Disjunctive invariants for numerical systems ⋆ ⋆⋆

Jérôme Leroux

Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, Pavillon André-Aisenstadt, CP 6128 succ Centre Ville, H3C 3J7, Montréal, QC Canada.
leroujer@iro.umontreal.ca

Abstract. We apply linear algebra techniques to over-approximate the reachability relation of a numerical system (Petri nets, counters automata, timed automata and so on) by a transitive and reflexive finite union of affine spaces. Thanks to this kind of approximation, we naturally define the notion of disjunctive place invariants. All the results presented in this paper have been implemented as a plug-in for our symbolic model-checker FAST and applied to the 40 systems available on the FAST-homepage.

1 Introduction

The reachability problem often reduces to the effective computation of the reachability relation of a system. In general this computation is not possible and we cannot even decide if a given state is reachable from an initial one. These undecidability results explain why we are interested in developing some approximated computation of the reachability relation.

In this paper, we are interested in using linear algebra techniques in order to get an over-approximation of the reachability relation of a system that uses $m \geq 1$ rational variables x_1, ..., x_m, called a *numerical system*; This is for instance the case for timed automata, Petri nets and their extensions, and counters automata. Under some algebraic conditions often met, we have proved in [Ler04] that the set of affine relations, also called place invariants $c_0 + \sum_{i=1}^{m}(a_i x_i + a'_i x'_i) = 0$ valid for any couple $((x_1, \dots, x_m), (x'_1, \dots, x'_m))$ in the reachability relation of a numerical system, can be computed in polynomial time. Moreover, we have also shown that the over-approximation of the reachability relation obtained is equal to the least reflexive and transitive affine relation that contains it.

Unfortunately the computation of these invariants are often useless when the analyzed system have some control locations. In fact, in this case, we are naturally interested in computing some affine relations between the variables that depend on the control locations. That means, we want to compute a reflexive

⋆ Research funded by the Faculté des arts et des sciences of the Université de Montréal and by the Natural Sciences and Engineering Research Council of Canada through a discovery grant held by Pierre McKenzie.

⋆⋆ This work was partially carried out during the author's doctoral studies at Lab. Specification and Verification, ENS-Cachan (FRANCE).

and transitive finite union of affine relations (one affine relation for each pair of control locations) that over-approximates the reachability relation.

Our results.

- We introduce the class of finite union of affine spaces, called *semi-affine spaces*. By proving that any infinite intersection of semi-affine spaces remains semi-affine, we show that any relation over $\mathbb{Q}^m$ can be over-approximated by a least reflexive and transitive semi-affine relation called the *semi-affine star hull*. This property proves that independently of the knowledge of the control locations of the considered system, we can define the most precise semi-affine over-approximation.
- We prove that the semi-affine star hull of any affine relation is effectively computable. This result is used in a semi-algorithm for computing the semi-affine star hull of any semi-affine relation when it terminates. Even if the termination of this semi-algorithm is left open, we prove that it stops on a large class of semi-affine relations that enables to compute the semi-affine star hull of the reachability relation of any upward-closed finite linear system, a class that contains any reset/transfer Petri Net [DFS98, Cia94] and any Broadcast protocol [EN98, Del00].
- We have implemented this semi-algorithm as a plug-in for our symbolic model-checker FAST and we have experimented it over all the 40 examples of counters systems freely available on the FAST-homepage [Fas]. Thanks to the approach developed in this paper, our algorithm do not require the user to describe the control location of the system because it discovers them automatically during the computation.

Related works.
In [Kar76], Karr presented a polynomial time algorithm that computes the set of affine relations that hold in a control location of some numerical systems. Recently, the complexity of this algorithm was revisited in [MOS04b] and a fine upper-bound was presented. In [CH78], the use of convex polyhedrons rather than affine spaces allows to discover inequalities between variables $x_1 \leq 2x_2$. By replacing the affine spaces by roots of polynômes with a bounded degree, in [MOS04a], they show that equations of the form $x_1x_2 = x_3$ can be automatically discovered.

The computation of place invariants for many Petri nets extension was studied in [Cia94]. In [Ler04], this computation was proved to be possible for any numerical system as soon as the affine hull of the reachability relation in one steep is computable. For applications of place invariants to the verification of infinite state systems, see for instance [DRV01].

Plan of the paper.
Some definitions and techniques from the field of linear algebra are recalled in section 2. In the next one, we introduce the class of semi-affine spaces and the definition of semi-affine star hull of a relation. After having proved that the semi-affine star hull of an affine relation is effectively computable in section 4,

we show in section 5 how to use these result to implement a semi-algorithm that computes the semi-affine star hull of any semi-affine relation. Finally, in the last section 6, practical results provided by an implementation of the semi-affine star hull as a plug-in of our symbolic model-checker FAST [BFLP03] are presented.

Some proofs had to be omitted due to space constraints. A self-contained long version of this paper (with detailed proofs for all results) can be obtained from the author.

2 Elements of linear algebra

In this section, we recall some classical results of linear algebra.

The cardinal of a finite set X is written $\mathrm{card}(X)$. The set of rational numbers and non negative integers are respectively written $\mathbb{Q}$ and $\mathbb{N}$. The set of vectors with $m \geq 1$ components in a set X is written X^m. The *zero vector* $(0, \dots, 0)$ is just written 0. Given an integer $i \in \{1, \dots, m\}$ and a vector $x \in \mathbb{Q}^m$, the i-th component of x is written $x[i] \in X$. The 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 $i \in \{1, \dots, m\}$, $x, y \in \mathbb{Q}^m$, and $t \in \mathbb{Q}$. For any $i \in \{1, \dots, m\}$, we define the *unity vector* $\mathbf{e}_i \in \mathbb{Q}^m$ by $\mathbf{e}_i[j] = 0$ if $j \neq i$ and $\mathbf{e}_i[i] = 1$. The set of matrices with m rows and n columns in $\mathbb{Q}$ is written $\mathcal{M}_{m,n}(\mathbb{Q})$. When $m = n$, we denote by $\mathcal{M}_m(\mathbb{Q}) = \mathcal{M}_{m,m}(\mathbb{Q})$ the set of *square matrices*. The product of two matrices M, M' is written $M.M'$ and the product of a matrix M by a vector v is written $M.v$. 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 $A, B \subseteq \mathbb{Q}^m$ and $T \subseteq \mathbb{Q}$. When $A = \{a\}$, $B = \{b\}$ or $T = \{t\}$, we have $a + B = \{a\} + B$, $A + b = A + \{b\}$, $t.A = \{t\}.A$ and $T.a = T.\{a\}$.

An *affine space* A of $\mathbb{Q}^m$ is a subset of $\mathbb{Q}^m$ such that for any finite sequence $(t_i)_{i \in I}$ such that $\sum_{i \in I} t_i = 1$, we have $\sum_{i \in I} t_i.A \subseteq A$. The *affine hull* $\mathrm{aff}(X)$ of a set $X \subseteq \mathbb{Q}^m$ is the least affine space for the inclusion that contains X (recall that any infinite intersection of affine spaces remains an affine space). An *affine basis* of an affine space A is a minimal (for the inclusion) finite subset $B \subseteq A$ such that $A = \mathrm{aff}(B)$. Recall that the integer $\mathrm{card}(B) - 1$ is independent of B and its called the *dimension* of A. A *vector space* is an affine space such that $0 \in A$. The *direction* $\overrightarrow{A}$ of a *non empty* affine space A is the vector space defined by $\overrightarrow{A} = A - A$.

We recall the following lemma.

Lemma 2.1. *For any finite sequence of affine spaces $(A_i)_{i \in I}$ with $I \neq \emptyset$, and for any affine space $A \subseteq \bigcup_{i \in I} A_i$, there exists $i \in I$ such that $A \subseteq A_i$.*

For any function $f : D \to \mathbb{Q}^m$ such that $D \subseteq \mathbb{Q}^m$ and for any $i \geq 0$, we denote by f^i the function defined by the induction $f^0(x) = x$ for any $x \in \mathbb{Q}^m$ and $f^{i+1} = f^i \circ f$. For any function $f : D \to \mathbb{Q}^n$ and $f' : D' \to \mathbb{Q}^n$ such that $D, D' \subseteq \mathbb{Q}^m$, functions $f + f'$ and $t.f$ are respectively defined over $D \cap D'$ and D by $(f+f')(x) = f(x)+f'(x)$ and $(t.f)(x) = t.f(x)$. For any function $f : D \to \mathbb{Q}^m$

and for any $X \subseteq \mathbb{Q}^n$ and $Y \subseteq \mathbb{Q}^m$, sets $f(X)$ and $f^{-1}(Y)$ are respectively defined by $f(X) = \{f(x);\ x \in X \cap D\}$ and $f^{-1}(Y) = \{x \in D;\ f(x) \in Y\}$. A function $f : D \rightarrow \mathbb{Q}^m$ with $D \subseteq \mathbb{Q}^n$ is said *affine* if there exists a matrix $M \in \mathcal{M}_{m,n}(\mathbb{Q})$ and a vector $v \in \mathbb{Q}^m$ such that $f(x) = M.x + v$ for any $x \in D$. When $v = 0$, such a function is said *linear*.

The following technical lemma will be useful:

Lemma 2.2. *For any linear function $l : \mathbb{Q}^m \rightarrow \mathbb{Q}^m$, we can effectively compute some vector spaces V_0, V_1 and V_∞ and an integer $p \geq 1$ such that:*

- $\mathbb{Q}^m = V_0 + V_1 + V_\infty$,
- $l^m(V_0) = \{0\}$, $l(V_1) = V_1$, $l(V_\infty) = V_\infty$,
- $(l^p - l^0)^m(V_1) = \{0\}$,
- *For any $n \geq 1$, $(l^{n.p} - l^0)(V_1) = (l^p - l^0)(V_1)$, and*
- *For any $n \geq 1$, $(l^n - l^0)(V_\infty) = V_\infty$.*

A *(binary) relation (over $\mathbb{Q}^m$)* is a subset of $\mathbb{Q}^m \times \mathbb{Q}^m$. The *identity relation* I is defined by $I = \{(x, x);\ x \in \mathbb{Q}^m\}$. The composition of two relations $\mathcal{R}, \mathcal{R}'$ is written $\mathcal{R}.\mathcal{R}'$ and defined by $(x, y') \in \mathcal{R}.\mathcal{R}'$ is and only if there exists $x' \in \mathbb{Q}^m$ such that $(x, x') \in \mathcal{R}$ and $(x', y') \in \mathcal{R}'$. For any relation $\mathcal{R}$ and for any $i \geq 0$, we denote by $\mathcal{R}^i$ the relation defined by the induction $\mathcal{R}^0 = I$ and $\mathcal{R}^{i+1} = \mathcal{R}^i.\mathcal{R}$. A relation $\mathcal{R}$ is said *reflexive* if $I \subseteq \mathcal{R}$ and it is said *transitive* if $\mathcal{R}.\mathcal{R} \subseteq \mathcal{R}$. The *reflexive and transitive closure* $\mathcal{R}^*$ of a relation $\mathcal{R}$ is defined by $\mathcal{R}^* = \bigcup_{i=0}^{\infty} \mathcal{R}^i$.

3 Semi-affine star hull

Recall that we are interested in over-approximating the reachability relation of a numerical system by a reflexive and transitive finite union of affine relations. In this section, we show that there exists a unique minimal such over-approximation called the *semi-affine star hull*.

The following proposition proves that the class of finite union of affine spaces, called *semi-affine spaces*, is stable by any infinite intersection. In particular, the least semi-affine space $\mathrm{saff}(X)$ for the inclusion, that contains a given set $X \subseteq \mathbb{Q}^m$, called the *semi-affine hull*, can be easily defined as the intersection of all the semi-affine spaces that contain X.

Proposition 3.1. *Any finite or infinite intersection of semi-affine spaces is a semi-affine space.*

Proof. Let us first prove by induction over $k \geq -1$ that any non-increasing sequence of semi-affine spaces $(S_n)_{n \geq 0}$ such that the dimension of $\mathrm{aff}(S_0)$ is bounded k, is ultimately constant. If $k = -1$, we have $\mathrm{aff}(S_0) = \emptyset$ and in this case, $(S_n)_{n \geq 0}$ is constant. Now, assume the induction true for an integer $k \geq -1$ and let us consider a non increasing sequence of semi-affine spaces $(S_n)_n n \in \mathbb{N}$ such that the dimension of $\mathrm{aff}(S_n)$ is equal to $k + 1$. Remark that if S_n is an affine space for any $n \geq 0$, then $(S_n)_{n \geq 0}$ is a non increasing sequence of affine spaces. In particular, this sequence is untimely constant. So, we can assume that there exists an integer $n_0 \geq 0$ such that S_{n_0} is not an affine space. There exists a finite class $\mathcal{C}$ of affine spaces such that $S_{n_0} = \bigcup_{A \in \mathcal{C}} A$. Let $A \in \mathcal{C}$. From $A \subseteq S_{n_0} \subseteq S_0 \subseteq \mathrm{aff}(S_0)$, we deduce that the dimension of A is less than or equal to $k+1$. Moreover, if it is equal to $k+1$, from $A \subseteq \mathrm{aff}(S_0)$, we deduce $A = \mathrm{aff}(S_0)$ and we get $S_{n_0} = A$ is an affine space which is a contradiction. As the sequence $(S_n \cap A)_{n \geq 0}$ is a non increasing sequence of semi-affine spaces such that the dimension of $\mathrm{aff}(S_n \cap A) \subseteq A$ is less than or equal to k, the induction hypothesis proves that there exists $n_A \geq 0$ such that $S_n \cap A = S_{n_A} \cap A$ for any $n \geq n_A$. Let us consider $N = \max_{A \in \mathcal{C}}(n_0, n_A)$. For any $n \geq N_A$, we have $S_n \subseteq S_{n_0} = \bigcup_{A \in \mathcal{C}} A$ and $S_n \cap A = S_N \cap A$. Therefore $S_n = S_N$ for any $n \geq N$ and we have proved the induction.

Now, let us consider a non empty class $\mathcal{C}$ of semi-affine spaces and assume by contradiction that $\bigcap_{S \in \mathcal{C}} S$ is not a semi-affine space. We are going to build by induction an increasing sequence $(\mathcal{C}_n)_{n \geq 0}$ of finite subsets of $\mathcal{C}$ such that $\bigcap_{S \in \mathcal{C}_{n+1}} S$ is strictly included in $\bigcap_{S \in \mathcal{C}_n} S$. Let $\mathcal{C}_0 = \emptyset$ and assume that $\mathcal{C}_0$, ..., $\mathcal{C}_n$ are build and let us build $\mathcal{C}_{n+1}$. Remark that $\bigcap_{S \in \mathcal{C}} S$ is not a semi-affine space. Hence, it cannot be equal to the semi-affine space $\bigcap_{S \in \mathcal{C}_n} S$. In particular, there exists $S' \in \mathcal{C}$ such that $S' \not\subseteq \bigcap_{S \in \mathcal{C}_n} S$. Let $\mathcal{C}_{n+1} = \mathcal{C}_n \cup \{S'\}$ and remark that $\bigcap_{S \in \mathcal{C}_{n+1}} S$ is strictly included in $\bigcap_{S \in \mathcal{C}_n} S$. So we can build by induction a strictly decreasing sequence of semi-affine spaces. This is in contradiction with the previous paragraph. Therefore $\bigcap_{S \in \mathcal{C}} S$ is semi-affine. □

Example 3.2. The semi-affine hull of a finite subset $X \subseteq \mathbb{Q}^m$ is equal to X because X is the finite union over $x \in X$ of the affine spaces $\{x\}$.

The following lemma will be useful to compute the semi-affine hull of some sets.

Lemma 3.3.

- *For any infinite subset* $X \subseteq \mathbb{Q}$, *we have* $\mathrm{saff}(X) = \mathbb{Q}$.
- *For any affine function* $f : \mathbb{Q}^m \to \mathbb{Q}^{m'}$ *and for any subset* $X \subseteq \mathbb{Q}^m$, *we have* $\mathrm{saff}(f(X)) = f(\mathrm{saff}(X))$.
- *For any* $X \subseteq X' \subseteq \mathbb{Q}^m$, *we have* $\mathrm{saff}(X) \subseteq \mathrm{saff}(X')$.
- *For any subsets* $X, X' \subseteq \mathbb{Q}^m$, *we have* $\mathrm{saff}(X \cup X') = \mathrm{saff}(X) \cup \mathrm{saff}(X')$.
- *For any subsets* $X, X' \subseteq \mathbb{Q}^m$, *we have* $\mathrm{saff}(X + X') = \mathrm{saff}(X) + \mathrm{saff}(X')$.

Example 3.4. The semi-affine hull of $\mathbb{N}^m$ is equal to $\mathbb{Q}^m$. In fact, from lemma 3.3, we deduce $\mathrm{saff}(\mathbb{N}^m) = \sum_{i=1}^m \mathrm{saff}(\mathbb{N}.\mathbf{e}_i) = \sum_{i=1}^m \mathrm{saff}(\mathbb{N}).\mathbf{e}_i = \sum_{i=1}^m \mathbb{Q}.\mathbf{e}_i = \mathbb{Q}^m$.

Proposition 3.1 also proves that the least reflexive and transitive semi-affine relation $\mathrm{saff}^*(\mathcal{R})$ for the inclusion that contains a given relation $\mathcal{R} \subseteq \mathbb{Q}^m \times \mathbb{Q}^m$, called the *semi-affine star hull*, can also by defined as the intersection of all the reflexive and transitive semi-affine relations that contain $\mathcal{R}$.

Example 3.5. Let us consider the relation $\mathcal{R} = \{(x, x') \in \mathbb{Q} \times \mathbb{Q};\ x' \geq x\}$ corresponding to a transition of a system that uses one clock x. In this case $\mathrm{saff}^*(\mathcal{R}) = \mathbb{Q} \times \mathbb{Q}$.

Example 3.6. Let us consider the relation $\mathcal{R} = \{(x, x'); \in \mathbb{N}^2 \times \mathbb{N}^2;\ x_1 \geq 1\ (x'_1, x'_2) = (0, x_2 + x_1)\}$ that corresponds to the effect of a transition in a counters system that "transfer the value of a counter x_1 into a counter x_2". We have $\mathrm{saff}^*(\mathcal{R}) = I \cup \{(x, x'); \in \mathbb{Q}^2 \times \mathbb{Q}^2;\ (x'_1, x'_2) = (0, x_2 + x_1)\}$ which is *not an affine space.*

4 Computation of the semi-affine star hull of an affine relation

This section contains the proof that the semi-affine star hull of an affine relation $\mathcal{R}$ is effectively computable. In order to get this result, we show that this computation can be reduced to the computation of the semi-affine hull of $\{(x, f^i(x)); i \geq 0\}$ where f is an affine function associated to $\mathcal{R}$.

The *definition domain* $D(\mathcal{R})$ of an affine relation $\mathcal{R}$ is the affine space naturally defined by $D(\mathcal{R}) = \{x \in \mathbb{Q}^m;\ \exists y \in \mathbb{Q}^m\ (x, y) \in \mathcal{R}\}$. For any $x \in D(\mathcal{R})$, the affine space $\mathcal{R}_x = \{y \in \mathbb{Q}^m;\ (x, y) \in \mathcal{R}\}$ is a not empty. Even if $\mathcal{R}_x$ obviously depends on x, the following lemma proves that this is no longer true for its direction $\overrightarrow{\mathcal{R}_x}$.

Lemma 4.1. *For any non empty affine relation $\mathcal{R}$ and for any $x_1, x_2 \in D(\mathcal{R})$ we have $\overrightarrow{\mathcal{R}_{x_1}} = \overrightarrow{\mathcal{R}_{x_2}}$.*

Proof. Let $v \in \overrightarrow{\mathcal{R}_{x_1}}$ and let us prove that $v \in \overrightarrow{\mathcal{R}_{x_2}}$. There exists $(x_1, y), (x_1, y') \in \mathcal{R}$ such that $v = y' - y$. As $x_2 \in D(\mathcal{R})$, there exists $(x_2, y_2) \in \mathcal{R}$. As $\mathcal{R}$ is an affine space, we have $(x_2, y_2 + v) = (x_2, y_2) + (x_1, y') - (x_1, y) \in \mathcal{R}$. Hence $y_2, y_2 + v \in \mathcal{R}_{x_2}$ and we have proved that $v \in \overrightarrow{\mathcal{R}_{x_2}}$. □

Therefore, for any non-empty affine relation $\mathcal{R}$, there exists a unique vector space $V(\mathcal{R})$, called *the direction* of $\mathcal{R}$ such that for any $x \in D(\mathcal{R})$, we have $\overrightarrow{\mathcal{R}_x} = V(\mathcal{R})$. We make the convention $V(\emptyset) = \mathbb{Q}^m$.

Example 4.2. Let $f : D \to \mathbb{Q}^m$ be an affine function defined over a non empty affine space D and let $\mathcal{R} = \{(x, f(x));\ x \in D\}$ be the *graph* of f. In this case, $D(\mathcal{R}) = D$ and $V(\mathcal{R}) = \{0\}$. In fact, we can prove that a non empty affine relation $\mathcal{R}$ is the graph of an affine function if and only if $V(\mathcal{R}) = \{0\}$.

Remark that $(D(\mathcal{R}^i))_{i \geq 0}$ is a decreasing sequence of affine spaces whereas $(V(\mathcal{R}^i))_{i \geq 0}$ is an increasing sequence of vector spaces. Let us denote by $D(\mathcal{R}^\infty) = \bigcap_{i \geq 0} D(\mathcal{R}^i)$ and $V(\mathcal{R}^\infty) = \bigcup_{i \geq 0} V(\mathcal{R}^i)$. The following lemma will be useful to compute effectively these sets.

Lemma 4.3. *For any affine relation $\mathcal{R}$ over $\mathbb{Q}^m$ such that $\mathcal{R}^{m+1} \neq \emptyset$, we have $D(\mathcal{R}^\infty) = D(\mathcal{R}^m)$ and $V(\mathcal{R}^\infty) = V(\mathcal{R}^m)$.*

Sets $D(\mathcal{R}^\infty)$ and $V(\mathcal{R}^\infty)$ enable us to associate to $\mathcal{R}$ an affine function f such that $\mathcal{R}^i$ is easily related to f^i for any $i \geq 0$.

Proposition 4.4. *For any affine relation $\mathcal{R}$ such that $\mathcal{R}^{m+1} \neq \emptyset$, we can effectively compute an affine function $f : D(\mathcal{R}^\infty) \to D(\mathcal{R}^\infty)$ such that for any $i \geq m$, we have:*

$$\mathcal{R}^i = \{(x, f^i(x));\ x \in D(\mathcal{R}^\infty)\} + (\{0\} \times V(\mathcal{R}^\infty))$$

Proof. We first prove that we can compute an affine function $f : \mathbb{Q}^m \to \mathbb{Q}^m$ such that $f(D(\mathcal{R}^{i+1})) \subseteq D(\mathcal{R}^i)$ for any $i \geq 0$ and such that $(x, f(x)) \in \mathcal{R}$ for any $x \in D(\mathcal{R})$. As the sequence $(D(\mathcal{R}^i))_{0 \leq i \leq m}$ is decreasing, we can compute a decreasing sequence B_0, ..., B_m of finite subsets of $\mathbb{Q}^m$ such that B_i is an affine basis of $D(\mathcal{R}^i)$. In particular B_0 is an affine basis of $\mathbb{Q}^m = D(\mathcal{R}^0)$. Let us build a function $F : B_0 \to \mathbb{Q}^m$. For any $b \in B_0 \backslash B_1$, let $F(b) = b$. For any $i \in \{1, \ldots, m-1\}$ and for any $b \in B_i \backslash B_{i+1}$, there exists $(b, y) \in \mathcal{R}^i$. So, we can find $F(b) \in \mathbb{Q}^m$ such that $(b, F(b)) \in \mathcal{R}$ and $(F(b), y) \in \mathcal{R}^{i-1}$. That means $F(b) \in D(\mathcal{R}^{i-1})$. Finally, let $b \in B_m$. As $b \in D(\mathcal{R}^m) = D(\mathcal{R}^{m+1})$, there exists $y \in \mathbb{Q}^m$ such that $(b, y) \in \mathcal{R}^{m+1}$. Hence, there exists $F(b) \in \mathbb{Q}^m$ such that $(b, F(b)) \in \mathcal{R}$ and $(f(b), y) \in \mathcal{R}^m$. So $F(b) \in D(\mathcal{R}^\infty)$. As B_0 is an affine basis of $\mathbb{Q}^m$, there exists a unique affine function f effectively computable such that $f(b) = F(b)$ for any $b \in B_0$. As for any $b \in D(\mathcal{R}^{i+1})$, we have $f(b) \in D(\mathcal{R}^i)$, we deduce $f(D(\mathcal{R}^{i+1})) \subseteq D(\mathcal{R}^i)$. Moreover, as $(b, f(b)) \in \mathcal{R}$ for any $b \in B_1$, we deduce $(x, f(x)) \in \mathcal{R}$ for any $x \in D(\mathcal{R})$.

Now, let us prove by induction over i the following equality $\mathcal{R}^i = \{(x, x');\ x \in D(\mathcal{R}^i);\ x' \in f^i(x) + V(\mathcal{R}^i)\}$. Remark that for $i = 0$ the equality is true. Assume it true for an integer i and let $x \in D(\mathcal{R}^{i+1})$. We have $f(x) \in D(\mathcal{R}^i)$. The induction hypothesis proves that $(f(x), f^i(f(x))) \in \mathcal{R}^i$. As $(x, f(x)) \in \mathcal{R}$, we have $(x, f^{i+1}(x)) \in \mathcal{R}^{i+1}$. By definition of $V(\mathcal{R}^{i+1})$, we have proved that $\mathcal{R}^{i+1} = \{(x, x');\ x \in D(\mathcal{R}^{i+1});\ x' \in f^{i+1}(x) + V(\mathcal{R}^{i+1})\}$ which proves the induction.

As $f(D(\mathcal{R}^{m+1})) \subseteq D(\mathcal{R}^m)$ and $D(\mathcal{R}^{m+1}) = D(\mathcal{R}^m) = D(\mathcal{R}^\infty)$, we have proved the inclusion $f(D(\mathcal{R}^\infty)) \subseteq D(\mathcal{R}^\infty)$. Moreover, from $D(\mathcal{R}^i) = D(\mathcal{R}^\infty)$ and $V(\mathcal{R}^i) = V(\mathcal{R}^\infty)$ for any $i \geq m$, we have proved the proposition. □

Let us now fix an affine relation $\mathcal{R}$ such that $D(\mathcal{R}^\infty) \neq \emptyset$. We denote by $f : D(\mathcal{R}^\infty) \to D(\infty)$ an affine function satisfying proposition 4.4. Let $l : \overrightarrow{D(\mathcal{R}^\infty)} \to \overrightarrow{D(\mathcal{R}^\infty)}$ be the linear function defined by $f(x) - f(x') = l(x - x')$ for any $x, x' \in D(\mathcal{R}^\infty)$. Let V_0, V_1 and V_∞ and $p \geq 1$ satisfying lemma 2.2. We are going to prove that $\mathrm{saff}(\mathcal{R}^*) = \mathrm{saff}^*(\mathcal{R}) = \mathcal{R}'$ where $\mathcal{R}'$ is defined by:

$$\mathcal{R}' = \bigcup_{i=0}^{m-1} \mathcal{R}^i \bigcup_{j=0}^{p-1} \mathrm{aff}(\mathcal{R}^{m+j} \cup \mathcal{R}^{m+j+p})$$

To obtain such an equality, we first show that the vector space $W_d = \mathbb{Q}.(f^{m+p}(d) - f^m(d)) + V_\infty + (l^p - l^0)(V_1)$ does not depend on $d \in D(\mathcal{R}^\infty)$.

Lemma 4.5. *For any $d_1, d_2 \in D(\mathcal{R}^\infty)$, we have $W_{d_1} = W_{d_2}$.*

Proof. From $(f^{m+p}(d_1) - f^m(d_1)) = (f^{m+p}(d_2) - f^m(d_2)) + (l^{m+p} - l^m)(d_1 - d_2)$, we deduce the inclusion $\mathbb{Q}.(f^{m+p}(d_1) - f^m(d_1)) + (l^{m+p} - l^m)(V_1) \subseteq \mathbb{Q}.(f^{m+p}(d_2) -$

$f^m(d_2)) + (l^{m+p} - l^m)(V_1)$. In particular, we have $W_{d_1} \subseteq W_{d_2}$. By symmetry, we have $W_{d_1} = W_{d_2}$. □

Therefore, we can naturally define W as the vector space satisfying $W = W_d$ for any $d \in D(\mathcal{R}^\infty)$.

Lemma 4.6. *For any $j \geq m$ and $n_1 \neq n_2$, we have:*

$$\mathcal{R}^j + (\{0\} \times W) = \mathrm{aff}(\mathcal{R}^{j+n_1.p} \cup \mathcal{R}^{j+n_2.p}) = (W \times \{0\}) + \mathcal{R}^j$$

Thanks to the previous lemma, we prove the following corollary:

Corollary 4.7. *We have* $\mathrm{saff}(\mathcal{R}^*) = \mathrm{saff}^*(\mathcal{R}) = \mathcal{R}'$.

Proof. Let us first prove that $\mathrm{saff}^*(\mathcal{R}) \subseteq \mathcal{R}'$. Lemma 4.6 shows that for any $j, j' \geq m$, we have $\mathcal{R}.\mathrm{aff}(\mathcal{R}^j \cup \mathcal{R}^{j+p}) = \mathcal{R}^{j+1} + (\{0\} \times W) \subseteq \mathcal{R}'$ and $\mathrm{aff}(\mathcal{R}^j \cup \mathcal{R}^{j+p}).\mathrm{aff}(\mathcal{R}^{j'} \cup \mathcal{R}^{j'+p}) = ((W \times \{0\}) + \mathcal{R}^j).(\mathcal{R}^{j'} + (\{0\} \times W)) \subseteq (W \times \{0\}) + \mathcal{R}^{j+j'} + (\{0\} \times W) = \mathcal{R}^{j+j'} + (\{0\} \times W) \subseteq \mathcal{R}'$. Hence $\mathcal{R}'$ is transitive. Moreover, as $\mathcal{R}'$ is reflexive ($I \subseteq \mathcal{R}'$) and contains $\mathcal{R}$, by minimality of the semi-affine star hull, we have $\mathrm{saff}^*(\mathcal{R}) \subseteq \mathcal{R}'$.

Next, we prove $\mathcal{R}' \subseteq \mathrm{saff}(\mathcal{R}^*)$. As $\mathrm{saff}(\mathcal{R}^*)$ is a semi-affine space, there exists a finite class of affine spaces $\mathcal{C}$ such that $\mathrm{saff}(\mathcal{R}^*) = \bigcup_{A \in \mathcal{C}} A$. Let $j \geq m$. As for any $n \geq 0$, we have $\mathcal{R}^{j+n.p} \subseteq \mathrm{saff}(\mathcal{R}^*)$, lemma 2.1 shows that there exists $A_n \in \mathcal{C}$ such that $\mathcal{R}^{j+n.p} \subseteq A_n$. However, the class $\mathcal{C}$ is finite. So there exists $n_1 \neq n_2$ such that $A = A_{n_1} = A_{n_2}$. From $\mathcal{R}^{j+n_1.p} \cup \mathcal{R}^{j+n_2.p} \subseteq A$, we deduce by minimality of the affine hull that $\mathrm{aff}(\mathcal{R}^{j+n_1.p} \cup \mathcal{R}^{j+n_2.p}) \subseteq A \subseteq \mathrm{saff}(\mathcal{R}^*)$. From lemma 4.6, we deduce that $\mathcal{R}' \subseteq \mathrm{saff}^*(\mathcal{R})$.

From $\mathrm{saff}(\mathcal{R}^*) \subseteq \mathrm{saff}^*(\mathcal{R})$ and the two previously proved inclusions, we are done. □

In particular, we have proved the following theorem.

Theorem 4.8. *The semi-affine star hull of any affine relation is effectively computable.*

Remark 4.9. The hard part to implement an algorithm that computes the semi-affine star hull of an affine relation, is the computation of an integer $p \geq 1$ that satisfies lemma 2.2. In fact, when p is computed, we can just use the equality $\mathrm{saff}^*(\mathcal{R}) = \bigcup_{i=0}^{m-1} \mathcal{R}^i \bigcup_{j=0}^{p-1} \mathrm{aff}(\mathcal{R}^{m+j} \cup \mathcal{R}^{m+j+p})$. In [Ler03], a precise analysis of the complexity proves that such an integer p can be computed in polynomial time and it can be bounded by $p \leq (4m)^{2m}$. That shows that the semi-affine star hull of an affine relation is computable in *exponential time* in the *worst case*.

5 Computation of the semi-affine star hull of a semi-affine relation

In the previous section, we have proved that there exists an algorithm that computes the semi-affine star hull of any affine relation. We are going to prove that this algorithm can be naturally used to implement a semi-algorithm that computes the semi-affine star hull of any semi-affine relation when it terminates. Even if we are not able to prove the termination of our semi-algorithm in the general case, we prove that it is sufficient for computing the semi-affine star hull of the reachability relation of any *upward-closed finite linear systems*, a class of systems that contains any reset/transfer Petri Nets [DFS98, Cia94] and any Broadcast Protocols [EN98, Del00].

By definition, for any semi-affine space S, there exists a finite class $\mathcal{C}$ of affine spaces such that $S = \bigcup_{A\in\mathcal{C}} A$. Remark that such a finite class $\mathcal{C}$ is not unique. However, if we only consider the maximal elements of $\mathcal{C}$ for the inclusion, we are going to prove that we obtain a class that only depends on S.

Definition 5.1. *A* component *of a semi-affine space S is a maximal affine space $A \subseteq S$ for the inclusion. The set of components of S is written* $\text{comp}(S)$.

Proposition 5.2. *For any semi-affine space S, the set of components* $\text{comp}(S)$ *is finite and satisfies $S = \bigcup_{A\in\text{comp}(S)} A$. Moreover, for any finite class $\mathcal{C}$ of affine spaces such that $S = \bigcup_{A\in\mathcal{C}} A$, the set of maximal elements in $\mathcal{C}$ for the inclusion is equal to* $\text{comp}(S)$.

Proof. Let S be a semi-affine space. There exists a finite class $\mathcal{C}$ of affine spaces such that $S = \bigcup_{A\in\mathcal{C}} A$. Let us consider the class $\mathcal{C}_0$ of maximal affine spaces in $\mathcal{C}$ for the inclusion and let us prove that $\text{comp}(S) = \mathcal{C}_0$. Let $A \in \text{comp}(S)$. From $A \subseteq \bigcup_{A'\in\mathcal{C}} A'$ and lemma 2.1, we deduce that there exists $A' \in \mathcal{C}$ such that $A \subseteq A'$. By definition of $\mathcal{C}_0$, there exists $A_0 \in \mathcal{C}_0$ such that $A' \subseteq A_0$. Moreover, as $A \in \text{comp}(S)$ and $A \subseteq A_0 \subseteq S$, by maximality of A, we have $A = A_0$ and we have proved that $A \in \mathcal{C}_0$. Now, let us consider $A_0 \in \mathcal{C}_0$. Let us consider an affine space A such that $A_0 \subseteq A \subseteq S$ and let us prove that $A_0 = A$. From $A \subseteq \bigcup_{A'\in\mathcal{C}} A'$, we deduce that there exists $A' \in \mathcal{C}$ such that $A \subseteq A'$. As $A_0 \subseteq A'$ and $A' \in \mathcal{C}$, by maximality of A_0, we deduce $A_0 = A'$. Inclusions $A_0 \subseteq A \subseteq A' = A_0$ show that $A_0 = A$ and we have proved that $A_0 \subseteq S$ is maximal. Hence $A_0 \in \text{comp}(S)$. $\square$

Remark 5.3. The previous proposition enables to canonically represent a semi-affine space by its finite set of components. This is a useful property in order to implement a semi-affine library.

We can now provide our semi-algorithm that computes the semi-affine star hull of a semi-affine relation.

Theorem 5.4. *When semi-algorithm 1 stops, it returns the semi-affine star hull of the input relation.*

Definition 5.5. *A* numerical system *N is a tuple $N = (\Sigma, (\mathcal{R}_a)_{a\in\Sigma})$ where Σ is a finite set of actions and $\mathcal{R}_a$ is a relation over $\mathbb{Q}^m$ defined by a formula in the first order theory $\langle\mathbb{Q}^m, \mathbb{N}^m, +, \leq\rangle$.*

Algorithm 1 Semi-algorithm that computes the semi-affine star hull.

input: A semi-affine relation $\mathcal{R}_0$.
output: The semi-affine star-hull of $\mathcal{R}_0$.

$\mathcal{R} \leftarrow I \bigcup_{\mathcal{R}_a \in \mathrm{comp}(\mathcal{R}_0)} \mathrm{saff}^*(\mathcal{R}_a)$
while $\mathcal{R}.\mathcal{R} \not\subseteq \mathcal{R}$ **do**
  $\mathcal{R} \leftarrow \bigcup_{\mathcal{R}_a, \mathcal{R}_b \in \mathrm{comp}(\mathcal{R})} \mathrm{saff}^*(\mathcal{R}_a.\mathcal{R}_b)$
return $\mathcal{R}$

The termination of semi-algorithm 1 is an open problem. We are going to prove that under some natural conditions over N (often meet in practice), the effective computation of the semi-affine star hull of the *reachability relation* $\mathcal{R}_P^*$ defined as the reflexive and transitive closure of the *reachability relation in one step* $\mathcal{R}_P = \bigcup_{a \in \Sigma} \mathcal{R}_a$, is effectively computable.

An affine function $f : D \to \mathbb{N}^m$ defined over a non empty set $D \subseteq \mathbb{N}^m$ such that $D + \mathbb{N}^m \subseteq D$, is said *upward-closed*. Remark that there exists a unique couple (M_f, v_f) where $M_f \in \mathcal{M}_m(\mathbb{Q})$ and $v_f \in \mathbb{Q}^m$ such that $f(x) = M_f.x + v_f$ for any $x \in D_f$.

Definition 5.6 ([FL02]). *An* upward-closed finite linear system P *is a tuple* $P = (\Sigma, (f_a)_{a \in \Sigma})$ *where* Σ *is a non empty finite alphabet of actions and* f_a *is an upward-closed affine function, such that the monoïd* $\mathcal{M}_P$ *generated by the product of the matrices* M_{f_a}, $a \in \Sigma$ *is finite.*

Naturally, a numerical system $N = (\Sigma, (\mathcal{R}_a)_{a \in \Sigma})$ can be naturally associated to an upward-closed finite linear system $S = (\Sigma, (f_a)_{a \in \Sigma})$ by $\mathcal{R}_a = \{(x, f_a(x));\ x \in D_a\}$. The *reachability relation in one step* $\mathcal{R}_P$ is defined by $\mathcal{R}_P = \bigcup_{a \in \Sigma} \mathcal{R}_a$ and the relation $\mathcal{R}_P^*$ is naturraly called *reachability relation*. Recall that the *reachability problem* that corresponds to decide if a given couple (x, x') is in $\mathcal{R}_P^*$, was proved to be *undecidable* for the reset/transfer Petri nets [DFS98], a *subclass of upward-closed finite linear systems*. However, we are going to prove that the semi-affine star hull of the reachability relation is effectively computable by using the semi-algorithm 1.

Proposition 5.7. *For any upward-closed finite linear system* P*, the semi-affine hull* $\mathrm{saff}(\mathcal{R}_P)$ *is effectively computable and it is equal to* $\bigcup_{a \in \Sigma} \{(x, M_{f_a}.x + v_{f_a});\ x \in \mathbb{Q}^m\}$.

Proof. Let us consider an upward-closed linear function f. We have just to prove that $\mathrm{saff}(\mathcal{R}) = \{(x, M_f.x + v_f);\ x \in \mathbb{Q}^m\}$ where $\mathcal{R} = \{(x, f(x));\ x \in D_f\}$. Let us consider the affine function $F : \mathbb{Q}^m \to \mathbb{Q}^m \times \mathbb{Q}^m$ defined by $F(x) = (x, M_f.x + v_f)$ for any $x \in \mathbb{Q}^m$. As $\mathcal{R} = F(D_f)$, lemma 3.3 proves that $\mathrm{saff}(\mathcal{R}) = F(\mathrm{saff}(D_f))$. As D_f is not empty, there exists $d \in D_f$. Moreover, as $D_f + \mathbb{N}^m \subseteq D_f$, we deduce $d + \mathbb{N}^m \subseteq D_f$. Lemma 3.3 proves that $\mathrm{saff}(d + \mathbb{N}^m) = d + \mathrm{saff}(\mathbb{N}^m)$ and example 3.4 shows that $\mathrm{saff}(\mathbb{N}^m) = \mathbb{Q}^m$. □

Proposition 5.8. *For any upward-closed finite linear system P, the semi-algorithm 1 terminates on the input* $\mathrm{saff}(\mathcal{R}_P)$.

Proof. Let us consider a non empty finite alphabet Σ, and a finite sequence $(f_a)_{a\in\Sigma}$ of affine functions $f_a : \mathbb{Q}^m \to \mathbb{Q}^m$. For any word $\sigma = a_1 \dots a_n$ over Σ, let us consider the affine function f_σ naturally defined by $f_\sigma = f_{a_n} \circ \dots \circ f_{a_1}$ if $n \geq 0$ and $f_\epsilon(x) = x$ for any $x \in \mathbb{Q}^m$ otherwise. The relation $\mathcal{R}_\sigma$ is defined by $\mathcal{R}_\sigma = \{(x, f_\sigma(x));\ x \in \mathbb{Q}^m\}$. Remark that there exists a unique matrix $M_\sigma \in \mathcal{M}_m(\mathbb{Q})$ and a unique vector $v_\sigma \in \mathbb{Q}^m$ such that $f_\sigma(x) = M_\sigma.x + v_\sigma$ for any $x \in \mathbb{Q}^m$. Vector v_σ can be easily linked to the sequence $(M_a, v_a)_{a\in\Sigma}$ by introducing for any word $\sigma = a_1 \dots a_n$ and for any $i \in \{0, \dots, n\}$, the word $\sigma[i] = a_{i+1} \dots a_n$ if $i < n$ and $\sigma[n] = \epsilon$ otherwise. Thanks to this notation, we have $v_\sigma = \sum_{i=1}^{n} M_{\sigma[i]}.v_{a_i}$. We assume that the monoïd $\mathcal{M} = \{M_\sigma;\ \sigma \in \Sigma^*\}$ is finite and we denote by k the cardinal of $\mathcal{M}$. We have to prove that semi-algorithm 1 terminates on $\mathcal{R}_0 = \bigcup_{a\in\Sigma}\{(x, f_a(x));\ x \in \mathbb{Q}^m\}$.

For any word σ, let us denote by $\mathcal{C}_\sigma = \{M_{\sigma[i]};\ i \in \{0, \dots, |\sigma|\}\}$ and let W_σ be the vector space generated by the vectors $M.v_w$ where $M \in \mathcal{C}_\sigma$ and $w \in \Sigma^{\leq k}$ is such that $M.M_w = M$. We can now define the relation $\mathcal{R}' = \bigcup_\sigma(\mathcal{R}_\sigma + (\{0\} \times W_\sigma))$.

We first prove that $\mathrm{saff}^*(\mathcal{R}) \subseteq \mathcal{R}'$ by proving that $\mathcal{R}'$ is transitive and semi-affine.

In order to prove the transitivity, let $x, y, y' \in \mathbb{Q}^m$ such that $(x, y) \in \mathcal{R}_{\sigma_1} + (\{0\} \times W_{\sigma_1}))$ and $(y, y') \in \mathcal{R}_{\sigma_2} + (\{0\} \times W_{\sigma_2}))$. We have $y = f_{\sigma_1}(x) + v_1$ where $v_1 \in W_{\sigma_1}$ and $y' = f_{\sigma_2}(y) + v_2$ where $v_2 \in W_{\sigma_2}$. In particular $y' = f_{\sigma_1\sigma_2}(x) + M_{\sigma_2}(v_1) + v_2$. However, by construction of W_σ, we have $M_{\sigma_2}(W_{\sigma_1}) + W_{\sigma_2} \subseteq W_{\sigma_1\sigma_2}$. In particular $M_{\sigma_2}(v_1) + v_2 \in W_{\sigma_1\sigma_2}$ and we have proved that $y' \in f_{\sigma_1\sigma_2}(x) + W_{\sigma_1\sigma_2}$. We have proved that $\mathcal{R}'$ is transitive.

To show that $\mathcal{R}'$ is semi-affine, we are going to prove that for any word σ such that $|\sigma| \geq k^2$, there exists a word σ' such that $|\sigma'| < |\sigma|$ and $\mathcal{R}_\sigma + (\{0\} \times W_\sigma) \subseteq \mathcal{R}_{\sigma'} + (\{0\} \times W_{\sigma'})$.

Let us prove that there exists $j < j'$ such that $j' - j \leq k$, $M_{\sigma[j]} = M_{\sigma[j']}$ and $\mathcal{C}_{\sigma[j]} = \mathcal{C}_{\sigma[j']}$. As the sequence $(\mathcal{C}_{\sigma[k.i]})_{0\leq i\leq k}$ is a decreasing sequence of sets that contain at least 1 element and at most k elements, there exists $1 \leq i \leq k$ such that $\mathcal{C}_{\sigma[k.(i-1)]} = \mathcal{C}_{\sigma[k.i]}$. Moreover, as $|\mathcal{M}| = k$, there exists j, j' such that $k.(i-1) \leq j < j' \leq k.i$ and $M_{\sigma[j]} = M_{\sigma[j']}$. Now, remark that $j' - j \leq k$, $M_{\sigma[j]} = M_{\sigma[j']}$ and $\mathcal{C}_{\sigma[j]} = \mathcal{C}_{\sigma[j']}$.

As $j < j'$, there exists a word $w \in \Sigma^{j'-j}$ such that $\sigma[j] = w(\sigma[j'])$. Let w' be the word such that $\sigma = w'(\sigma[j])$. Let us prove that we can consider $\sigma' = w(\sigma[j'])$. As $\mathcal{C}_{\sigma[j]} = \mathcal{C}_{\sigma[j']}$, we have $\mathcal{C}_\sigma = \mathcal{C}_{\sigma'}$ and in particular $W_\sigma = W_{\sigma'}$. Moreover, from $M_{\sigma[j]} = M_{\sigma[j']}$, we deduce $M_{\sigma[j']}M_w = M_{\sigma[j']}$. From $M_{\sigma[j']} \in \mathcal{C}_{\sigma'}$, we deduce $M_{\sigma[j']}.v_w \in W_{\sigma'}$. Now, just remark that for any $x \in \mathbb{Q}^m$, we have $f_\sigma(x) = f_{w'.w.(\sigma[j'])}(x) = M_{\sigma[j']}(M_w.f_{w'}(x) + v_w) + v_{\sigma[j']} = f_{\sigma'}(x) + M_{\sigma[j']}.v_w$. We have proved $\mathcal{R}_\sigma + (\{0\} \times W_\sigma) \subseteq \mathcal{R}_{\sigma'} + (\{0\} \times W_{\sigma'})$.

Therefore, $\mathcal{R}'$ is semi-affine.

As $\mathcal{R}'$ is a reflexive and transitive semi-affine relation that contains $\mathcal{R}_0$, by minimality of the semi-affine star hull, we deduce $\text{saff}^*(\mathcal{R}_0) \subseteq \mathcal{R}'$.

Now, remark that any word $\sigma \in \Sigma^*$ can be decomposed into $\sigma = \sigma_0 \dots \sigma_m$ such that there exists a sequence $(w_j)_{1\leq j \leq m}$ of words in $\Sigma^{\leq k}$ satisfying $M_{\sigma_j \dots \sigma_m} M_{w_j} = M_{\sigma_j \dots \sigma_m}$ and such that $W_\sigma = \sum_{j=0}^{m} \mathbb{Q}.M_{\sigma_j \dots \sigma_m}.v_{w_j}$. Let us prove that we have the following equality:

$$\mathcal{R}_\sigma + (\{0\} \times W_\sigma) = \mathcal{R}_{\sigma_0}.\text{saff}(\mathcal{R}_{w_1}^*).\mathcal{R}_{\sigma_1} \dots \text{saff}(\mathcal{R}_{w_m}^*).\mathcal{R}_{\sigma_m} \tag{1}$$

Let $j \in \{1, \dots, m\}$ and let us consider the affine function $F_j : \mathbb{Q}^m \times \mathbb{Q}^m \to \mathbb{Q}^m \times \mathbb{Q}^m$ defined by $F_j(x, x') = (x, f_{\sigma_j \dots \sigma_m}(x'))$. As $M_{\sigma_j \dots \sigma_m} M_{w_j} = M_{\sigma_j \dots \sigma_m}$, we have $f_{\sigma_j \dots \sigma_m}(f_{w_j}^n(x)) = f_{\sigma_j \dots \sigma_m}(x) + n.M_{\sigma_j \dots \sigma_m} v_{w_j}$ for any $x \in \mathbb{Q}^m$ and $n \in \mathbb{N}$. Hence, $F_j(x, f_{w_j}^n(x')) = F_j(x, x') + n.(0, M_{\sigma_j \dots \sigma_m} v_{w_j})$ for any $(x, x') \in \mathbb{Q}^m \times \mathbb{Q}^m$. Lemma 3.3 proves that $\text{saff}(\{F_j(x, f_{w_j}^n(x'));\ n \geq 0;\ x, x' \in \mathbb{Q}^m\}) = F_j(\mathbb{Q}^m \times \mathbb{Q}^m) + \mathbb{Q}.(0, M_{\sigma_j \dots \sigma_m} v_{w_j}) = \mathcal{R}_{\sigma_j \dots \sigma_m} + \mathbb{Q}.(0, M_{\sigma_j \dots \sigma_m} v_{w_j})$ and $\text{saff}(\{F_j(x, f_{w_j}^n(x'));\ n \geq 0;\ x, x' \in \mathbb{Q}^m\}) = F_j(\text{saff}(\{(x, f_{w_j}^n(x');\ n \geq 0;\ x, x' \in \mathbb{Q}^m\} = \text{saff}(\mathcal{R}_{w_j}^*).\mathcal{R}_{\sigma_j \dots \sigma_m}$. We have proved that $\mathcal{R}_{\sigma_j \dots \sigma_m} + \mathbb{Q}.(0, M_{\sigma_j \dots \sigma_m} v_{w_j}) = \text{saff}(\mathcal{R}_{w_j}^*).\mathcal{R}_{\sigma_j \dots \sigma_m}$. An immediate induction proves the equality (1).

Finally, let us consider the semi-affine relation $\mathcal{R}_i$ where $i \geq 1$ is equal to the relation $\mathcal{R}$ in line 6 at its ith execution. Let $i_0 \geq \ln_2(k^2)$. By construction, for any $i \geq i_0$, we have $\text{saff}^*(\mathcal{R}_w) \subseteq \mathcal{R}_i$ for any word $w \in \Sigma^{\leq k}$ and $\mathcal{R}_\sigma \subseteq \mathcal{R}_i$ for any σ such that $|\sigma| \leq k^2$. Let $i_1 \geq \ln_2(m)$ and now remark that for any $i \geq i_0 + i_1$, and for any word σ such that $|\sigma| \leq k^2$, we have $\mathcal{R}_\sigma + (\{0\} \times W_\sigma) \subseteq \mathcal{R}_i$. Therefore, $\mathcal{R}' \subseteq \mathcal{R}_i$. From $\mathcal{R}_i \subseteq \text{saff}^*(\mathcal{R}_0)$ and $\text{saff}^*(\mathcal{R}_0) \subseteq \mathcal{R}'$, we deduce $\mathcal{R}_i = \text{saff}^*(\mathcal{R}_0)$. In particular, after at most $i_0 + i_1$ times line 6 is executed, the condition in line 5 is no longer true and the semi-algorithm terminates. □

Remark 5.9. We can bound the time taken by the semi-algorithm 1 to compute $\text{saff}^*(\mathcal{R}_P)$ exponentially in the size of $\text{saff}(\mathcal{R}_P)$ and the cardinal of the monoïd $\mathcal{M}_P$. Recall that an immediate corollary of [MS77], enables to bound the cardinal of $\mathcal{M}_P$ by an exponential function that only depends on m.

The following lemma is important because it proves that if we can effectively compute the semi-affine hull of a relation $\mathcal{R}$ and if we can also compute the semi-affine star hull of this semi-affine relation, then, in fact we can compute the semi-affine star hull of $\mathcal{R}^*$.

Lemma 5.10. *For any relation $\mathcal{R}$ over $\mathbb{Q}^m$, we have* $\text{saff}^*(\mathcal{R}^*) = \text{saff}^*(\text{saff}(\mathcal{R}))$.

Proof. From $\mathcal{R} \subseteq \mathcal{R}^* \subseteq \text{saff}^*(\mathcal{R}^*)$, we deduce by minimality of the semi-affine hull the inclusion $\text{saff}(\mathcal{R}) \subseteq \text{saff}^*(\mathcal{R}^*)$. By minimality of the semi-affine star hull we get $\text{saff}^*(\text{saff}(\mathcal{R})) \subseteq \text{saff}^*(\mathcal{R}^*)$. Moreover, as $\mathcal{R} \subseteq \text{saff}(\mathcal{R}) \subseteq \text{saff}^*(\text{saff}(\mathcal{R}))$ and $\text{saff}^*(\text{saff}(\mathcal{R}))$ is reflexive and transitive, we deduce $\mathcal{R}^* \subseteq \text{saff}^*(\text{saff}(\mathcal{R}))$. By minimality of the semi-affine star hull, we obtain the other inclusion $\text{saff}^*(\mathcal{R}^*) \subseteq \text{saff}^*(\text{saff}(\mathcal{R}))$. □

Corollary 5.11. *The semi-affine star hull of the reachability relation of an upward-closed finite linear system is effectively computable.*

Proof. Let us consider an upward-closed finite linear system P. Corollary 5.7 proves that $\text{saff}(\mathcal{R}_P)$ is computable. Proposition 5.8 proves that the semi-algorithm 1 terminates on $\text{saff}(\mathcal{R}_P)$ and it computes $\text{saff}^*(\text{saff}(\mathcal{R}_P))$. Lemma 5.10 shows that this semi-affine relation is equal to $\text{saff}^*(\mathcal{R}_P^*)$. □

6 Applications and Implementations

In our symbolic model-checker FAST [BFLP03], a plug-in that computes the semi-affine star hull of an affine relation has been implemented. Moreover, in order to experiment the semi-algorithm 1 over the 40 counters systems provided on the FAST-homepage [Fas], we have implemented an algorithm that computes the semi-affine hull of a set represented by a *Number Decision Diagram (NDD)* [WB00, Ler04], the internal *symbolic representation* used by the tools FAST and LASH [Las]. All the details concerning this implementation can be found in [Ler03].

Semi-algorithm 1 terminates on the computation of the semi-affine star hull of the reachability relation of *almost* all the 40 systems. On some cases the computation was *not possible* because the *reachability relation was finite* but *very large*. In fact, in this case, example 3.2 shows that the number of components of the semi-affine star hull is equal to the number of elements in the reachability relation. Some new *symbolic representations for semi-affine spaces* have to be developped in order to scale with this state space explosion problem.

Rather than providing a long tabular with the semi-affine star hull of the reachability relation of the 40 systems we have considered, we illustrate our method on one of this system, the MESI protocol, a simple cache coherence protocol studied in [EN98].

The MESI protocol is an upward-closed finite linear system $P = (\Sigma, (f_a)_{a\in\Sigma})$ that uses $m = 4$ counters and $|\Sigma| = 3$ actions $\Sigma = \{a_1, a_2, a_3\}$. Vectors in $\mathbb{Q}^4$ are denoted by $(x_{mo}, x_{ex}, x_{sh}, x_{inv})$ (the names of the variable intuitively corresponds to number of memory lines in the states: *modified*, *exclusive*, *shared* and *invalidate*). We have:

- $D_{a_1} = \{x \in \mathbb{N}^4\ x_{inv} \geq 1\}$
  and $f_{a_1}(x_{mo}, x_{ex}, x_{sh}, x_{inv}) = (0, 0, x_{sh} + x_{ex} + x_{mo} + 1, x_{inv} - 1)$.
- $D_{a_2} = \{x \in \mathbb{N}^4\ x_{ex} \geq 1\}$
  and $f_{a_1}(x_{mo}, x_{ex}, x_{sh}, x_{inv}) = (x_{mo} + 1, x_{ex} - 1, x_{sh}, x_{inv})$.
- $D_{a_3} = \{x \in \mathbb{N}^4\ x_{sh} \geq 1 \text{ or } x_{inv} \geq 1\}$
  and $f_{a_1}(x_{mo}, x_{ex}, x_{sh}, x_{inv}) = (0, 1, 0, x_{mo} + x_{ex} + x_{sh} + x_{inv} - 1)$.

The *set of initial states* of the MESI is given by $X_0 = \{(0, 0, 0, x_{inv});\ x_{inv} \in \mathbb{N}\}$. We want to check that for any $(x_0, x') \in \mathcal{R}_P^*$ such that $x_0 \in X_0$, we have $x'_{mo} + x'_{ex} \leq 1$. Let us denote by $\mathcal{R}_{bad}$ the relation corresponding to this property and defined by $(x_{mo}, x_{ex}, x_{sh}, x_{inv})\mathcal{R}_{bad}(x'_{mo}, x'_{ex}, x'_{sh}, x'_{inv})$ if and only if

$(x_{mo}, x_{ex}, x_{sh}, x_{inv}) \in X_0$ and $x'_{mo} + x'_{ex} \geq 2$. We just have to check that $\mathcal{R}_P^* \cap \mathcal{R}_{bad} = \emptyset$.

By computing the semi-affine star hull of the reachability relation of P, we obtain the following semi-affine relation:

$$\begin{array}{c} (x_{mo}, x_{ex}, x_{sh}, x_{inv}) \mathrm{saff}^*(\mathcal{R}_P^*)(x'_{mo}, x'_{ex}, x'_{sh}, x'_{inv}) \\ \text{if and only if} \end{array}$$
$$\begin{array}{l} (x'_{mo} + x'_{ex} = 0 \wedge x'_{sh} + x'_{inv} = x_{mo} + x_{ex} + x_{sh} + x_{inv}) \vee \\ (x'_{mo} = x_{mo} \wedge x'_{ex} = x_{ex} \wedge x'_{sh} = x_{sh} \wedge x'_{inv} = x_{inv}) \vee \\ (x'_{mo} + x'_{ex} = x_{mo} + x_{ex} \wedge x'_{sh} = x_{sh} \wedge x'_{inv} = x_{inv}) \vee \\ (x'_{mo} + x'_{ex} = 1 \wedge x'_{sh} = 0 \wedge x_{mo} + x_{ex} + x_{sh} + x_{inv} = x'_{inv} + 1) \end{array}$$

From $\mathrm{saff}^*(\mathcal{R}_P^*) \cap \mathcal{R}_{bad} = \emptyset$ we deduce the property $\mathcal{R}_P^* \cap \mathcal{R}_{bad} = \emptyset$. However, the computation of the place invariants (the least reflexive and transitive affine relation that contains $\mathcal{R}_P^*$, see [Ler04]) just provides the relation $x'_{mo} + x'_{ex} + x'_{sh} + x'_{inv} = x_{mo} + x_{ex} + x_{sh} + x_{inv}$ which is not sufficient for proving the property. This problem provides from the fact that place invariants provide a large over-aproximation of the reachability relation of a numerical system N as soon as there exists an action $a \in \Sigma$ such that $\mathcal{R}_a$ is "reset/transfer transition". When the numerical system N does not use such a relation, in practice, the semi-affine star hull of the reachability relation $\mathcal{R}_N^*$ is equal to the least reflexive and transitive affine relation that contains $\mathcal{R}_N^*$. This is for instance the case for any *Petri Net* (see [Ler03]).

Acknowledgments: I am delighted to thank my advisor, Alain Finkel for all the interesting remarks he provides me during my doctoral studies.

References

[BFLP03] Sébastien Bardin, Alain Finkel, Jérôme Leroux, and Laure Petrucci. FAST: Fast Acceleration of Symbolic Transition systems. In *Proc. 15th Int. Conf. Computer Aided Verification (CAV'2003), Boulder, CO, USA, July 2003*, volume 2725 of *Lecture Notes in Computer Science*, pages 118–121. Springer, 2003.

[CH78] Patrick Cousot and Nicholas Halbwachs. Automatic discovery of linear restraints among variables of a program. In *Conference Record of the Fifth annual ACM Symposium on Principles of Programming Languages*, pages 84–96. ACM, ACM, January 1978.

[Cia94] Gianfranco Ciardo. Petri nets with marking-dependent arc cardinality: Properties and analysis. In *Proc. 15th Int. Conf. Application and Theory of Petri Nets (ICATPN'94), Zaragoza, Spain, June 1994*, volume 815 of *Lecture Notes in Computer Science*, pages 179–198. Springer, 1994.

[Del00] Gorgio Delzanno. Verification of consistency protocols via infinite-state symbolic model checking: A case study. In *Proc. IFIP Joint Int. Conf. Formal Description Techniques & Protocol Specification, Testing, and Verification (FORTE-PSTV'00), Pisa, Italy, Oct. 2000*, volume 183 of *IFIP Conference Proceedings*, pages 171–186. Kluwer Academic, 2000.

[DFS98] Catherine Dufourd, Alain Finkel, and Philippe Schnoebelen. Reset nets between decidability and undecidability. In *Proc. 25th Int. Coll. Automata, Languages, and Programming (ICALP'98), Aalborg, Denmark, July 1998*, volume 1443 of *Lecture Notes in Computer Science*, pages 103–115. Springer, 1998.

[DRV01] Gorgio Delzanno, Jean-Francois Raskin, and Laurent Van Begin. Attacking symbolic state explosion. In *Proc. 13th Int. Conf. Computer Aided Verification (CAV'2001), Paris, France, July 2001*, volume 2102 of *Lecture Notes in Computer Science*, pages 298–310. Springer, 2001.

[EN98] E. Allen Emerson and Kedar S. Namjoshi. On model checking for non-deterministic infinite-state systems. In *Proc. 13th IEEE Symp. Logic in Computer Science (LICS'98), Indianapolis, IN, USA, June 1998*, pages 70–80. IEEE Comp. Soc. Press, 1998.

[Fas] FAST homepage. `http://www.lsv.ens-cachan.fr/fast/`.

[FL02] Alain Finkel and Jérôme Leroux. How to compose Presburger-accelerations: Applications to broadcast protocols. In *Proc. 22nd Conf. Found. of Software Technology and Theor. Comp. Sci. (FST&TCS'2002), Kanpur, India, Dec. 2002*, volume 2556 of *Lecture Notes in Computer Science*, pages 145–156. Springer, 2002.

[Kar76] Michael Karr. Affine relationship among variables of a program. *Acta Informatica*, 6:133–141, 1976.

[Las] LASH homepage. `http://www.montefiore.ulg.ac.be/~boigelot/research/lash/`.

[Ler03] Jérôme Leroux. *Algorithmique de la vérification des systèmes à compteurs. Approximation et accélération. Implémentation de l'outil Fast.* PhD thesis, Ecole Normale Supérieure de Cachan, Laboratoire Spécification et Vérification. CNRS UMR 8643, décembre 2003.

[Ler04] Jérôme Leroux. The affine hull of a binary automaton is computable in polynomial time. In *5th Int. Workshop on Verification of Infinite-State Systems*, Electronic Notes in Theor. Comp. Sci., 2004. to appear.

[MOS04a] Markus Müller-Olm and Helmut Seidl. Precise interprocedural analysis through linear algebra. In *Proceedings of the 31st ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 330–341. ACM Press, 2004.

[MOS04b] Markus Müller-Olm and Helmut Seidl. A note on karr's algorithm. In *In Proc. 31st Int. Coll. on Automata, Languages and Programming (ICALP'04), Turku, Finland, July 2004*, Lecture Notes in Computer Science. Springer, 2004. To appear.

[MS77] Arnold Mandel and Imre Simon. On finite semigroups of matrices. *Theoretical Computer Science*, 5(2):101–111, October 1977.

[WB00] Pierre Wolper and Bernard Boigelot. On the construction of automata from linear arithmetic constraints. In *Proc. 6th Int. Conf. Tools and Algorithms for the Construction and Analysis of Systems (TACAS'2000), Berlin, Germany, Mar.-Apr. 2000*, volume 1785 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2000.