denote by $p_f(x) = x - \lfloor x \rfloor$, and let us denote by $|x| \geq 0$ the absolute value of x.

The set X^m is called the set of vectors with $m \in \mathbb{N}\backslash\{0\}$ components in a set X. Given an integer $i \in \{1, \ldots, m\}$ and a vector $x \in X^m$, the i-th component of x is written $x[i] \in X$. For any $j \in \{1, \ldots, m\}$, vector $\mathbf{e}_j \in \mathbb{R}^m$ is defined by $\mathbf{e}_j[j] = 1$ and $\mathbf{e}_j[i] = 0$ for any $i \in \{1, \ldots, m\}\backslash\{j\}$. We denote by $\mathbf{e}_0$ the vector $\mathbf{e}_0 = (0, \ldots, 0)$. Vectors $x + y$ and $t.x$ are defined by $(x + y)[i] = (x[i]) + (y[i])$ and $(t.x)[i] = t.(x[i])$ for any $i \in \{1, \ldots, m\}$, $x, y \in \mathbb{R}^m$, $t \in \mathbb{R}$. For any $x \in \mathbb{R}^m$, let us consider the norm $||x||_\infty = \max_i |x[i]|$. We denote by $\langle x, y\rangle = \sum_{i=1}^m x[i].y[i]$, the *dot product* of two vectors $x, y \in \mathbb{R}^m$. We naturally define $A + B = \{a + b;\ (a, b) \in A \times B\}$ and $T.A = \{t.a;\ (t, a) \in T \times A\}$ for any $A, B \subseteq \mathbb{R}^m$ and $T \subseteq \mathbb{R}$. For any $a, b \in \mathbb{R}^m$ and $t \in \mathbb{R}$, let us define $a + B = \{a\} + B$, $A + b = A + \{b\}$, $t.A = \{t\}.A$ and $T.a = T.\{a\}$.

2.2 Polyhedral closed convex sets

The *open ball* centered in $x \in \mathbb{R}^m$ with a radius $\epsilon > 0$ is the subset $B_{x,\epsilon} = \{y \in \mathbb{R}^m;\ ||x - y||_\infty < \epsilon\}$. Recall that a subset $X \subseteq \mathbb{R}^m$ is said *open* if for any $x \in X$ there exists $\epsilon > 0$ such that $B_{x,\epsilon} \subseteq X$. A *closed set* X is a subset of $\mathbb{R}^m$ such that difference $\mathbb{R}^m \backslash X$ is open. Recall that any finite or infinite intersection of closed sets is closed. In particular, any set $X \subseteq \mathbb{R}^m$ is included into a minimal (for the inclusion) closed set $\mathrm{cl}(X)$.

A vector $v = \sum_{i=1}^{n} t_i.v_i$ where $t_1, ..., t_n \in \mathbb{R}$ and $v_1, ..., v_n$ are some vectors in a subset $V \subseteq \mathbb{R}^m$ is called a *linear combination* in V. Such a combination is said to be: (1) *conic*, if $t_i \in \mathbb{R}_+$; (2) *affine*, if $\sum_{i=1}^{n} t_i = 1$; (3) *convex*, if it is both conic and affine. An *affine space A of* $\mathbb{R}^m$ is a subset of $\mathbb{R}^m$ stable by affine combinations of vectors in A, and a *convex set C of* $\mathbb{R}^m$ is a subset of $\mathbb{R}^m$ stable by convex combinations of vectors in C. Recall that the class of affine spaces and closed convex sets are stable by finite and infinite intersection. In particular, any set $X \subseteq \mathbb{R}^m$ is included into a minimal (for $\subseteq$) affine space $\mathrm{aff}(X)$ and convex set $\mathrm{conv}(X)$. Recall also that the closure of a convex set remains a convex set. The *direction* $\overrightarrow{A}$ of an affine space A is the affine space $\overrightarrow{A} = A - A$.

The following lemma will be useful in the sequel.

Lemma 2.1 *Let C be a convex set and $\mathcal{C}$ be a non-empty finite class of affine spaces such that $C \subseteq \bigcup_{A \in \mathcal{C}} A$. There exists $A \in \mathcal{C}$ such that $C \subseteq A$.*

Proof : Let us consider a convex set C and let us prove by induction over $n \in \mathbb{N}\backslash\{0\}$ that for any non-empty finite set $\mathcal{C}$ of affine spaces such that $C \subseteq \bigcup_{A \in \mathcal{C}} A$ and $|\mathcal{C}| = n$, there exists $A \in \mathcal{C}$ such that $C \subseteq A$. Naturally the case $n = 1$ is immediate. Assume that the induction hypothesis is true for an integer $n \in \mathbb{N}\backslash\{0\}$ and let us consider a non-empty finite set $\mathcal{C}$ of affine spaces such that $C \subseteq \bigcup_{A \in \mathcal{C}} A$ and $|\mathcal{C}| = n+1$. Let us consider $A \in \mathcal{C}$. The case $C \subseteq A$ is immediate so we can assume that $C \not\subseteq A$. Let us consider $\mathcal{C}' = \mathcal{C}\backslash\{A\}$. As $C \not\subseteq A$, there exists $a_0 \in C\backslash A$. Let $a_1 \in C$ and remark that C convex implies $a_t = a_0.(1-t) + t.a_1 \in C$ for any $0 \leq t \leq 1$. By definition of $\mathcal{C}$, we deduce that for such a real $t \in \mathbb{R}$, there exists $A_t \in \mathcal{C}$ such that $a_t \in A_t$. As the set of $t \in \mathbb{R}$ such that $0 \leq t \leq 1$ is infinite whereas $\mathcal{C}$ is finite, there exists $A' \in \mathcal{C}$ and two different $0 \leq t \leq 1$ such that $a_t \in A'$. As A' is an affine space, we deduce that $a_t \in A'$ for any t, and in particular $a_0, a_1 \in A'$. From $a_0 \in A'$ and $a_0 \notin A$, we deduce that $A' \in \mathcal{C}'$, and we have proved that $a_1 \in \bigcup_{A' \in \mathcal{C}'} A'$. We have proved that $C \subseteq \bigcup_{A' \in \mathcal{C}'} A'$. From $|\mathcal{C}'| = n$, the induction proves that there exists $A'' \in \mathcal{C}'$ such that $C \subseteq A''$. We have proved the induction hypothesis for $\mathcal{C}$. We are done. $\square$

A *closed half-space* H of an affine space A is a subset of A of the form $H = H_{A,\alpha,\#,c}$ where $H_{A,\alpha,\#,c} = \{x \in A;\ \langle \alpha, x \rangle \# c\}$ where $(\alpha, \#, c) \in (\overrightarrow{A}\backslash\{\mathbf{e}_0\}) \times \{\leq, \geq\} \times \mathbb{R}$ (see figure 1). Given such an half-space $H = H_{A,\alpha,\#,c}$,

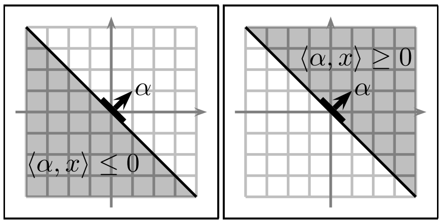

Figure 1. Let $A = \mathbb{R}^2$, $\alpha = (1, 1)$. On the left $H_{A,\alpha,\leq,0}$. On the right $H_{A,\alpha,\geq,0}$.

we denote by $H^=$ the affine space $H^= = H_{A,\alpha,=,c}$ and we denote by H^{-1} and $\overrightarrow{H}$ respectively the closed half-space $H^{-1} = H_{A,-\alpha,\#,-c}$ and $\overrightarrow{H} = H_{\overrightarrow{A},\alpha,\#,0}$. Naturally, $H^=$, H^{-1} and $\overrightarrow{H}$ only depends on H and not on a couple $(A, \alpha, \#, c)$ defining H.

Recall that a subset $X \subseteq \mathbb{R}^m$ is a closed convex set of $\mathbb{R}^m$ if and only if it is equal to a *finite or infinite* intersection of closed half-spaces of $\mathbb{R}^m$. A *polyhedral closed convex set* C is a finite intersection of closed half-spaces. The following lemma 2.2 recall that there exists a unique minimal (for $\subseteq$) finite set $\mathcal{H}(C)$ of closed half spaces of $\mathrm{aff}(C)$, called the *set of constraints of* C, such that $C = \mathrm{aff}(C) \cap \bigcap_{H \in \mathcal{H}(C)} H$.

Lemma 2.2 *Let C be a polyhedral closed convex set, $A = \mathrm{aff}(C)$ be its affine hull, and $\mathcal{H}(C)$ be the class of closed half-spaces H of A such that $C \subseteq H$ and $\mathrm{aff}(C \cap H^=) = H^=$. Then $\mathcal{H}(C)$ is the minimal (for the inclusion) finite class of closed half-spaces $\mathcal{H}$ of A such that $C = A \cap \bigcap_{H \in \mathcal{H}} H$.*

Proof : Let C be a polyhedral closed convex set and let $A = \mathrm{aff}(C)$. Naturally, if $A = \emptyset$ we are done. So, we can assume that $A \neq \emptyset$.

Let us first prove that there exists a finite sequence $((\alpha_i, c_i))_{i \in I}$ of couples in $(\overrightarrow{A}\backslash\{\mathbf{e}_0\}) \times \mathbb{R}$ such that $C = A \cap \bigcap_{i \in I} H_{A,\alpha_i,\leq,c_i}$. As C is a polyhedral closed convex set, there exists a finite sequence $(A_j, \alpha'_j, \#_j, c'_j)_{j \in J}$ of tuples such that A_j is an affine space, $(\alpha'_j, c'_j) \in (\overrightarrow{A_j}\backslash\{\mathbf{e}_0\}) \times \mathbb{R}$, and $\#_j \in \{\leq, \geq\}$ such that $C = \mathbb{R}^m \cap \bigcap_{j \in J} H_{A_j,\alpha'_j,\#_j,c'_j}$. From $C \subseteq A$, we deduce that $C = C \cap A$ and in particular $C = A \cap \bigcap_{j \in J} (A \cap H_{A_j,\alpha'_j,\#_j,c'_j})$. By replacing (α'_j, c'_j) by $(-\alpha'_j, -c'_j)$, we can assume that $\#_j$ is equal to $\leq$. Moreover, as $C \subseteq A_j$, we get $A = \mathrm{aff}(C) \subseteq A_j$ and in particular $A \cap A_j = A$ and we deduce that $A \cap H_{A_j,\alpha'_j,\leq,c'_j} = \{x \in A;\ \langle \alpha'_j, x \rangle \leq c'_j\}$. Thanks to the *orthogonal projection*, we deduce that there exists $\alpha_j \in \overrightarrow{A}$ such that $\langle \alpha'_j, v \rangle = \langle \alpha_j, v \rangle$ for any $v \in \overrightarrow{A}$. Let us consider $x_0 \in A$ (recall that

$A \neq \emptyset$). We have $\langle \alpha'_j, x\rangle = \langle \alpha'_j, (x - x_0) + x_0\rangle = \langle \alpha_j, x - x_0\rangle + \langle \alpha'_j, x_0\rangle = \langle \alpha_j, x\rangle + \langle \alpha'_j - \alpha_j, x_0\rangle$. Hence $A \cap H_{A_j,\alpha_j,\leq,c'_j} = \{x \in A;\ \langle \alpha_j, x\rangle \leq c_j\}$ where $c_j = c'_j - \langle \alpha'_j - \alpha_j, x_0\rangle$. Remark that if $\alpha_j = \mathbf{e}_0$ then this set is equal to A (because C is not empty from $A \neq \emptyset$). Therefore $C = A \cap \bigcap_{i\in I} H_{A,\alpha_i,\leq,c_i}$ where I is the set of $i \in J$ such that $\alpha_i \neq \mathbf{e}_0$. We are done.

Let $(\alpha, c) \in (\overrightarrow{A}\backslash\{\mathbf{e}_0\}) \times \mathbb{R}$ and let $((\alpha_i, c_i))_{i\in I}$ a sequence of couples in $(\overrightarrow{A}\backslash\{\mathbf{e}_0\}) \times \mathbb{R}$ such that $C = A \cap \bigcap_{i\in I} H_{A_i,\alpha_i,\leq,c_i}$. We denote by H the closed half-space $H = H_{A,\alpha,\leq,c}$ and $H_i = H_{A,\alpha_i,\leq,c_i}$.

We first prove that there exists a vector $x_0 \in A$ such that $\langle \alpha_i, x_0\rangle < 0$ for any $i \in I$. Remark that $C \subseteq \mathrm{aff}(A \cap \bigcap_{i\in I}(H_i\backslash H_i^=)) \bigcup_{i\in I} H_i^=$, from lemma 2.1, we deduce that either $C \subseteq \mathrm{aff}(A \cap \bigcap_{i\in I}(H_i\backslash H_i^=))$ of there exists $i \in I$ such that $C \subseteq H_i^=$. The last case is not possible because otherwise we get $A = \mathrm{aff}(C)$ is included into $H_i^=$. Hence from the first case, we deduce that $A \cap \bigcap_{i\in I}(H_i\backslash H_i^=)$ is not empty an in particular there exists a vector x_0 in this set.

Now, let us prove that if $H \in \mathcal{H}(C)$ then there exists $i \in I$ such that $H = H_i$. Let $x \in C \cap H^=$. For any $i \in I$, we have $\langle \alpha_i, x_i\rangle = c_i$. Let us consider the vector $y_\epsilon = x + \epsilon.\alpha$ where $\alpha \in \mathbb{R}$. Remark that $\langle \alpha, y_\epsilon\rangle > \langle \alpha, x\rangle = c$ for any $\epsilon > 0$. From $C \subseteq H$, we deduce that $y_\epsilon \in A\backslash C$. Hence, for any $\epsilon > 0$, there exists $i \in I$ such that $\langle \alpha_i, y_\epsilon\rangle > c_i$. In particular $y_\epsilon \in \bigcup_{i\in I}\{y \in A;\ \langle \alpha_i, y\rangle = 0\}$ for any $\epsilon > 0$. As this set is closed, we deduce that x is also in this set (as a limit of elements in this set). Hence $C \cap H^= \subseteq \bigcup_{i\in I} H_i^=$. From lemma 2.1, we deduce that there exists $i \in I$ such that $C \cap H^= \subseteq H_i^=$. From $H^= = \mathrm{aff}(C \cap H^=)$, we deduce that $H^= \subseteq H_i^=$. As H and H_i are two half-spaces of A, we get $H^= = H_i^=$. Hence $H_i = H$ or $H_i = H^{-1}$. Just remark that if $H_i = H^{-1}$, then $H \cap H_i = H^=$. In particular, from $C \subseteq H$ and $C \subseteq H_i$, we deduce that $C \subseteq H^=$ which is in contradiction with $\mathrm{aff}(C) = A$. Hence $H = H_i$.

Next, let us prove that if $i_0 \in I$ is such that $H_{i_0} \notin \mathcal{H}(C)$, then $C = A \cap \bigcap_{i\in I'} H_i$ where $I' = I\backslash\{i_0\}$. Remark that $C \subseteq H_{i_0}$ and from $H_{i_0} \notin \mathcal{H}(C)$, we deduce that $\mathrm{aff}(C \cap H_{i_0}^=)$ is strictly included in $H_{i_0}^=$. In particular, there exists a vector $v \in \overrightarrow{H_{i_0}^=}\backslash\overrightarrow{\mathrm{aff}}(C \cap H_{i_0}^=)$. Assume by contradiction that there exists $x_1 \in A \cap \bigcap_{i\in I'} H_i\backslash H_{i_0}$. As $\langle \alpha_i, x_0\rangle < c_i$, there exists $\epsilon > 0$ such that for any $t \in \mathbb{R}$ satisfying $0 \leq t \leq \epsilon$, we have $\langle \alpha_i, x_0 + t.v\rangle \leq c_i$ for any $i \in I$. Let $z_t = \frac{1}{\langle \alpha_{i_0}, x_1 - x_0\rangle}.((c_{i_0} - \langle \alpha_{i_0}, x_0\rangle).x_1 + (\langle \alpha_{i_0}, x_1\rangle - c_{i_0}).(x_0 + t.v))$. And remark that z_t is a convex combination of x_1 and $x_0 + t.v$. In particular $z_t \in A \cap \bigcap_{i\in I'} H_i$. Moreover, the computation of $\langle \alpha_{i_0}, z_t\rangle$ shows that $z_t \in H_{i_0}^=$. Therefore $z_t \in C \cap H_{i_0}^=$, and in particular $z_t \in \mathrm{aff}(C \cap H_{i_0}^=)$ for any $0 \leq t \leq \epsilon$. In particular $\mathbb{Q}.v \in \overrightarrow{\mathrm{aff}}(C \cap H_{i_0}^=)$ which is a contradiction. Therefore $C = A \cap \bigcap_{i\in I'} H_i$.

The two previous paragraphs prove the lemma. □

A polyhedral closed convex set C is said *rational* if it is equal to a finite intersection of $H_{\mathbb{R}^m,\alpha,\#,c}$ where $(\alpha, c) \in (\mathbb{Q}^m\backslash\{\mathbf{e}_0\}) \times \mathbb{Q}$ and $\# \in \{\leq, \geq\}$. Recall that if C is a rational polyhedral closed convex set, then $\mathrm{aff}(C)$ is rational and any $H \in \mathcal{H}(C)$ is rational.

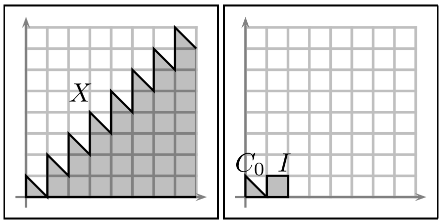

Figure 2. $X = (C_0 + \mathbb{N}.(1,1)) \cup (I + \mathbb{N}.\mathbf{e}_1 + \mathbb{N}.(1,1))$.

2.3 Linear first order theory

A set $X \subseteq \mathbb{R}^m$ is definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ if and only if it is equal to a finite union of sets of the form $C + b + \sum_{p\in P} \mathbb{N}.p$, where $C \subseteq [0, 1[^m$ is definable in FO $(\mathbb{R}, +, \leq)$, $b \in \mathbb{Z}^m$ is called the *basis*, and $P \in \mathcal{P}_f(\mathbb{Z}^m)$ is a finite set of vectors called the set of *periods*. The set $\sum_{p\in P} \mathbb{N}.p$ is also denoted by P^*. Recall also that $\mathrm{cl} \circ \mathrm{conv}(X)$ is a rational polyhedral closed convex set for any set $X \subseteq \mathbb{R}^m$ definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$.

Example 2.3 *Let* $X = (C_0 + \mathbb{N}.(1,1)) \cup (I + \mathbb{N}.\boldsymbol{e}_1 + \mathbb{N}.(1,1))$ *be the set represented in figure 2, where* $C_0 = \{x \in \mathbb{R}^2;\ x[1] \geq 0 \wedge x[2] \geq 0 \wedge x[1] + x[2] \leq 1\}$ *and* $I = \{x \in \mathbb{R}^2; 1 \leq x[1] \leq 2 \wedge 0 \leq x[2] \leq 1\}$. *Remark that* X *is definable in FO* $(\mathbb{R}, \mathbb{Z}, +, \leq)$.

3 Flatenning and Acceleration

In this section, the flatenning framework for computing the reachability set of an initialized system thanks to acceleration is recalled.

3.1 Notations

An *alphabet* Σ is a finite set. Given an alphabet Σ, we denote by Σ^+ the set of non-empty *words* over Σ. Given a non-empty word $\sigma = b_1 \ldots b_k$ of $k \in \mathbb{N}\backslash\{0\}$ elements $b_i \in \Sigma$, and an integer $j \in \{1, \ldots, k\}$, we denote by $\sigma[j] = b_j$. We denote by ϵ the empty word. As usual Σ^* denotes the set of words $\Sigma^+ \cup \{\epsilon\}$ and a *language* $\mathcal{L}$ is a subset of Σ^*. The *concatenation* of $\sigma_1 \in \Sigma^*$ and $\sigma_2 \in \Sigma^*$ is denoted by $\sigma_1.\sigma_2$. Given a word $\sigma \in \Sigma^*$, we define as usual σ^k where

$k \in \mathbb{N}$ and $\sigma^* = \{\sigma^k;\ k \in \mathbb{N}\}$. The *length* of a word $\sigma \in \Sigma^*$ is denoted by $|\sigma| \in \mathbb{N}$. We also denote by $\Sigma^{\leq n}$ where $n \in \mathbb{N}$ the set of words $\sigma \in \Sigma^*$ such that $|\sigma| \leq n$.

A *graph* G is a tuple $G = (Q, T, \alpha, \beta)$ such that Q is a *finite set of states*, T is a *finite set of transitions*, $\alpha, \beta : T \to Q$ are the *source and target functions*. A *path* π in such a graph is a word $\pi \in T^+$ such that there exists $n \in \mathbb{N}\backslash\{0\}$ and a sequence $q_0, t_1, q_1, \ldots, t_n, q_n$ of $n+1$ states $q_i \in Q$ and n transitions $t_i \in T$ such that $\pi = t_1 \ldots t_n$ and such that $(\alpha(t_i), \beta(t_i)) = (q_{i-1}, q_i)$ for any i. The set of paths is denoted by $\Pi(G)$. Given such a path π, we denote by $\alpha(\pi)$ and $\beta(\pi)$ the states q_0 and q_n. A *loop* θ is a path such that $\alpha(\theta) = \beta(\theta)$.

A *relation* $\mathcal{R}$ is a subset of $S_1 \times S_2$ where S_1 and S_2 are two sets. We denote by $s_1 \mathcal{R} s_2$ if $(s_1, s_2) \in \mathcal{R}$. Such a relation is said *one-to-one* if there exists a unique $s_2 \in S_2$ such that $s_1 \mathcal{R} s_2$ for any $s_1 \in S_1$, and if there exists a unique $s_1 \in S_1$ such that $s_1 \mathcal{R} s_2$ for any $s_2 \in S_2$. A *binary relation* $\mathcal{R}$ over a set S is a relation $\mathcal{R} \subseteq S_1 \times S_2$ such that $S_1 = S = S_2$. Given such a binary relation $\mathcal{R}$, we denote by $\mathrm{Post}_{\mathcal{R}} : \mathcal{P}(S) \to \mathcal{P}(S)$ the function defined for any $X \subseteq S$ by $\mathrm{Post}_{\mathcal{R}}(X) = \{s' \in S;\ \exists x \in X;\ x \mathcal{R} s'\}$. The *concatenation* $\mathcal{R}_1.\mathcal{R}_2$ of two binary relations over a set S is the binary relation over S defined by $s \mathcal{R}_1.\mathcal{R}_2 s'$ if and only if there exists $s_i \in S$ such that $s \mathcal{R}_1 s_i$ and $s_i \mathcal{R}_2 s'$. The *identity binary relation* I_S over S is defined by $s I_S s'$ if and only if $s = s'$. Given a binary relation $\mathcal{R}$ over a set S, the sequence $(\mathcal{R}^k)_{k \in \mathbb{N}}$ is uniquely defined by $\mathcal{R}^0$ is the identity binary relation over S, $\mathcal{R}^1 = \mathcal{R}$, and satisfying $\mathcal{R}^{k_1+k_2} = \mathcal{R}^{k_1}.\mathcal{R}^{k_2}$ for any $k_1, k_2 \in \mathbb{N}$. The binary relation $\mathcal{R}^*$ is defined by $\mathcal{R}^* = \bigcup_{k \in \mathbb{N}} \mathcal{R}^k$. Without ambiguity, a function $f : S \to S$ is also seen as the binary relation $\mathcal{R}$ over S defined by $s \mathcal{R} s'$ if and only if $s' = f(s)$. In particular $f^k(X)$, $f^*(X)$, $\mathrm{Post}^k_{\mathcal{R}}(X)$, and $\mathrm{Post}^*_{\mathcal{R}}(X)$ are well defined for any $k \in \mathbb{N}$ and $X \subseteq S$.

3.2 Systems

A *system* is a tuple $\mathcal{S} = (G, S, (\mathcal{R}_t)_{t \in T})$, where $G = (Q, T, \alpha, \beta)$ is a graph, S is a (finite or infinite) set, and $(\mathcal{R}_t)_{t \in T}$ is a sequence of binary relations over S. A *configuration* is an element of $Q \times S$. The sequence $(\mathcal{R}_t)_{t \in T}$ is extended into the unique sequence $(\mathcal{R}_\pi)_{\pi \in \Pi(G)}$ satisfying $\mathcal{R}_{\pi_1.\pi_2} = \mathcal{R}_{\pi_1}.\mathcal{R}_{\pi_2}$ for any $\pi_1, \pi_2 \in \Pi(G)$ such that $\beta(\pi_1) = \alpha(\pi_2)$. The *reachability relation along a path* $\pi \in \Pi(G)$ is the binary relation $\xrightarrow{\pi}$ over the set of configurations defined by $(q, s) \xrightarrow{\pi} (q', s')$ if and only if $(\alpha(\pi), \beta(\pi)) = (q, q')$ and $s \mathcal{R}_\pi s'$. We also denote by $\xrightarrow{\epsilon}$ the identity binary relation over the set of configurations. Given a subset $\rho \subseteq \Pi(G) \cup \{\epsilon\}$, we also denote by $\xrightarrow{\rho}$ the binary relation $\xrightarrow{\rho} = \bigcup_{\pi \in \rho} \xrightarrow{\pi}$. The *global reachability relation* is the binary relation $\xrightarrow{\Pi(G) \cup \{\epsilon\}}$.

An *initialized system* is a tuple $(\mathcal{S}, (q_0, s_0))$ such that $\mathcal{S} = (G, S, (\mathcal{R}_t)_{t \in T})$ is a system, $(q_0, s_0) \in Q_0 \times S$ is the *initial configuration*. The *reachability set of an initialized system* is the following set:

$$\mathrm{Post}_{\xrightarrow{\Pi(G) \cup \{\epsilon\}}}(\{(q_0, s_0)\})$$

3.3 Flattening

In order to compute the reachability set of an initialized system, in [BFLS05] and [LS05], algorithms based on *flattening* have been proposed. Flattening idea (see bellow the definition) uses the fact that in practice the meta-transition $\mathcal{R}^*_\theta$ is effectively computable for any loop θ.

A *Linear Regular Expression (LRE)* [LS05] ρ of a graph G is a subset of $\Pi(G) \cup \{\epsilon\}$ such that there exists $n \in \mathbb{N}\backslash\{0\}$, a sequence π_0, θ_1, π_1, ..., θ_n, π_n of $n+1$ paths π_i and n loops θ_i such that $\rho = \pi_0.\theta_1^*.\pi_1 \ldots \pi_{n-1}.\theta_n^*.\pi_n$. A *Semi Linear Regular Expression (SLRE)* ρ is a finite union of LRE.

A *flattening* ρ *of an initialized system* $(\mathcal{S}, (q_0, s_0))$ is a SLRE ρ such that:

$$\mathrm{Post}_{\xrightarrow{\Pi(G) \cup \{\epsilon\}}}(\{(q_0, s_0)\}) = \mathrm{Post}_{\xrightarrow{\rho}}(\{(q_0, s_0)\})$$

Remark 3.1 *A* flattening ρ of a system $\mathcal{S}$ *is a SLRE* ρ *such that* $\xrightarrow{\Pi(G) \cup \{\epsilon\}} = \xrightarrow{\rho}$. *Naturally, a flattening* ρ *of a system* $\mathcal{S}$ *is also a flattening of* $(\mathcal{S}, (q_0, s_0))$ *for any initial configuration* $(q_0, s_0) \in Q \times S$.

Intuitively, algorithms for computing the reachability set of an initialized system thanks to a flattening are based on the choice of a *symbolic representation* [BFLS05] for some subsets of S such that (1) the inclusion $X_1 \subseteq X_2$ of two symbolically represented subsets $X_1, X_2 \subseteq S$ is decidable, and (2) a symbolic representation of $X_1 \cup X_2$ is effectively computable from symbolic representations of X_1 and X_2, and (3) the set $\{s_0\}$ can be symbolically represented, and (4) a symbolic representation of $\mathrm{Post}_{\mathcal{R}_t}(X)$ is effectively computable from any symbolically represented subset $X \subseteq S$ and for any transition $t \in T$, and (5) a symbolic representation of $\mathrm{Post}^*_{\mathcal{R}_\theta}(X)$ is effectively computable for any loop θ and for any symbolically represented subset $X \subseteq S$.

If a symbolic representation satisfies (1),(2),(3),(4), and (5), in [BFLS05, LS05], we have proved that if there exists a flattening ρ of the initialized system $(\mathcal{S}, q_0, X_0)$, then a symbolic representation of the reachability set of this initialized system is effectively computable.

In practice, the most difficult and technical part of this approach is to provide an algorithm performing (5).

3.4 Acceleration

Sébastien Bardin and Alain Finkel shown in [BF04] that up to our knowledge, all the algorithms computing meta-transitions $\mathcal{R}^*$ where $\mathcal{R}$ is a binary relation over a set S corresponding to a sequence of transitions of a system, and $X \subseteq S$ compute the set $\text{acc}(\mathcal{R}, X) = \bigcup_{k\in\mathbb{N}}(\text{Post}^k_{\mathcal{R}}(X) \times \{k\})$ as an intermediate step. In this article, this set $\text{acc}(\mathcal{R}, X)$ is called the *acceleration* of $(\mathcal{R}, X)$.

Acceleration and fix-point computation are linked because (1) by projecting away the second component of $\text{acc}(\mathcal{R}, X)$, we obtain the fix-point $\text{Post}^*_{\mathcal{R}}(X)$, and (2) the acceleration of $(\mathcal{R}, X)$ is equal to $\text{Post}^*_{[\mathcal{R}]}(X \times \{0\})$ where $[\mathcal{R}]$ is the binary relation over $S \times \mathbb{R}$ defined by $(s, k)[\mathcal{R}](s', k')$ if and only if $s\mathcal{R}s'$ and $k' = k + 1$.

However, whereas there does not exist a "simple (from a decidability point of view) property" in order to check if a set $Z \subseteq S$ is equal to $\text{Post}^*_{\mathcal{R}}(X)$ (we can just check that Z is a fix-point $\text{Post}_{\mathcal{R}}(Z) \subseteq Z$ that contains $X \subseteq Z$), the following lemma shows that we can easily check if a set $Z \subseteq S \times \mathbb{N}$ is equal to $\text{acc}(\mathcal{R}, X)$.

Lemma 3.2 *[Submitted to CAV'06] Given a couple $(\mathcal{R}, X)$ where $\mathcal{R}$ is a binary relation over a set S and X is a subset of S, a subset $Z \subseteq S \times \mathbb{N}$ is equal to acc$(\mathcal{R}, X)$ if and only if $Z = \text{Post}_{[\mathcal{R}]}(Z) \cup (X \times \{0\})$.*

Proof : Naturally, the set $Z = \text{acc}(\mathcal{R}, X)$ satisfies $Z = \text{Post}_{[\mathcal{R}]}(Z) \cup (X \times \{0\})$. For the converse, let us consider a subset $Z \subseteq S \times \mathbb{N}$ such that $Z = \text{Post}_{[\mathcal{R}]}(Z) \cup (X \times \{0\})$ and let us prove by induction over $k \in \mathbb{N}$ that $Z \cap (S \times \{k\}) = \text{Post}^k_{\mathcal{R}}(X) \times \{k\}$. As $Z = \text{Post}_{[\mathcal{R}]}(Z) \cup (X \times \{0\})$, we get $Z \cap (S \times \{0\}) = X \times \{0\} = \text{Post}^0_{\mathcal{R}}(X) \times \{0\}$. Assume the induction true for an integer $k \in \mathbb{N}$. From $Z = \text{Post}_{[\mathcal{R}]}(Z) \cup (X \times \{0\})$, we get $Z \cap (S \times \{k + 1\}) = \text{Post}_{[\mathcal{R}]}(Z) \cap (S \times \{k + 1\}) = \text{Post}_{[\mathcal{R}]}(Z \cap (S \times \{k\}))$. Induction hypothesis proves that $Z \cap (S \times \{k\}) = \text{Post}^k_{\mathcal{R}}(X) \times \{k\}$. Therefore $\text{Post}_{[\mathcal{R}]}(Z \cap (S \times \{k\})) = \text{Post}^{k+1}_{\mathcal{R}}(X) \times \{k + 1\}$ and we have proved the induction. From $Z = \bigcup_{k\in\mathbb{N}}(Z \cap (S \times \{k\}))$, we get $Z = \text{acc}(\mathcal{R}, X)$. □

The previous lemma proves that if $\text{acc}(\mathcal{R}, X)$ can be represented by a symbolic representation, such that (1) the inclusion $Z_1 \subseteq Z_2$ of two symbolically represented subsets $Z_1, Z_2 \subseteq S \times \mathbb{N}$ is decidable, and (2) a symbolic representation of $\text{Post}_{[\mathcal{R}]}(Z) \cup (X \times \{0\})$ is effectively computable from any symbolically represented subset $Z \subseteq S \times \mathbb{N}$, then a symbolic representation of $\text{acc}(\mathcal{R}, X)$ is effectively computable just by enumerating symbolic representations of subsets of $S \times \mathbb{N}$ and check if $Z = \text{acc}(\mathcal{R}, X)$ thanks to lemma 3.2.

In particular, for the logic $\text{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$, we deduce the following theorem 3.3.

Theorem 3.3 *Let $(\mathcal{R}, X)$ be a couple definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ such that its acceleration acc$(\mathcal{R}, X)$ is definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$. We can effectively compute a formula in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ that defines the acceleration acc$(\mathcal{R}, X)$.*

Proof : In fact just enumerate the formulas ϕ in $\text{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$ that define a set $Z \subseteq \mathbb{R}^m \times \mathbb{N}$ and remark that a formula ϕ' in $\text{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$ defining $Z' = \text{Post}_{[\mathcal{R}]}(Z) \cup (X \times \{0\})$ is effectively computable. As we can decide if ϕ and ϕ' define the same set, lemma 3.2, shows that we can effectively computes a formula ϕ in $\text{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$ that defines $\text{acc}(\mathcal{R}, X)$. □

In practice, such an enumerative algorithm is not possible. Efficient algorithms performing acceleration computation are based on three points (1) the inclusion $Z_1 \subseteq Z_2$ of two symbolically represented subsets $Z_1, Z_2 \subseteq S \times \mathbb{N}$ is decidable, and (2) a symbolic representation of $\text{Post}^k_{\mathcal{R}}(X) \times \{k\}$ is computable for any bounded integer $k \in \mathbb{N}$, and (3) a symbolic representation of the acceleration of $(\mathcal{R}, X)$ can be *extrapolated* from the $k \in \mathbb{N}$ symbolic representations of the sets $\text{Post}^0_{\mathcal{R}}(X) \times \{0\}$, ..., $\text{Post}^{k-1}_{\mathcal{R}}(X) \times \{k - 1\}$, and (4) the correctness of the extrapolation is decided thanks to lemma 3.2

Remark 3.4 *The tool* TREX *implements the previous points (1), (2), (3) and (4) for the* Parametric Difference Bound Matrices (PDBM) *[AAB00, ABLS01].*

Remark 3.5 *The* acceleration *acc$(\mathcal{R})$ of a binary relation $\mathcal{R}$ over a set S is the subset of $(S \times S) \times \mathbb{N}$ defined by acc$(\mathcal{R}) = \bigcup_{k\in\mathbb{N}}(\mathcal{R}^k \times \{k\})$. Naturally, the acceleration of a relation can be reduced to the acceleration of a particular couple $(\mathcal{R}_2, I_S)$. In fact, let us consider the binary relation $\mathcal{R}_2$ defined over $S \times S$ by $(s_1, s_2)\mathcal{R}_2(s'_1, s'_2)$ if and only if $s_1 = s'_1$ and $s_2\mathcal{R}s'_2$, and remark that acc$(\mathcal{R})$ = acc$(\mathcal{R}_2, I_S)$ where I_S is the identity binary relation I_S over S.*

4 Linear hybrid automata (LHA)

A *linear hybrid automaton (LHA)* [BJ03, AHH96] $\mathcal{A}$ is a tuple $\mathcal{A} = (G, \mathbb{R}^m, (\text{inv}_q, \text{flow}_q)_{q\in Q}, (\text{pre}_t, \text{reset}_t, \text{post}_t)_{t\in T})$ where $G = (Q, T, \alpha, \beta)$ is a graph such that intuitively each state $q \in Q$ is labelled by a couple $(\text{inv}_q, \text{flow}_q)$ where inv_q is a rational polyhedral closed convex set of $\mathbb{R}^m$, called the *invariant in* q and where flow_q is a subset of $\mathbb{R}^m$ equal to a Cartesian product of sets of the form $[l, u]$ with $l, u \in \mathbb{Q}$, called the *control flow in* q, and such that each transition $t \in T$ is labelled by a tuple $(\text{pre}_t, \text{reset}_t, \text{post}_t)$ where reset_t is a subset of $\{1, \dots, m\}$ called the set of variables *reseted by* t, and where pre_t and post_t are two rational polyhedral closed convex sets of $\mathbb{R}^m$ respectively called the *pre invariant of* t and *post invariant of* t.

A system can be easily associated to a LHA, by introducing two kind of binary relations, respectively associated to the *continuous semantics*, and the *discrete* one.

The *continuous semantics* of $\mathcal{A}$ is given by the sequence $(\text{Wait}_q)_{q\in Q}$ of binary relation over $\mathbb{R}^m$ defined by $x\text{Wait}_q x'$ if and only if $x' \in x + \mathbb{R}_+.\text{flow}_q$ and $x, x' \in \text{inv}_q$. Recall [BJ03] that the binary relation Wait_q is a rational polyhedral closed convex binary relation over $\mathbb{R}^m$ satisfying $\text{Wait}_q.\text{Wait}_q = \text{Wait}_q$.

The *discrete semantics* of $\mathcal{A}$ is given by the sequence $(\text{Fire}_t)_{t\in T}$ of binary relations over $\mathbb{R}^m$ defined by $x\text{Fire}_t x'$ if and only if $x \in \text{pre}_t$, $x' \in \text{post}_t$, and $x'[i] = 0$ if $i \in \text{reset}_t$ and $x'[i] = x[i]$ otherwise.

The system $\mathcal{S}$ associated to a LHA $\mathcal{A}$ is defined by $\mathcal{S} = (G, S, (\mathcal{R}_t)_{t\in T})$ where $S = \mathbb{R}^m$ and $\mathcal{R}_t$ is the binary relation over $\mathbb{R}^m$ defined by:

$$\mathcal{R}_t = \text{Wait}_{\alpha(t)}.\text{Fire}_t.\text{Wait}_{\beta(t)}$$

Recall that the reachability problem of deciding if a configuration (q, s) is in the reachability set of an initialized LHA is undecidable in general and hence we can just hope to develop good semi-algorithms (see the introduction). Following the flattening approach, we are interested in using formulas in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ as a symbolic representation, and effectively computing a formula in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ defining $\text{Post}^*_{\mathcal{R}_\theta}(X)$ for any loop θ of a LHA and any set X defined in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$. Recall that [BJ03] shows that $\mathcal{R}_\theta$ is a rational polyhedral closed convex binary relation. Unfortunately, in general $\text{Post}^*_{\mathcal{R}_\theta}(X)$ is not definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$. Nevertheless, there exists some interesting classes of rational polyhedral closed convex binary relations such that $\mathcal{R}^*$ is definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$. In the following, these classes are recalled and we prove that the set $\text{acc}(\mathcal{R})$ is definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ in each case.

4.1 Relations of [BJ03]

In [BJ03], authors proved that the binary relation $\mathcal{R}_\theta$ associated to a loop θ in a LHA $\mathcal{A}$ is a rational polyhedral closed convex binary relation and they provide an algorithm for computing $\mathcal{R}^*_\theta$ if the binary relation $\mathcal{R}_\theta$ has the special structure given in the following theorem.

Theorem 4.1 ([BJ03]) *Let $\mathcal{R}$ be a binary relation over $\mathbb{R}^m$ such that there exist three rational polyhedral closed convex sets I, I' and F such that $(x, x') \in \mathcal{R}$ if and only if $x \in I \wedge x' \in I' \wedge (x' - x) \in F$. Then $\mathcal{R}^*$ is effectively definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$.*

Proof : We are going to prove that $\text{acc}(\mathcal{R})$ is defined by the following formula $\phi(x, x', k)$:

$$\phi(x, x', k) :=$$
$$(k = 0 \wedge (x, x') \in \mathcal{R}^0)$$
$$\vee\ (k = 1 \wedge (x, x') \in \mathcal{R})$$
$$\vee\ (k \in \mathbb{N}\backslash\{0, 1\} \wedge \exists y, y' \in \mathbb{R}^m;\ \begin{cases} y, y' \in I \cap I' \\ \wedge (x, y) \in \mathcal{R} \\ \wedge (y', x') \in \mathcal{R} \\ \wedge y' - y \in (k-2).F \end{cases}$$

Let us first consider $(x, x', k) \in \text{acc}(\mathcal{R})$, and let us prove that (x, x', k) satisfies ϕ. Remark that if $k \in \{0, 1\}$ then (x, x', k) satisfies ϕ. So we can assume that $k \in \mathbb{N}\backslash\{0, 1\}$. From $(x, x') \in \mathcal{R}^k$, we deduce that there exists x_0, ..., x_k in $\mathbb{R}^m$ such that $x_0 = x$, $x_k = x'$ and such that $(x_i, x_{i+1}) \in \mathcal{R}$ for any $i \in \{0, \dots, k-1\}$. From $x_0\mathcal{R}x_1$ and $x_1\mathcal{R}x_2$ (recall that $k \geq 2$), we get $x_1 \in I \cap I'$, and from $x_{k-2}\mathcal{R}x_{k-1}$ and $x_{k-1}\mathcal{R}x_k$, we get $x_{k-1} \in I \cap I'$. Remark that if $k = 2$, then $x_1 = x_{k-1}$, and in particular (x_1, x_k, k) satisfies ϕ. Assume that $k > 2$, as $x_{i-1} - x_i \in H$, we deduce that $\frac{1}{k-2}\sum_{i=1}^{k-2}(x_i - x_{i+1})$ is a linear combination of vectors in the convex set F. As this linear combination is equal to $\frac{1}{k-2}(x_1 - x_{k-1})$, we have proved that $(x_1 - x_{k-1}) \in (k-2).F$. Therefore we have proved that (x, x', k) satisfies ϕ.

For the converse, let us consider $(x, x', k) \in \mathbb{R}^m \times \mathbb{R}^m \times \mathbb{R}$ that satisfies ϕ, and let us prove that $(x, x', k) \in \text{acc}(\mathcal{R})$. By definition of ϕ, we get $k \in \mathbb{N}$. Remark that if $k \in \{0, 1\}$, we get $(x, x', k) \in \text{acc}\mathcal{R}$. Assume that $k \geq 2$. By definition of ϕ, there exists $x_1, x_{k-1} \in I \cap I'$ such that $(x, x_1) \in \mathcal{R}$, $(x_{k-1}, x') \in \mathcal{R}$, and such that $x' - x \in (k-2).F$. Naturally, if $k = 2$, then $x = x'$ and we deduce that $(x, x', k) \in \text{acc}(\mathcal{R})$. Let us assume that $k > 2$. In this case, the vector $v = \frac{x_{k-1} - x_1}{k-2}$ is well defined and it is a vector in F. Let us consider the sequence $(x_i)_{2\leq i\leq k-2}$ defined by $x_i = x_1 + (i-1).v$ for any $i \in \{2, \dots, k-2\}$. The equality $x_i = x_1 + (i-1).v$ even holds for $i \in \{1, k-1\}$. Remark that $x_{i+1} - x_i = v \in F$ for any $i \in \{1, \dots, k-2\}$. Moreover, from $x_i = (1 - \frac{i-1}{k-2}).x_1 + \frac{i-1}{k-2}.x_{k-1}$, we deduce that x_i is a convex linear combination of vectors in the convex set $I \cap I'$. Hence $x_i \in I \cap I'$. We have proved that $(x_{i+1}, x_i) \in \mathcal{R}$.

Therefore $(x_1, x_{k+1}) \in \mathcal{R}^{k-1}$ and we get $(x, x') \in \mathcal{R}^k$. We have proved that $(x, x', k) \in \mathrm{acc}(\mathcal{R})$. $\square$

From the previous theorem, we deduce that the acceleration $\mathrm{acc}(\mathcal{R})$ of such a binary relation is definable in $\mathrm{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$.

Corollary 4.2 *Let $\mathcal{R}$ be a binary relation over $\mathbb{R}^m$ such that there exists three rational polyhedral closed convex sets I, I' and F such that $(x, x') \in \mathcal{R}$ if and only if $x \in I \wedge x' \in I' \wedge (x' - x) \in F$. Then $\mathcal{R}$ is a rational polyhedral closed convex binary relation such that $acc(\mathcal{R})$ is effectively definable in $FO(\mathbb{R}, \mathbb{Z}, +, \leq)$.*

Proof : Remark that $[\mathcal{R}]$ is a binary relation over $\mathbb{R}^{m+1}$ that satisfies $(x, k)[\mathcal{R}](x', k')$ if and only if $(x, k) \in (I \times \mathbb{R}) \wedge (x', k') \in (I' \times \mathbb{R}) \wedge (x', k') - (x, k) \in F \times \{1\}$. From theorem 4.1, we deduce that $[\mathcal{R}]^*$ can be defined by a formula $\phi(x, k, x', k')$ in $\mathrm{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$. Now, just remark that $\mathrm{acc}(\mathcal{R})$ is defined by $\phi(x, 0, x', k) \wedge k \in \mathbb{N}$ and we have proved that $\mathrm{acc}(\mathcal{R})$ is definable in $\mathrm{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$. $\square$

4.2 Relations of [CJ98]

Recall that a *Timed Automaton (TA)* is a LHA such that $\mathrm{flow}_q = \{1\}^m$ for any state $q \in Q$ and such that inv_q, pre_t and post_t are equal to a Cartesian product of sets of the form $[l, u]$ with $l, u \in \mathbb{Q}$. In [CJ98], authors proved that any TA owns a flattening and the reflexive and transitive closures $\mathcal{R}_\theta^*$ of any loop θ of the TA is effectively definable in $\mathrm{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$.

The proof is based on the following theorem and a variable changing that transforms relations $\mathcal{R}_t$ of a TA into *DBM-definable* binary relations: A subset $X \subseteq \mathbb{R}^m$ is said *DBM-definable* if it can be defined as a conjunction of formulas of the form $x[i] - x[j] \# c$ where $(\#, c) \in \{\leq, <, =, >, \geq\} \times \mathbb{Q}$.

Theorem 4.3 ([CJ98]) *Let $\mathcal{R}$ be a DBM-definable binary relation over $\mathbb{R}^m$. The binary relation $\mathcal{R}^*$ is effectively definable in $FO(\mathbb{R}, \mathbb{Z}, +, \leq)$.*

Remark 4.4 *For any DBM-definable binary relation $\mathcal{R}$ over $\mathbb{R}^m$, the set $acc(\mathcal{R})$ is definable in $FO(\mathbb{R}, \mathbb{Z}, +, \leq)$. In fact, just remark that $[\mathcal{R}]$ remains DBM-definable, hence $[\mathcal{R}]^*$ is definable in $FO(\mathbb{R}, \mathbb{Z}, +, \leq)$ from the previous theorem. We deduce that $acc(\mathcal{R})$ is definable in $FO(\mathbb{R}, \mathbb{Z}, +, \leq)$.*

In fact, thanks to the same reduction and thanks to the previous theorem, we deduce that the acceleration $\mathrm{acc}(\mathcal{R}_\theta)$ is definable in $\mathrm{FO}(\mathbb{R}, \mathbb{Z}, + \leq)$ for any loop θ in a TA.

Corollary 4.5 *Let θ be a loop in a Timed Automaton. Then $\mathcal{R}_\theta$ is a rational polyhedral closed convex binary relation such that $acc(\mathcal{R}_\theta)$ is definable in $FO(\mathbb{R}, \mathbb{Z}, +, \leq)$.*

Proof : Let us consider a TA $\mathcal{A} = (G, \mathbb{R}^m, (\mathrm{inv}_q, \mathrm{flow}_q)_{q \in Q}, (\mathrm{pre}_t, \mathrm{reset}_t, \mathrm{post}_t)_{t \in T})$. For any transition $t \in T$, let us consider the binary relation $\mathcal{R}_{E,t}$ defined over $\mathbb{R}^m \times \mathbb{R} \times \mathbb{R}$ by $(d, z, k)\mathcal{R}_{E,t}(d', z', k')$ if and only if:

$$\begin{cases} \bigwedge_{i \in \mathrm{reset}_t} z \leq d'[i] \leq z' \\ \bigwedge_{i \notin \mathrm{reset}_t} d'[i] = d[i] \\ \bigwedge_{i_1, i_2 \in \mathrm{reset}_t} d'[i_1] = d'[i_2] \\ z \leq z' \\ (z, \dots, z) - d \in \mathrm{pre}_t \\ (z', \dots, z') - d' \in \mathrm{post}_t \\ k' = k + 1 \end{cases}$$

We can easily check that we have $(d, z, k)\mathcal{R}_{E,t}(d', z', k')$ if and only if $((z, \dots, z) - d)\mathcal{R}_t((z', \dots, z') - d')$ and $k' = k + 1$, for any $(d, z, k), (d', z', k') \in \mathbb{R}^m \times \mathbb{R} \times \mathbb{R}$.

Let us consider the unique sequence $(\mathcal{R}_{E,\pi})_{\pi \in \Pi(G)}$ that naturally extends $(\mathcal{R}_{E,t})_{t \in T}$. As the composition of two DBM-definable binary relation remains DBM-definable, we deduce that $\mathcal{R}_{E,\pi}$ is DBM-definable for any path $\pi \in \Pi(G)$.

Naturally, we have $(d, z, k)\mathcal{R}_{E,\pi}(d', z', k')$ if and only if $((z, \dots, z) - d)\mathcal{R}_\pi((z', \dots, z') - d')$ and $k' = k + |\pi|$, for any $(d, z, k), (d', z', k') \in \mathbb{R}^m \times \mathbb{R} \times \mathbb{R}$, and for any path $\pi \in \Pi(G)$.

Let θ be a loop. As $\mathcal{R}_{E,\theta}$ is DBM-definable, theorem 4.3 proves that $\mathcal{R}_{E,\theta}^*$ is definable in $\mathrm{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$. Let $\phi_E(d, z, k, d', z', k')$ be a formula in this logic defining $\mathcal{R}_{E,\theta}^*$ and remark that $\mathrm{acc}(\mathcal{R}_\theta)$ is defined by $\phi(x, x', k) := \exists d, z, d', z';\ x = (z, \dots, z) - d \wedge x' = (z', \dots, z') - d' \wedge \phi_E(d, z, 0, d', z', |\theta|.k)$. $\square$

5 Linear extrapolation acceleration

In this section, we present a complete semi-algorithm that computes a formula in $\mathrm{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$ that defines the acceleration of a rational polyhedral closed convex binary relation thanks to a *linear extrapolation operator*, as soon as such a formula exists.

Two polyhedral closed convex sets C_1 and C_2 are said *isomorph* if $\overrightarrow{\mathrm{aff}}(C_1) = \overrightarrow{\mathrm{aff}}(C_2)$ and $\{\overrightarrow{H};\ H \in \mathcal{H}(C_1)\} = \{\overrightarrow{H};\ H \in \mathcal{H}(C_2)\}$. Let $A_1 = \mathrm{aff}(C_1)$ and $A_2 = \mathrm{aff}(C_2)$. From $\overrightarrow{A_1} = \overrightarrow{A_2}$, we deduce that there exists a sequence $(\alpha_i)_{i \in I}$ of vectors in $\mathbb{R}^m$ and a sequence $(c_{i,k})_{(i,k) \in I \times \{1,2\}}$ in $\mathbb{R}$ such that $\overrightarrow{A_k} = \{x \in \mathbb{R}^m;\ \langle \alpha_i, x \rangle = c_{i,k}\}$ for any $k \in \{1, 2\}$. Moreover, from $\{\overrightarrow{H};\ H \in \mathcal{H}(C_1)\} = \{\overrightarrow{H};\ H \in$

$\mathcal{H}(C_2)\}$, we deduce that there exists a sequence $(\alpha_H)_{H\in\mathcal{H}}$ of vectors in $\mathbb{R}^m$, and a sequence $(c_{H,k})_{(H,k)\in\mathcal{H}\times\{1,2\}}$ in $\mathbb{R}$ such that $H = H_{A_k,\alpha_H,\leq,c_{H,k}}$. Given $t_1, t_2 \in \mathbb{R}$ such that $t_1 \neq t_2$, we denote by $C_1 \overset{(t_1,t_2)}{\nabla} C_2$ (it only depends on C_1, C_2 and t_1, t_2) the polyhedral closed convex set of tuples $(x,t) \in \mathbb{R}^m \times \mathbb{R}$ such that:

$$\bigwedge_{i\in I} \langle \alpha_i, x\rangle \leq \frac{t-t_2}{t_1-t_2}.c_{i,1} + \frac{t_1-t}{t_1-t_2}.c_{i,2}$$
$$\wedge \bigwedge_{H\in\mathcal{H}} \langle \alpha_H, x\rangle \leq \frac{t-t_2}{t_1-t_2}.c_{H,1} + \frac{t_1-t}{t_1-t_2}.c_{H,2}$$

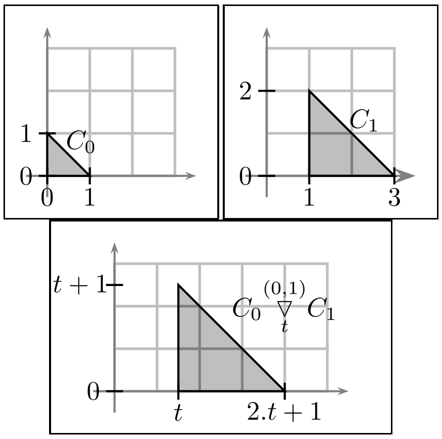

Figure 3. The linear extrapolation operator

Consider two isomorph polyhedral closed convex sets C_1 and C_2, and a real $t \in \mathbb{R}$, we denote by $C_1 \underset{t}{\overset{(t_1,t_2)}{\nabla}} C_2$ (see figure 3) the polyhedral closed convex sets of $x \in \mathbb{R}^m$ such that $(x,t) \in C_1 \overset{(t_1,t_2)}{\nabla} C_2$. Remark that $C_1 \underset{t}{\overset{(t_1,t_2)}{\nabla}} C_2$ is a *linear extrapolation* equal to C_1 if $t = t_1$ and equal to C_2 if $t = t_2$. Remark also that $C_1 \overset{(t_1,t_2)}{\nabla} C_2$ is rational if $t_1, t_2 \in \mathbb{Q}$ and C_1, C_2 are rational.

Example 5.1 *Let $C_0 = \{x \in \mathbb{R}^2;\ x[1] \geq 0 \wedge x[2] \geq 0 \wedge x[1]+x[2] \leq 1\}$ and $C_1 = \{x \in \mathbb{R}^2;\ x[1] \geq 1 \wedge x[2] \geq 0 \wedge x[1]+x[2] \leq 3\}$ be two polyhedral closed convex sets given in figure 3. Remark that C_0 and C_1 are isomorph. The polyhedral closed convex set $C_0 \underset{t}{\overset{(0,1)}{\nabla}} C_1$ is represented in the same figure. Remark that $\bigcup_{k\in\mathbb{N}} C_0 \underset{k}{\overset{(0,1)}{\nabla}} C_1$ is definable in FO $(\mathbb{R},\mathbb{Z},+,\leq)$ and corresponds to the set represented in figure 2.*

We are going to prove the following main theorem of this paper.

Theorem 5.2 *Let $\mathcal{R}$ be a rational polyhedral closed convex binary relation over $\mathbb{R}^m$ such that $acc(\mathcal{R})$ is definable in FO $(\mathbb{R},\mathbb{Z},+,\leq)$. There exists $k_0 < k_1$ such that $\mathcal{R}^{k_0+r}$ and $\mathcal{R}^{k_1+r}$ are isomorph for any $r \in \{0,\dots,p-1\}$ where $p = k_1 - k_0$, and such that $acc(\mathcal{R})$ is defined by the following formula $\phi_{\mathcal{R},k_0,k_1}(x,x',k)$:*

$$\phi_{\mathcal{R},k_0,k_1}(x,x',k) :=$$
$$\bigvee_{c=0}^{k_0-1} \begin{pmatrix} (x,x') \in \mathcal{R}^c \\ \wedge k = c \end{pmatrix}$$
$$\bigvee_{r=0}^{p-1} \begin{pmatrix} (x,x',k) \in \left(\mathcal{R}^{k_0+r} \overset{(k_0+r,k_1+r)}{\nabla} \mathcal{R}^{k_1+r}\right) \\ \wedge k \in k_0 + r + \mathbb{N}.p \end{pmatrix}$$

We first prove some lemmas.

Lemma 5.3 *Let $(C_k)_{k\in\mathbb{N}}$ be a sequence of rational polyhedral closed convex sets of $\mathbb{R}^m$ such that $X = \bigcup_{k\in\mathbb{N}}(C_k \times \{k\})$ is definable in FO $(\mathbb{R},\mathbb{Z},+,\leq)$. There exists $k_0 \in \mathbb{N}$, $p \in \mathbb{N}\backslash\{0\}$, a finite set J, a partition $(J_r)_{0\leq r\leq p-1}$ of J, two sequences $(C_j^0)_{j\in J}$ and $(C_j^1)_{j\in J}$ of non-empty rational polyhedral closed convex sets of $\mathbb{R}^m$ such that $C_{k_0+r+n.p} = \bigcup_{j\in J_r}(C_j^0 + n.C_j^1)$ for any $r \in \{0,\dots,p-1\}$ and for any $n \in \mathbb{N}$.*

Proof : As X is definable in FO $(\mathbb{R},\mathbb{Z},+,\leq)$, there exists a finite set I, a sequence $(X_i)_{i\in I}$ of subsets $X_i \subseteq [0,1[^{m+1}$ definable in FO $(\mathbb{R},+,\leq)$, a sequence $(b_i)_{i\in I}$ of vectors $b_i \in \mathbb{Z}^{m+1}$ and a sequence $(P_i)_{i\in I}$ of finite sets $P_i \in \mathcal{P}_f(\mathbb{Z}^{m+1})$ such that $X = \bigcup_{i\in I}(X_i + b_i + P_i^*)$. As $X \subseteq \mathbb{R}^m \times \mathbb{N}$, we deduce that $X_i \subseteq \mathbb{R}^m \times \{0\}$, $b_i \in \mathbb{Z}^m \times \mathbb{N}$, and $P_i \in \mathcal{P}_f(\mathbb{Z}^m \times \mathbb{N})$. The set $Y_i = \{(x[1],\dots,x[m]);\ x \in X_i\}$ is definable in FO $(\mathbb{R},+,\leq)$. Let us denote by $P_i^0 = \{(x[1],\dots,x[m]);\ x \in P_i \wedge x[m+1] = 0\}$ and let $P_i^> = P_i\backslash(P_i^0 \times \{0\})$. There exists an integer $p \in \mathbb{N}\backslash\{0\}$, such that $x[m+1]$ divides p for any $x \in \bigcup_{i\in I} P_i^>$. Let us consider the set $Z_i = \{\frac{p}{x[m+1]}.(x[1],\dots,x[m]);\ x \in P_i^>\}$, and let $B_i = b_i + \sum_{x\in P_i^>}\{0,\dots,p-1\}.x$. Remark that $B_i \in \mathcal{P}_f(\mathbb{Z}^m \times \mathbb{N})$, $P_i^0 \in \mathcal{P}_f(\mathbb{Z}^m)$, and $Z_i \in \mathcal{P}_f(\mathbb{Z}^m)$ are such that $b_i + P_i^* = B_i + (P_i^0)^* \times \{0\} + (Z_i \times \{p\})^*$. Let us consider an integer $k_0 \in \mathbb{N}$ such that $b[m+1] < k_0$ for any $b \in \bigcup_{i\in I} B_i$, and let $B_{(i,r)}$ be the set of $b \in B_i$ such that $b[m+1] \in k_0 + r + p.\mathbb{Z}$. Let us denote by J the set of tuples $(i,r) \in I \times \{0,\dots,p-1\}$ such that the set $H_{(i,r)} = B_{(i,r)} + Y_i + (P_i^0)^*$ is not empty and such that $Z_i \neq \emptyset$. Let us consider the partition $(J_r)_{0\leq r\leq p-1}$ of J defined by $J_r = J \cap (I \times \{r\})$. We have proved the following equality for any $r \in \{0,\dots,p-1\}$ and for any $n \in \mathbb{N}$:

$$C_{k_0+r+n.p} = \bigcup_{(i,r)\in J_r} \left(H_{(i,r)} + \{z \in \mathbb{Z}^m;\ (z,n.p) \in Z_i^*\}\right)$$

As $H_{(i,r)}$ is non-empty and definable in FO $(\mathbb{R},\mathbb{Z},+,\leq)$, we deduce that $C_{(i,r)}^0 = \mathrm{cl} \circ \mathrm{conv}(H_{i,r})$ is a non-empty rational polyhedral closed convex set. As Z_i is a non-empty finite set, we deduce that $C^1_{(i,r)} = \mathrm{cl} \circ \mathrm{conv}(Z_i)$ is also a non-empty polyhedral closed convex set. Remark that this set satisfies the following equality for any $n \in \mathbb{N}$:

$$\mathrm{conv}\left(\{z \in \mathbb{Z}^m;\ (z, n.p) \in Z^*_i\}\right) = n.C^1_{(i,r)}$$

As $C_{k_0+r+p.n}$ is a polyhedral closed convex set, we deduce that $C^0_j + n.C^1_j \subseteq C_{k_0+r+p.n}$ for any $j \in J_r$. We have proved the lemma. □

Lemma 5.4 *Let $(C_j)_{j\in J}$ be a finite sequence of polyhedral closed convex sets such that $C = \bigcup_{j\in J} C_j$ is a convex set. Then we have the following equality:*

$$C = \bigcup_{j\in J;\ \mathrm{aff}(C_j)=\mathrm{aff}(C)} C_j$$

Proof: Naturally if $C = \emptyset$, we are done. So, we can assume that $C \neq \emptyset$. Let $(A_j)_{j\in J}$ be the sequence of affine spaces $A_j = \mathrm{aff}(C_j)$. From $C_j \subseteq C$, we deduce that $A_j \subseteq A$ for any $j \in J$. Let us denote by $J' = \{j \in J;\ A_j = A\}$. Consider the set $C' = \bigcup_{j\in J'} C_j$ and let us prove that $C' = C$. Naturally, we have the inclusion $C' \subseteq C$. Let us prove the converse inclusion. We denote by $X_1 = C \backslash (\bigcup_{j\in J\backslash J'} A_j)$. Remark that $C \subseteq \mathrm{aff}(X_1) \cup \bigcup_{j\in J\backslash J'} A_j$ and A is not included in A_j. Hence, from lemma 2.1, we deduce that $A \subseteq \mathrm{aff}(X_1)$. In particular X_1 is not empty and there exists $x_1 \in X_1$. Let $x_0 \in C$ and let us define for any $t \in \mathbb{R}$ the vector $x_t = t.x_1 + (1-t).x_0$. As x_1 and x_0 are in the convex set C, the vector $x_t = t.x_1 + (1-t).x_0$ is in C if $0 \leq t \leq 1$. Remark that if $x_t \in \bigcup_{j\in J\backslash J'} A_j$ for an infinite number of $0 \leq t \leq 1$, then there exists $j \in J\backslash J'$ such that $x_t \in A_j$ for at least two different t. In particular, as A_j is an affine space, we deduce that $x_t \in A_j$ for any t. So $x_1 \in A_j$ which is impossible. There exists $0 < \epsilon < 1$ such that $x_t \in X_1$ for any $0 < t < \epsilon$. Hence $x_0 \in \mathrm{cl}(X_1)$. As $X_1 \subseteq C'$ and C' is closed (as a finite union of closed sets), we get $\mathrm{cl}(X_1) \subseteq C'$. Hence $x_0 \in C'$ and we have proved the other inclusion $C \subseteq C'$. □

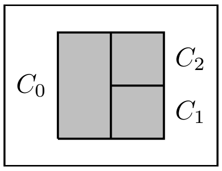

Figure 4. $C = C_0 \cup C_1 \cup C_2$

Figure 4 provides an intuitive idea of the following lemma 5.4.

Lemma 5.5 *Let $(C_j)_{j\in J}$ be a finite sequence of polyhedral closed convex sets such that $C = \bigcup_{j\in J} C_j$ is a convex set, and such that $\mathrm{aff}(C_j) = \mathrm{aff}(C)$ for any $j \in J$. Then $\mathcal{H}(C) \subseteq \bigcup_{j\in J} \mathcal{H}(C_j)$.*

Proof: Let $H \in \mathcal{H}(C)$. Lemma 2.2 shows that $C \subseteq H$ and $\mathrm{aff}(C \cap H^=) = H^=$. As $C \cap H^=$ is a convex set such that $C \cap H^= \subseteq \bigcup_{j\in J} \mathrm{aff}(C_j \cap H^=)$, lemma 2.1 proves that there exists $j \in J$ such that $C \cap H^= \subseteq \mathrm{aff}(C_j \cap H^=)$. Hence $H^= = \mathrm{aff}(C \cap H^=) \subseteq \mathrm{aff}(C_j \cap H^=)$. As $C_j \cap H^= \subseteq H^=$, we also deduce the inclusion $\mathrm{aff}(C \cap H^=) \subseteq H^=$. Therefore $\mathrm{aff}(C_j \cap H^=) = H^=$. Moreover, as $C_j \subseteq C \subseteq H$, lemma 2.2 shows that $H \in \mathcal{H}(C_j)$. □

Lemma 5.6 ([Ler04]) *Let X_1 and X_2 be two subsets of $\mathbb{R}^m$. We have $\mathrm{aff}(X_1 + X_2) = \mathrm{aff}(X_1) + \mathrm{aff}(X_2)$.*

Proof : From $X_1 \subseteq \mathrm{aff}(X_1)$ and $X_2 \subseteq \mathrm{aff}(X_2)$, we get $X_1 + X_2 \subseteq \mathrm{aff}(X_1) + \mathrm{aff}(X_2)$. Moreover, as $\mathrm{aff}(X_1) + \mathrm{aff}(X_2)$ is an affine space, we get $\mathrm{aff}(X_1 + X_2) \subseteq \mathrm{aff}(X_1) + \mathrm{aff}(X_2)$. Let us prove the converse inclusion. From any $x_1 \in X_1$, we have $x_1 + X_2 \subseteq X_1 + X_2 \subseteq \mathrm{aff}(X_1 + X_2)$. Hence $\mathrm{aff}(x_1 + X_2) \subseteq \mathrm{aff}(X_1 + X_2)$. From $\mathrm{aff}(x_1 + X_2) = x_1 + \mathrm{aff}(X_2)$, we deduce that $X_1 + \mathrm{aff}(X_2) \subseteq \mathrm{aff}(X_1 + X_2)$. In particular $X_1 + a_2 \subseteq \mathrm{aff}(X_1 + X_2)$ for any $a_2 \in \mathrm{aff}(X_2)$. We deduce that $\mathrm{aff}(X_1) + a_2 \subseteq \mathrm{aff}(X_1 + X_2)$. Therefore $\mathrm{aff}(X_1) + \mathrm{aff}(X_2) \subseteq \mathrm{aff}(X_1 + X_2)$. □

Lemma 5.7 *Let A be a non-empty affine space, let J be a finite set, let $(C_j)_{j\in J}$ be a sequence of non-empty polyhedral closed convex sets such that $\mathrm{aff}(C_j) = A$, let $(V_j)_{j\in J}$ be a sequence of non-empty polyhedral closed convex sets such that $\mathrm{aff}(V_j) \subseteq \overrightarrow{A}$. We assume that $C_n = \bigcup_{j\in J}(C_j + n.V_j)$ is convex for any $n \in \mathbb{N}$. There exists a finite class $\mathcal{H}$ of closed half-spaces of A, and a sequence $(v_H)_{H\in\mathcal{H}}$ of vectors in $\overrightarrow{A}$, there exists $n_0 \in \mathbb{N}$ such that we have the following equality for any $n \geq n_0$:*

$$\mathcal{H}(C_n) = \{H + n.v_H;\ H \in \mathcal{H}\}$$

Proof: Let us denote by $C_{j,n}$ the convex set $C_{j,n} = C_j + n.V_j$. First remark that $\mathrm{aff}(C_{j,n}) = \mathrm{aff}(C_j) + n.\mathrm{aff}(V_j)$. From $\mathrm{aff}(V_j) \subseteq \overrightarrow{A}$, we deduce that $\mathrm{aff}(C_{j,n}) = A$. A quantification elimination (Fourier-Motskin) shows that there exists a finite set I, a sequence $(I_j)_{j\in J}$ of subsets $I_j \subseteq I$, a sequence $((\alpha_i, a_i, c_i))_{i\in I}$ of tuples $(\alpha_i, a_i, c_i) \in (\overrightarrow{A}\backslash\{\mathbf{e}_0\}) \times \mathbb{R} \times \mathbb{R}$ such that $C_{j,n} = A \cap \bigcap_{i\in I_j} H_{i,n}$ where $H_{i,n} = \{x \in A;\ \langle \alpha_i, x\rangle \leq c_i + n.a_i\}$. Naturally, we can assume without loss of generality that $\mathbb{R}_+.\alpha_{i_1} = \mathbb{R}_+.\alpha_{i_2}$ implies $\alpha_{i_1} = \alpha_{i_2}$. We can also assume that if $\alpha_{i_1} = \alpha_{i_2}$ then $(a_{i_1}, c_{i_1}) \neq (a_{i_2}, c_{i_2})$.

Lemma 5.5 proves that $\mathcal{H}(C_n) \subseteq \bigcup_{j\in J} \mathcal{H}(C_{j,n})$. In particular $\mathcal{H}(C_n) \subseteq \{H_{i,n};\ i \in I\}$. Let us consider the set $I_{j,n}$ of $i \in I_j$ such that $H_{i,n} \in \mathcal{H}(C_n) \cap \mathcal{H}(C_{j,n})$, and remark that $\mathcal{H}(C_n) = \{H_{i,n};\ i \in I_n\}$ where $I_n = \bigcup_{j\in J} I_{j,n}$.

Let us prove that for any $n_1 \leq n_2$ in $\mathbb{N}$ and for any $j \in J$, if $i \in I_{j,n_1} \cap I_{j,n_2}$, then $i \in I_{j,n}$ for any $n \in \{n_1, \ldots, n_2\}$. Naturally, if $n_1 = n_2$ we are done. So, we can assume that $n_1 < n_2$. Moreover, if $n = 0$, then $n = n_1$ and we are done. So we can also assume that $n \in \mathbb{N}\backslash\{0\}$. The property is obtained by first proving the inclusion $\frac{1}{n_1-n_2}((n-n_2).(C_{j,n_1} \cap H^{=}_{i,n_1}) + (n_1-n).(C_{j,n_2} \cap H^{=}_{i,n_2})) \subseteq C_{j,n} \cap H^{=}_{i,n}$. Let $x_k \in C_{j,n_k} \cap H^{=}_{i,n_k}$ where $k \in \{1,2\}$. There exists $c_k \in C_j$ and $v_k \in V_j$ such that $x_k = c_k + n_k.v_k$. Let $x = \frac{1}{n_1-n_2}((n-n_2).x_1 + (n_1-n).x_2)$ and remark that $x = c + n.v$ where $c = \frac{1}{n_1-n_2}((n-n_2).c_1 + (n_1-n).c_2)$ and $v = \frac{1}{n.(n_1-n_2)}((n-n_2).x_1 + (n_1-n).x_2)$. As C_j and V_j are convex, we deduce that $c \in C_j$ and $v \in V_j$. Moreover, as $x_k \in H_{i,n_k}$, we get $\langle \alpha_i, x_k\rangle = c_i + n_k.a_i$. Hence $\langle \alpha_i, x\rangle = c_i + n.a_i$ and we have proved that $x \in C_{j,n} \cap H^{=}_{i,n}$. We deduce that $\frac{1}{n_1-n_2}((n-n_2).(C_{j,n_1} \cap H^{=}_{i,n_1}) + (n_1-n).(C_{j,n_2} \cap H^{=}_{i,n_2})) \subseteq C_{j,n} \cap H^{=}_{i,n}$. In particular, as $\mathrm{aff}(C_{j,n_k} \cap H^{=}_{i,n_k}) = H^{=}_{i,n_k}$, we get $\frac{1}{n_1-n_2}((n-n_2).H^{=}_{i,n_1} + (n_1-n).H^{=}_{i,n_2}) \subseteq \mathrm{aff}(C_{j,n} \cap H^{=}_{i,n})$. We deduce that $H^{=}_{i,n} \subseteq \mathrm{aff}(C_{j,n} \cap H^{=}_{i,n})$. In particular $i \in I_{j,n}$.

From the previous paragraph, we deduce that $(I_{j,n})_{n\in\mathbb{N}}$ is a non-increasing sequence for $\subseteq$. In particular, there exists $n_j \in \mathbb{N}$ such that $I_{j,n} = I_{j,n_j}$ for any $n \geq n_j$. Consider $n_0 = \max_{j\in J}(n_j)$ and remark that we have proved that $I_n = I_{n_0}$ for any $n \geq n_0$, and in particular $\mathcal{H}(C_n) = \{H_{i,n};\ i \in I_{n_0}\}$ for any $n \geq n_0$.

Let $\mathcal{H} = \{H_{i,0};\ i \in I_{n_0}\}$ and let us show that $H_{i_1,0} = H_{i_2,0}$ implies $i_1 = i_2$. In fact, in this case $\mathbb{R}_+.\alpha_{i_1} = \mathbb{R}_+.\alpha_{i_2}$ which implies $\alpha_{i_1} = \alpha_{i_2}$. Moreover, as $H_{i_1,n}$ and $H_{i_2,n}$ are both in $\mathcal{H}(C_n)$ for any $n \geq n_0$, we deduce that they are equal. Hence $(a_{i_1}, c_{i_1}) = (a_{i_2}, c_{i_2})$, and we deduce that $i_1 = i_2$.

For any $i \in I$, let us consider $v_i = \frac{a_i}{\langle\alpha_i,\alpha_i\rangle}.\alpha_i$ and just remark that $H_{i,n} = H_{i,0} + n.v_i$. So, we are done. □

Now, we can prove the following proposition.

Proposition 5.8 *Let us consider a sequence $(C_k)_{k\in\mathbb{N}}$ of rational polyhedral closed convex sets such that $X = \bigcup_{k\in\mathbb{N}}(C_k \times \{k\})$ is definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$. There exists $k_0 < k_1$ such that C_{k_0+r} and C_{k_1+r} are isomorph for any $r \in \{0, \ldots, p-1\}$ where $p = k_1 - k_0$, and such that:*

$$C_{k_0+r+n.p} = C_{k_0+r} \underset{k_0+r+n.p}{\overset{(k_0+r,k_1+r)}{\nabla}} C_{k_1+r}$$

for any $r \in \{0, \ldots, p-1\}$ and for any $n \in \mathbb{N}$.

Proof : From lemma 5.3, we deduce that there exists $k_2 \in \mathbb{N}$, $p \in \mathbb{N}\backslash\{0\}$, a finite set J, a partition $(J_r)_{0\leq r\leq p-1}$ of J, two sequences $(C^0_j)_{j\in J}$ and $(C^1_j)_{j\in J}$ of non-empty polyhedral closed convex sets of $\mathbb{R}^m$ such that $C_{k_2+r+n.p} = \bigcup_{j\in J_r}(C^0_j + n.C^1_j)$ for any $r \in \{0, \ldots, p-1\}$ and for any $n \in \mathbb{N}$.

Let us consider an integer $r \in \{0, \ldots, p-1\}$ such that J_r is not empty.

Let $J_{r,n}$ be the set of $j \in J_r$ such that $\mathrm{aff}(C^0_j + n.C^1_j) = \mathrm{aff}(C_{k_2+r+n.p})$. From lemma 5.4, we deduce that $C_{k_2+r+n.p} = \bigcup_{j\in J_{r,n}}(C^0_j + n.C^1_j)$. In particular, as this set is not empty, we get $J_{r,n} \neq \emptyset$.

Let us prove that $J_{r,n} = J_{r,1}$ for any $n \geq 1$. Consider $j_1 \in J_{r,n_1}$ and $j_2 \in J_{r,n_2}$ with $n_1, n_2 \geq 1$. We have $\mathrm{aff}(C_{k_2+r+n_1.p}) = \mathrm{aff}(C^0_{j_1} + n_1.C^1_{j_1}) = \mathrm{aff}(C^0_{j_1}) + n_1.\mathrm{aff}(C^1_{j_1})$. Moreover, as $C^0_{j_2} + n_1.C^1_{j_2} \subseteq C_{k_2+r+n_1.p}$, we deduce the inclusion $\mathrm{aff}(C^0_{j_2}) + n_1.\mathrm{aff}(C^1_{j_2}) \subseteq \mathrm{aff}(C^0_{j_1}) + n_1.\mathrm{aff}(C^1_{j_1})$. Symmetrically, we also get the inclusion $\mathrm{aff}(C^0_{j_1}) + n_2.\mathrm{aff}(C^1_{j_1}) \subseteq \mathrm{aff}(C^0_{j_2}) + n_2.\mathrm{aff}(C^1_{j_2})$. The direction of the two previous inclusion, provides (recall that $n_1, n_2 \neq 0$) the equality $\overrightarrow{\mathrm{aff}}(C^0_{j_2}) + \overrightarrow{\mathrm{aff}}(C^1_{j_2}) = \overrightarrow{\mathrm{aff}}(C^0_{j_1}) + \overrightarrow{\mathrm{aff}}(C^1_{j_1})$. In particular the affine spaces of the inclusion $\mathrm{aff}(C^0_{j_1} + n_2.C^1_{j_1}) \subseteq \mathrm{aff}(C^0_{j_2} + n_2.C^1_{j_2})$ have the same direction and they must be equal. So $\mathrm{aff}(C^0_{j_1} + n_2.C^1_{j_1}) = \mathrm{aff}(C^0_{j_2} + n_2.C^1_{j_2})$ and we deduce $j_1 \in J_{r,n_2}$ and symmetrically $j_2 \in J_{r,n_1}$. We have proved that $J_{r,n} = J_{r,1}$ for any $n \geq 1$.

Let us consider a vector $a \in \bigcup_{j\in J_{r,1}} C^1_j$, and let $V_j = C^1_j - a$ and $C_j = C^0_j + C^1_j$ for any $j \in J_{r,1}$. Remark that we have $W_n = \bigcup_{j\in J_{r,1}}(C_j + n.V_j)$ for any $n \in \mathbb{N}$ where $W_n = C_{k_2+r+p+n.p} - n.a$. Let A be the affine hull $A = \mathrm{aff}(W_0)$ and remark that $\mathrm{aff}(C_j) = A$ and $\mathrm{aff}(V_j) \subseteq \overrightarrow{A}$ for any $j \in J_{r,1}$. Lemma 5.5 shows that there exists $n_r \in \mathbb{N}$, a finite class $\mathcal{H}_r$ of closed half-spaces of A, a sequence $(v_H)_{H\in\mathcal{H}_r}$ of vectors in $\mathbb{R}^m$ such that $\mathcal{H}(W_n) = \{H + n.v_H;\ H \in \mathcal{H}_r\}$ for any $n \geq n_r$. Hence $\mathcal{H}(C_{k_2+r+(n+1).p}) = \{H + n.(v_H + a);\ H \in \mathcal{H}_r\}$ and $\mathrm{aff}(C_{k_2+r+(n+1).p}) = A + n.a\}$ for any $n \geq n_r$.

By considering an integer $k_0 \in \mathbb{N}$ such that $k_0 \geq k_2 + (n_r+1).p$ for any $r \in \{0, \ldots, p-1\}$ such that $J_r \neq \emptyset$, and by considering $k_1 = k_0 + p$, just remark that we have proved the proposition. □

The proof of the theorem 5.2 is obtained by applying the previous proposition to the sequence $(\mathcal{R}^k)_{k\in\mathbb{N}}$ by remarking that $\mathcal{R}^k$ is a rational polyhedral closed convex set of $\mathbb{R}^{2.m}$ for any $k \in \mathbb{N}$.

We obtain the following theorem.

Theorem 5.9 *Let $\mathcal{R}$ be a rational polyhedral closed convex binary relation over $\mathbb{R}^m$ such that acc$(\mathcal{R})$ is definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$. The semi-algorithm provided in figure 5*

```
input: A rational polyhedral closed convex binary relation R.
output: A formula φ(x, x', k) defining acc(R).

k_1 := 1
repeat forever
        for each k_0 < k_1 such that
        R^{k_0+r} and R^{k_1+r} are isomorph
         for every 0 ≤ r ≤ k_1 − k_0 do:
                compute the formula φ := φ_{R,k_0,k_1}
                if ∃x'φ(x, x', k) ∧ x'Rx'' and
                φ(x, x'', k + 1) are equivalent then
                        return φ
                end if
        end do
        k_1 := k_1 + 1
end repeat
```

Figure 5. A complete semi-algorithm

terminates and returns a formula in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ *defining acc*$(\mathcal{R})$.

Proof : Theorem 5.2 and lemma 3.2. $\square$

6 Conclusion

We have presented two new complete semi-algorithms that compute a formula in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ defining the acceleration acc$(\mathcal{R})$ of a binary relation $\mathcal{R}$ definable in this logic: a semi-algorithm for the general class based on an enumerative method, and another one for the restricted class of rational polyhedral closed convex binary relations based on a linear extrapolation of acc$(\mathcal{R})$ from two powers $\mathcal{R}^{k_0}$ and $\mathcal{R}^{k_1}$ of $\mathcal{R}$. Whereas we can easily prove (submitted to CAV'06) that we cannot decide if acc$(\mathcal{R})$ is definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ in the general case, the same problem for the restricted class of rational closed convex binary relations remains an open problem. Finally, remark that we have presented large classes of binary relations whose the acceleration is definable in FO $(\mathbb{R}, \mathbb{Z}, +, \leq)$ and in particular, we deduce directly a new acceleration/flatenning based algorithm for computing the reachability relation of any timed automata.

References

[AAB00] Aurore Annichini, Eugene Asarin, and Ahmed Bouajjani. Symbolic techniques for parametric reasoning about counter and clock systems. In *Proc. 12th Int. Conf. Computer Aided Verification (CAV'2000), Chicago, IL, USA, July 2000*, volume 1855 of *Lecture Notes in Computer Science*, pages 419–434. Springer, 2000.

[ABLS01] Aurore Annichini, Ahmed Bouajjani, Yassine Lakhnech, and Mihaela Sighireanu. Languages, rewriting systems, and verification of infinite-state systems. In *Proc. 8th Int. Symp. Static Analysis (SAS'2001), Paris, France, July 2001*, volume 2126 of *Lecture Notes in Computer Science*, pages 335–355. Springer, 2001.

[AHH96] Rajeev Alur, Thomas A. Henzinger, and Pei-Hsin Ho. Automatic symbolic verification of embedded systems. *IEEE Transactions on Software Engineering*, 22:81–201, 1996.

[BF04] Sébastien Bardin and Alain Finkel. Composition of accelerations to verify infinite heterogeneous systems. In *Proc. 2nd Int. Symp. Automated Technology for Verification and Analysis (ATVA'2004), Taipei, Taiwan, Nov. 2004*, volume 3299 of *Lecture Notes in Computer Science*, pages 248–262. Springer, 2004.

[BFLS05] Sébastien Bardin, Alain Finkel, Jérôme Leroux, and Philippe Schnoebelen. Flat acceleration in symbolic model checking. In *Proc. 3rd Int. Symp. on Automated Technology for Verification and Analysis (ATVA'2005), Taipei, Taiwan, Oct. 2005*, volume 3707 of *Lecture Notes in Computer Science*, pages 474–488. Springer, 2005.

[BJ03] Bernard Boigelot and Frédéric Herbreteau Sébastien Jodogne. Hybrid acceleration using real vector automata. In *Proc. 15th Int. Conf. Computer Aided Verification (CAV'2003), Boulder, CO, USA, July 2003*, volume 2725 of *Lecture Notes in Computer Science*, pages 193–205. Springer, 2003.

[BLW04] Bernard Boigelot, Axel Legay, and Pierre Wolper. Omega-regular model checking. In Springer-Verlag, editor, *Proc. 10th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'2004), Barcelona, March 2004*, Lecture Notes in Computer Science, pages 561–575, 2004.

[CJ98] Hubert Comon and Yan Jurski. Multiple counters automata, safety analysis, and Presburger arithmetic. In *Proc. 10th Int. Conf. Computer Aided Verification (CAV'98), Vancouver, BC,* *Canada, June-July 1998*, volume 1427 of *Lecture Notes in Computer Science*, pages 268–279. Springer, 1998.

[Ler04] Jérôme Leroux. Disjunctive invariants for numerical systems. In *Proc. 2nd Int. Symp. Automated Technology for Verification and Analysis (ATVA'2004), Taipei, Taiwan, Nov. 2004*, volume 3299 of *Lecture Notes in Computer Science*, pages 99–107. Springer, 2004.

[LS05] Jérôme Leroux and Grégoire Sutre. Flat counter automata almost everywhere! In *Proc. 3rd Int. Symp. on Automated Technology for Verification and Analysis (ATVA'2005), Taipei, Taiwan, Oct. 2005*, volume 3707 of *Lecture Notes in Computer Science*, pages 489–503. Springer, 2005.

[Sch87] Alexander Schrijver. *Theory of Linear and Integer Programming*. John Wiley and Sons, New York, 1987.