Decomposition of Decidable First-Order Logics over Integers and Reals

Florent Bouchy[1], Alain Finkel[1], Jérôme Leroux[2]

[1]LSV, CNRS, ENS Cachan [2]LaBRI, CNRS, Université de Bordeaux

TIME 2008
Montréal, QC, Canada

Motivation

Initial observation

Lack of efficient means to verify systems with counters and clocks enjoying at the same time :
effective data structure, expressive guards and actions,
exact computation, decidable automated acceleration.

Motivation

Initial observation

Lack of efficient means to verify systems with counters and clocks enjoying at the same time :
effective data structure, expressive guards and actions, exact computation, decidable automated acceleration.

Objective

- a Tool computing reachable states

Motivation

Initial observation

Lack of efficient means to verify systems with counters and clocks enjoying at the same time :
effective data structure, expressive guards and actions, exact computation, decidable automated acceleration.

Objective

- a Tool computing reachable states
- based on an adapted Symbolic Representation

Motivation

Initial observation

Lack of efficient means to verify systems with counters and clocks enjoying at the same time :
effective data structure, expressive guards and actions, exact computation, decidable automated acceleration.

Objective

- a Tool computing reachable states
- based on an adapted Symbolic Representation
- for systems featuring Integer and Real variables

Motivation

Initial observation

Lack of efficient means to verify systems with counters and clocks enjoying at the same time :
effective data structure, expressive guards and actions, exact computation, decidable automated acceleration.

Objective

- a Tool computing reachable states
- based on an adapted Symbolic Representation
- for systems featuring Integer and Real variables
- to verify models that are generally undecidable

Motivation

Initial observation

Lack of efficient means to verify systems with counters and clocks enjoying at the same time :
effective data structure, expressive guards and actions, exact computation, decidable automated acceleration.

Objective

- a Tool computing reachable states
- based on an adapted Symbolic Representation
- for systems featuring Integer and Real variables
- to verify models that are generally undecidable

☞ *This paper only deals with the symbolic representation for integers and reals*

Outline

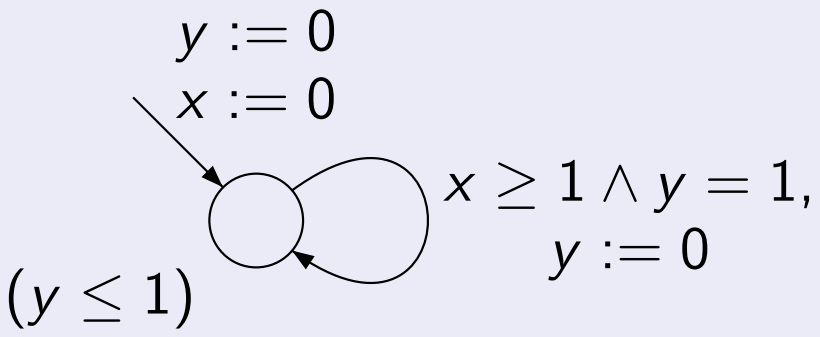
1. **Symbolic Representations for $\mathbb{R}^n$**
   - Difference Bound Matrices (DBM)
   - Abstractions for DBM
   - Parametric DBM
   - Finite Unions of Sums
2. **Decomposition of Decidable Logics**
   - Presburger extended to reals : $\mathrm{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$
   - Constrained Parametric DBM (CPDBM)
   - Real Vector Automata (RVA)
3. **Implementation**
   - GENEPI
   - Integer-Decimal Functions (IDF)

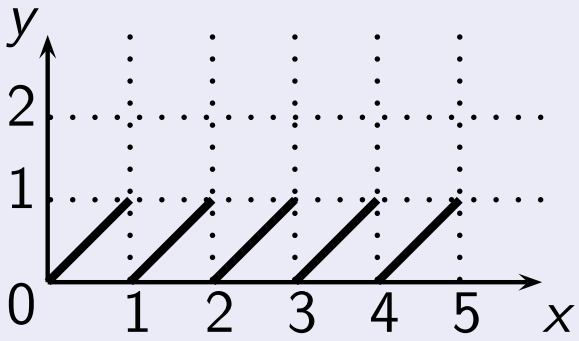
Outline

1. **Symbolic Representations for $\mathbb{R}^n$**
   - Difference Bound Matrices (DBM)
   - Abstractions for DBM
   - Parametric DBM
   - Finite Unions of Sums
2. **Decomposition of Decidable Logics**
   - Presburger extended to reals : $\mathrm{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$
   - Constrained Parametric DBM (CPDBM)
   - Real Vector Automata (RVA)
3. **Implementation**
   - GENEPI
   - Integer-Decimal Functions (IDF)

Example

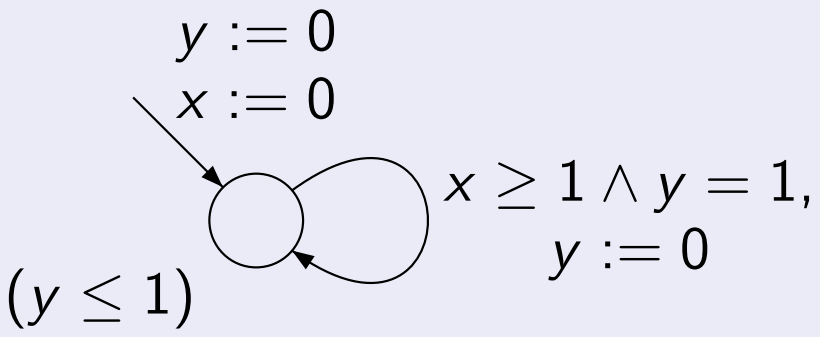
A Timed Automaton from [BBFL03]

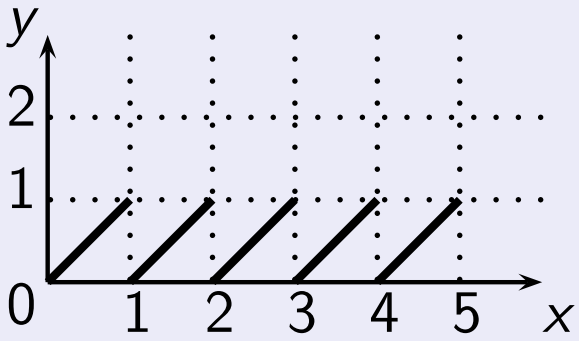




Example

A Timed Automaton from [BBFL03]





An infinity of associated DBM

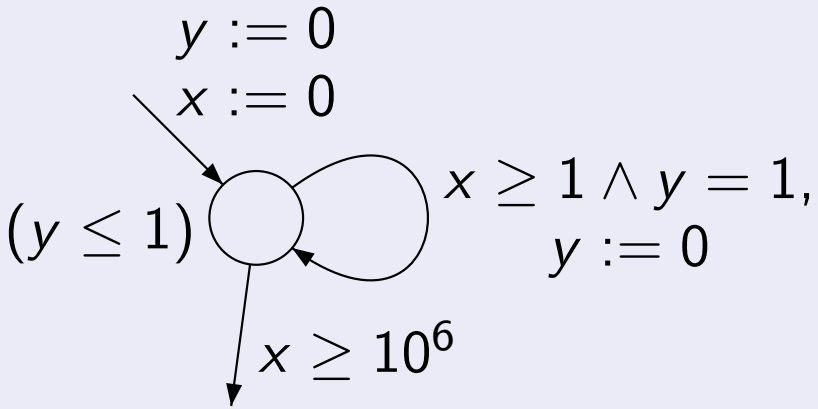
$$\left\{ \begin{array}{c} \\ 0 \\ x \\ y \end{array} \begin{array}{c} \begin{array}{ccc} 0 & x & y \end{array} \\ \begin{pmatrix} 0 & -i & 0 \\ i+1 & 0 & i \\ 1 & -i & 0 \end{pmatrix} \end{array} \right\}_{i \geq 0}$$

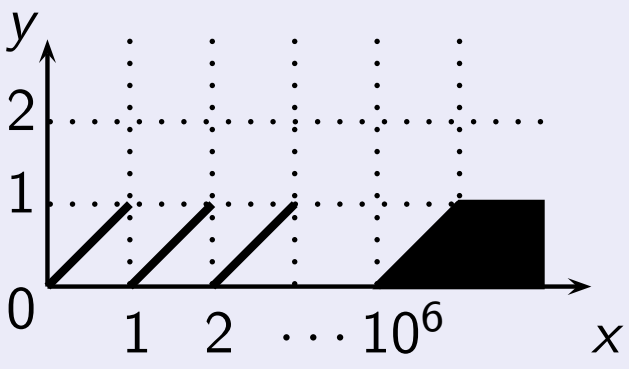
Outline

1. **Symbolic Representations for $\mathbb{R}^n$**
   - Difference Bound Matrices (DBM)
   - Abstractions for DBM
   - Parametric DBM
   - Finite Unions of Sums
2. **Decomposition of Decidable Logics**
   - Presburger extended to reals : $\mathrm{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$
   - Constrained Parametric DBM (CPDBM)
   - Real Vector Automata (RVA)
3. **Implementation**
   - GENEPI
   - Integer-Decimal Functions (IDF)

An example abstraction

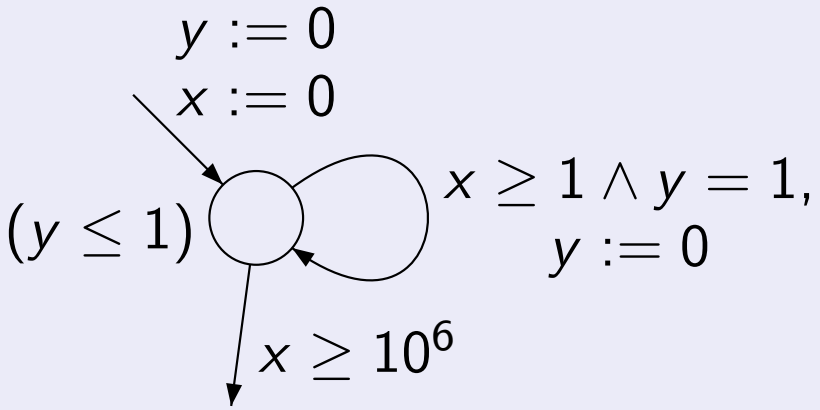
A slight modification of the automaton

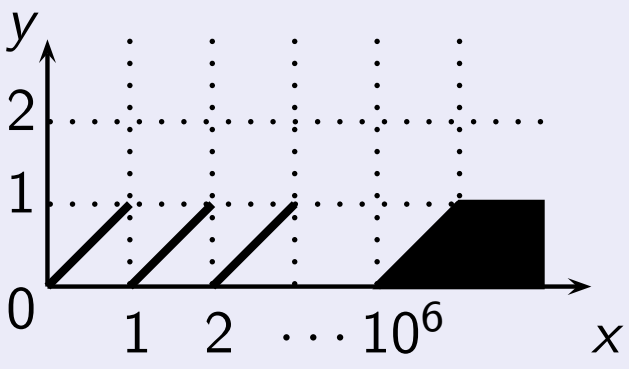




An example abstraction

A slight modification of the automaton





The associated DBM (still too many)

$$\left\{ \left\{ \begin{array}{c} \\ 0 \\ x \\ y \end{array} \begin{array}{c} \begin{array}{ccc} 0 & x & y \end{array} \\ \begin{pmatrix} 0 & -i & 0 \\ i+1 & 0 & i \\ 1 & -i & 0 \end{pmatrix} \end{array} \right\}_{0 \leq i \leq 10^6} , \begin{array}{c} \\ 0 \\ x \\ y \end{array} \begin{array}{c} \begin{array}{ccc} 0 & x & y \end{array} \\ \begin{pmatrix} 0 & \infty & 0 \\ \infty & 0 & \infty \\ 1 & -10^6 & 0 \end{pmatrix} \end{array} \right\}$$

Outline

1. **Symbolic Representations for $\mathbb{R}^n$**
   - Difference Bound Matrices (DBM)
   - Abstractions for DBM
   - Parametric DBM
   - Finite Unions of Sums
2. **Decomposition of Decidable Logics**
   - Presburger extended to reals : $\mathrm{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$
   - Constrained Parametric DBM (CPDBM)
   - Real Vector Automata (RVA)
3. **Implementation**
   - GENEPI
   - Integer-Decimal Functions (IDF)

Parametric DBM

Definition (DBM)

Square matrix composed of elements $(\prec_{i,j}, c_{i,j})$ *in* $\{\leq, <\} \times \mathbb{Z}$ *defining constraints on two clocks* x_i *and* x_j *:* $x_i - x_j \prec_{i,j} c_{i,j}$

Parametric DBM

Definition (DBM)

Square matrix composed of elements $(\prec_{i,j}, c_{i,j})$ *in* $\{\leq, <\} \times \mathbb{Z}$ *defining constraints on two clocks* x_i *and* x_j *:* $x_i - x_j \prec_{i,j} c_{i,j}$

Definition (CPDBM [AAB00])

DBM whose $c_{i,j}$ *are arithmetical terms defined by :*

$$t ::= 0 \mid 1 \mid v \mid t - t \mid t + t \mid t * t, \text{ where } v \in V,\ V \in \{\mathbb{Z}, \mathbb{R}, \dots\}$$

These terms are then constrained by a formula :

$$\phi ::= t \leq t \mid \neg\phi \mid \phi \vee \phi \mid \mathrm{Is\_integer}(t)$$

Outline

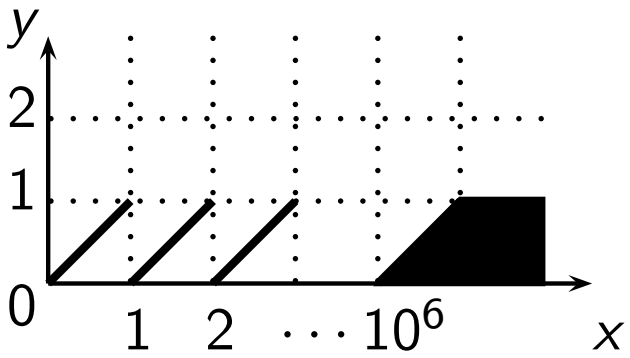
1. **Symbolic Representations for $\mathbb{R}^n$**
   - Difference Bound Matrices (DBM)
   - Abstractions for DBM
   - Parametric DBM
   - Finite Unions of Sums
2. **Decomposition of Decidable Logics**
   - Presburger extended to reals : $\mathrm{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$
   - Constrained Parametric DBM (CPDBM)
   - Real Vector Automata (RVA)
3. **Implementation**
   - Genepi
   - Integer-Decimal Functions (IDF)

Key idea

Extract the integer component from reals, to use periodicity

Key idea

Extract the integer component from reals, to use periodicity



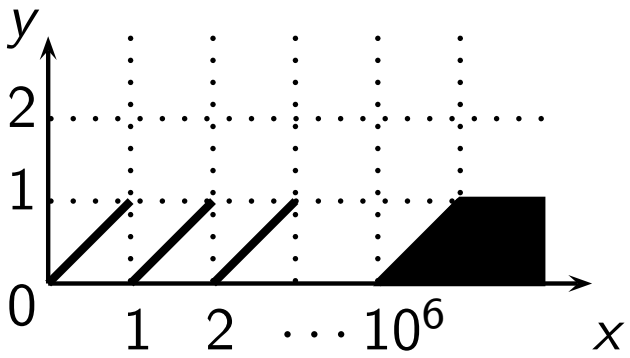
$= \{(x, y) \in [0, 1]^2 \mid x = y\}$

$= \{(x, y) \in [0, 1]^2 \mid x \geq y\}$

$= \{(x, y) \in [0, 1]^2\}$

Key idea

Extract the integer component from reals, to use periodicity



$$\nearrow = \{(x,y) \in [0,1]^2 \mid x = y\}$$
$$\blacktriangle = \{(x,y) \in [0,1]^2 \mid x \geq y\}$$
$$\blacksquare = \{(x,y) \in [0,1]^2\}$$

Finite Unions of Sums "Integer+Decimal"

$$\left(\{0,\ldots,10^6-1\} \times \{0\} + \nearrow\right)$$
$$\bigcup\left(\{10^6\} \times \{0\} + \blacktriangle\right)$$
$$\bigcup\left(\{10^6+1,\ldots,\infty\} \times \{0\} + \blacksquare\right)$$

Our representation

Our representation

- Let $\mathfrak{Z} \subseteq \mathrm{P}(\mathbb{Z}^n)$ and $\mathfrak{D} \subseteq \mathrm{P}(\mathbb{D}^n)$, where $\mathbb{D} = [0, 1[$

Our representation

- Let $\mathfrak{Z} \subseteq \mathrm{P}(\mathbb{Z}^n)$ and $\mathfrak{D} \subseteq \mathrm{P}(\mathbb{D}^n)$, where $\mathbb{D} = [0, 1[$
- Let $\mathfrak{Z} \uplus \mathfrak{D}$ be the class of every $R \subseteq \mathbb{R}^n$ such that $R = \bigcup_{i=1}^{p} (Z_i + D_i)$, where $(Z_i, D_i) \in \mathfrak{Z} \times \mathfrak{D}$ and $p \geq 1$

Our representation

- Let $\mathfrak{Z} \subseteq \mathrm{P}(\mathbb{Z}^n)$ and $\mathfrak{D} \subseteq \mathrm{P}(\mathbb{D}^n)$, where $\mathbb{D} = [0, 1[$
- Let $\mathfrak{Z} \uplus \mathfrak{D}$ be the class of every $R \subseteq \mathbb{R}^n$ such that $R = \bigcup_{i=1}^{p} (Z_i + D_i)$, where $(Z_i, D_i) \in \mathfrak{Z} \times \mathfrak{D}$ and $p \geq 1$
- Note that some R are not representable !

$$\text{Counter-example : } R = \bigcup_{j=1}^{\infty} \left(\{j\} + \left\{ \frac{1}{j+1} \right\} \right)$$

Our representation

- Let $\mathfrak{Z} \subseteq \mathrm{P}(\mathbb{Z}^n)$ and $\mathfrak{D} \subseteq \mathrm{P}(\mathbb{D}^n)$, where $\mathbb{D} = [0, 1[$
- Let $\mathfrak{Z} \uplus \mathfrak{D}$ be the class of every $R \subseteq \mathbb{R}^n$ such that $R = \bigcup_{i=1}^{p} (Z_i + D_i)$, where $(Z_i, D_i) \in \mathfrak{Z} \times \mathfrak{D}$ and $p \geq 1$

Definition

A class $\mathfrak{R} \subseteq \bigcup_{n \in \mathbb{N}} P(\mathbb{R}^n)$ is stable if it is closed under union, intersection, difference, cartesian product, quantification/projection, and permutation.

Our representation

- Let $\mathfrak{Z} \subseteq \mathrm{P}(\mathbb{Z}^n)$ and $\mathfrak{D} \subseteq \mathrm{P}(\mathbb{D}^n)$, where $\mathbb{D} = [0, 1[$
- Let $\mathfrak{Z} \uplus \mathfrak{D}$ be the class of every $R \subseteq \mathbb{R}^n$ such that $R = \bigcup_{i=1}^{p} (Z_i + D_i)$, where $(Z_i, D_i) \in \mathfrak{Z} \times \mathfrak{D}$ and $p \geq 1$

Definition

A class $\mathfrak{R} \subseteq \bigcup_{n \in \mathbb{N}} P(\mathbb{R}^n)$ is stable if it is closed under union, intersection, difference, cartesian product, quantification/projection, and permutation.

Proposition (Stability)

The class $\mathfrak{Z} \uplus \mathfrak{D}$ is stable if $\mathfrak{Z}$ and $\mathfrak{D}$ are stable.

Outline

1. Symbolic Representations for $\mathbb{R}^n$
   - Difference Bound Matrices (DBM)
   - Abstractions for DBM
   - Parametric DBM
   - Finite Unions of Sums
2. **Decomposition of Decidable Logics**
   - Presburger extended to reals : $\mathrm{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$
   - Constrained Parametric DBM (CPDBM)
   - Real Vector Automata (RVA)
3. Implementation
   - GENEPI
   - Integer-Decimal Functions (IDF)

Presburger extended to reals [BRW98, Wei99]

Theorem

$FO(\mathbb{R}, \mathbb{Z}, +, \leq) = FO(\mathbb{Z}, +, \leq) \uplus FO(\mathbb{D}, +, \leq)$

Presburger extended to reals [BRW98, Wei99]

Theorem

$FO(\mathbb{R}, \mathbb{Z}, +, \leq) = FO(\mathbb{Z}, +, \leq) \uplus FO(\mathbb{D}, +, \leq)$

Proof sketch :

$\boxed{\supseteq :}$ trivial.

$\boxed{\subseteq :}$ just distribute sets and relations over $\uplus$:

- $\mathbb{R}^n$ can be written $\mathbb{Z}^n + \mathbb{D}^n$
- $R_+ = \{\mathbf{r} \in \mathbb{R}^3 \mid r_1 + r_2 = r_3\}$ can be written
  $\bigcup_{c \in \{0,1\}} \{\mathbf{z} \in \mathbb{Z}^3 \mid z_1 + z_2 + c = z_3\} + \{\mathbf{d} \in \mathbb{D}^3 \mid d_1 + d_2 = d_3 + c\}$,
  where c stand for a carry
- similarly, $\emptyset$, $\leq$, $\mathbb{Z}^n$ are easily definable
- then, stability (from the previous Proposition) implies $\subseteq$ $\square$

Outline

1. Symbolic Representations for $\mathbb{R}^n$
   - Difference Bound Matrices (DBM)
   - Abstractions for DBM
   - Parametric DBM
   - Finite Unions of Sums
2. **Decomposition of Decidable Logics**
   - Presburger extended to reals : $\mathrm{FO}(\mathbb{R}, \mathbb{Z}, +, \leq)$
   - Constrained Parametric DBM (CPDBM)
   - Real Vector Automata (RVA)
3. Implementation
   - GENEPI
   - Integer-Decimal Functions (IDF)

Constrained Parametric DBM

Reminder : CPDBM [AAB00]

DBM whose $c_{i,j}$ arithmetical terms defined by

$$t ::= 0 \mid 1 \mid v \mid t - t \mid t + t \mid t * t, \text{ where } v \in V \ , V \in \{\mathbb{Z}, \mathbb{R}, \dots\}$$

These terms are then constrained by a formula

$$\phi ::= t \leq t \mid \neg\phi \mid \phi \vee \phi \mid \mathrm{Is\_integer}(t)$$

Constrained Parametric DBM

Reminder : CPDBM [AAB00]

DBM whose $c_{i,j}$ arithmetical terms defined by

$$t ::= 0 \mid 1 \mid v \mid t - t \mid t + t \mid t * t, \text{ where } v \in V \ , V \in \{\mathbb{Z}, \mathbb{R}, \dots\}$$

These terms are then constrained by a formula

$$\phi ::= t \leq t \mid \neg\phi \mid \phi \vee \phi \mid \mathrm{Is\_integer}(t)$$

- $\bigcup \mathrm{DBM}_{\mathbb{D}}$: finite unions of DBM included in $\mathbb{D}^n$

Constrained Parametric DBM

~~CPDBM~~ CP-DBM$_+$

DBM whose $c_{i,j}$ arithmetical terms defined by

$$t ::= 0 \mid 1 \mid v \mid t - t \mid t + t \mid \cancel{t/t/t}, \text{ where } v \in V \ , V \in \{\mathbb{Z}, \mathbb{R}, \dots\}$$

These terms are then constrained by a formula

$$\phi ::= t \leq t \mid \neg\phi \mid \phi \vee \phi \mid \mathrm{Is\_integer}(t) \mid \exists v.\phi$$

- $\bigcup \mathrm{DBM}_{\mathbb{D}}$: finite unions of DBM included in $\mathbb{D}^n$
- CP-DBM$_+$ = CPDBM with quantifiers but without multiplication

Constrained Parametric DBM

~~CPDBM~~ CP-DBM$_+$

DBM whose $c_{i,j}$ arithmetical terms defined by

$$t ::= 0 \mid 1 \mid v \mid t - t \mid t + t \mid \cancel{t/t/t}, \text{ where } v \in V \ , V \in \{\mathbb{Z}, \mathbb{R}, \dots\}$$

These terms are then constrained by a formula

$$\phi ::= t \leq t \mid \neg\phi \mid \phi \vee \phi \mid \mathrm{Is\_integer}(t) \mid \exists v.\phi$$

- $\bigcup \mathrm{DBM}_{\mathbb{D}}$: finite unions of DBM included in $\mathbb{D}^n$
- CP-DBM$_+$ = CPDBM with quantifiers but without multiplication

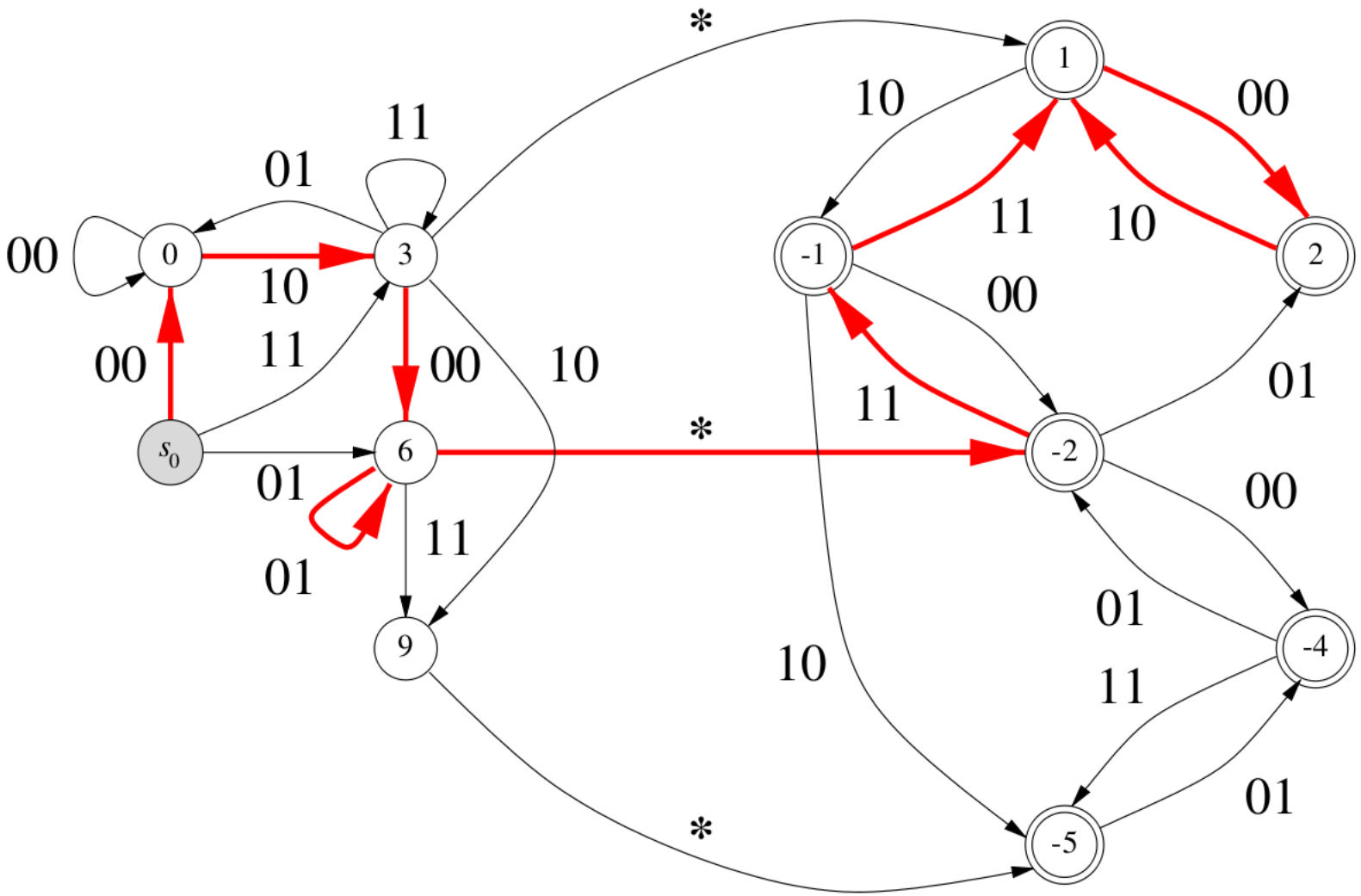
Proposition

$$\bigcup CP\text{-}DBM_+ = FO(\mathbb{Z}, +, \leq) \uplus \bigcup DBM_{\mathbb{D}}$$

Outline

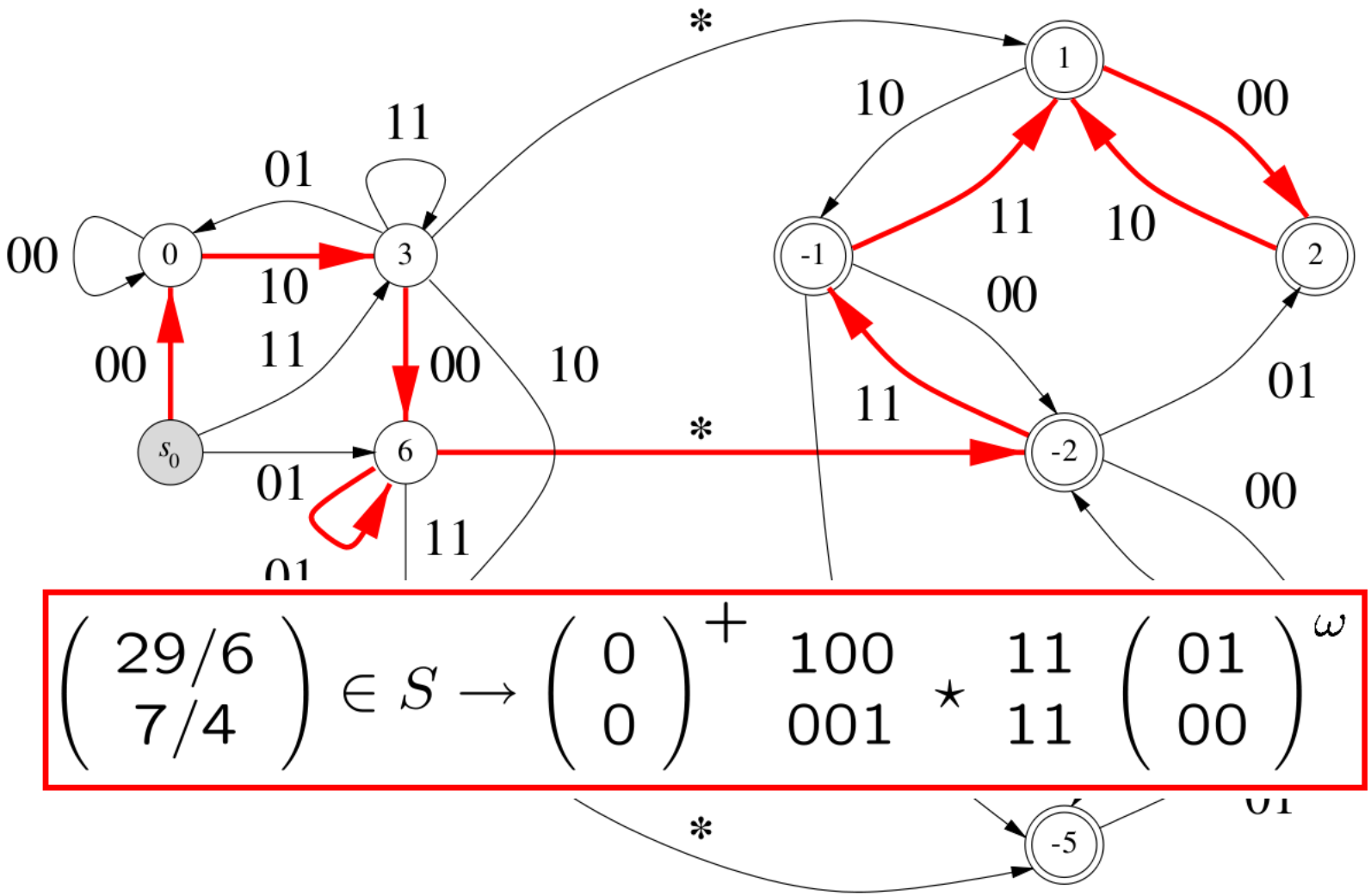
Real Vector Automata (RVA) [BRW98]

$$\{(x, y) \in \mathbb{R}^2 \mid 3x - 6y = 4\}$$



Real Vector Automata (RVA) [BRW98]

$$\{(x,y) \in \mathbb{R}^2 \mid 3x - 6y = 4\}$$



$$\begin{pmatrix} 29/6 \\ 7/4 \end{pmatrix} \in S \rightarrow \begin{pmatrix} 0 \\ 0 \end{pmatrix}^{+} \begin{matrix} 100 \\ 001 \end{matrix} \star \begin{matrix} 11 \\ 11 \end{matrix} \begin{pmatrix} 01 \\ 00 \end{pmatrix}^{\omega}$$

Real Vector Automata (RVA) [BRW98]

Proposition

$FO(\mathbb{R}, \mathbb{Z}, +, \leq, X_b) = FO(\mathbb{Z}, +, \leq, V_b) \uplus FO(\mathbb{D}, +, \leq, W_b)$

Real Vector Automata (RVA) [BRW98]

- $X_b(x, u, a)$ is the predicate being true iff
  - x can be written in basis b as the word $sa_1 \dots a_k \star a_{k+1} \dots$
  - for which $\exists i \in \mathbb{N}$ such that $a_i = a$ and $u = b^{k-i}$

Proposition

$$FO(\mathbb{R}, \mathbb{Z}, +, \leq, X_b) = FO(\mathbb{Z}, +, \leq, V_b) \uplus FO(\mathbb{D}, +, \leq, W_b)$$

Real Vector Automata (RVA) [BRW98]

- $X_b(x, u, a)$ is the predicate being true iff
  - x can be written in basis b as the word $sa_1 \dots a_k \star a_{k+1} \dots$
  - for which $\exists i \in \mathbb{N}$ such that $a_i = a$ and $u = b^{k-i}$
- $V_b : \mathbb{Z}\backslash\{0\} \to \mathbb{Z}$ is the function $V_b(z) = b^j$, where $j \in \mathbb{Z}$ is the greatest integer such that $b^{-j}z \in \mathbb{Z}$

Proposition

$$FO(\mathbb{R}, \mathbb{Z}, +, \leq, X_b) = FO(\mathbb{Z}, +, \leq, V_b) \uplus FO(\mathbb{D}, +, \leq, W_b)$$

Real Vector Automata (RVA) [BRW98]

- $X_b(x, u, a)$ is the predicate being true iff
  - x can be written in basis b as the word $sa_1 \dots a_k \star a_{k+1} \dots$
  - for which $\exists i \in \mathbb{N}$ such that $a_i = a$ and $u = b^{k-i}$
- $V_b : \mathbb{Z}\backslash\{0\} \to \mathbb{Z}$ is the function $V_b(z) = b^j$, where $j \in \mathbb{Z}$ is the greatest integer such that $b^{-j}z \in \mathbb{Z}$
- $W_b : \mathbb{D}\backslash\{0\} \to \mathbb{D}$ is the function $W_b(d) = b^j$, where $j \in \mathbb{Z}$ is the least integer such that $b^{-j}d \notin \mathbb{D}$

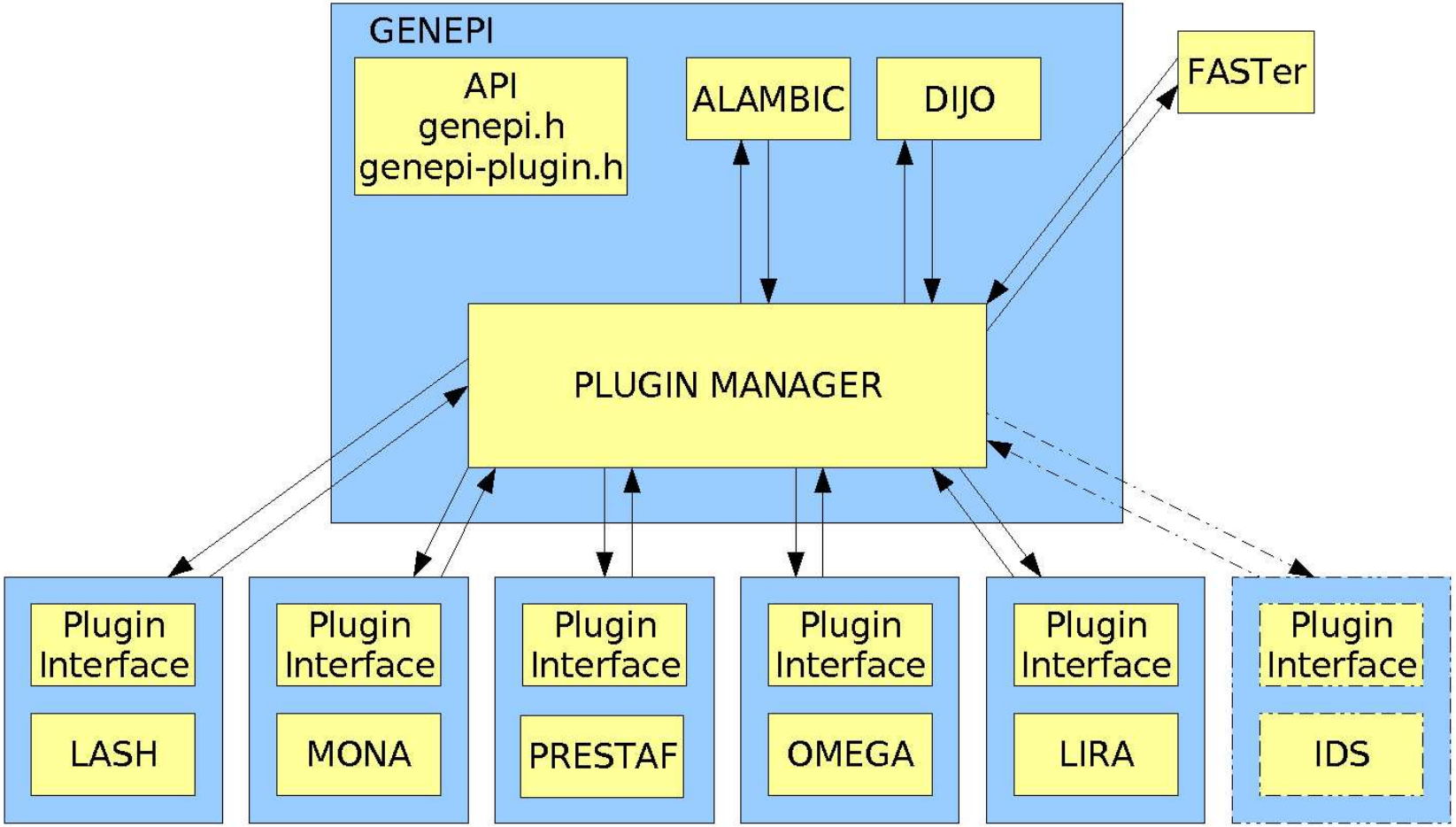
Proposition

$$FO(\mathbb{R}, \mathbb{Z}, +, \leq, X_b) = FO(\mathbb{Z}, +, \leq, V_b) \uplus FO(\mathbb{D}, +, \leq, W_b)$$

Outline

Generic Presburger API [LP06]

GENEPI : A modular framework for solvers and model-checkers



Outline

Integer-Decimal Functions (IDF)

Integer-Decimal Functions (IDF)

- We represent a set $R = \bigcup_{i=1}^{p} (Z_i + D_i)$ by a function :

$$\begin{aligned} f : \mathfrak{Z} &\longrightarrow \mathfrak{D} \\ Z_i &\longmapsto D_i \end{aligned}$$

Integer-Decimal Functions (IDF)

- We represent a set $R = \bigcup_{i=1}^{p} (Z_i + D_i)$ by a function :

$$\begin{aligned} f : \mathfrak{Z} &\longrightarrow \mathfrak{D} \\ Z_i &\longmapsto D_i \end{aligned}$$

- Its support of f is defined by : $\mathrm{supp}(f) = \{Z \mid f(Z) \neq \emptyset\}$

Integer-Decimal Functions (IDF)

- We represent a set $R = \bigcup_{i=1}^{p} (Z_i + D_i)$ by a function :

$$\begin{aligned} f : \mathfrak{Z} &\longrightarrow \mathfrak{D} \\ Z_i &\longmapsto D_i \end{aligned}$$

- Its support of f is defined by : $\text{supp}(f) = \{Z \mid f(Z) \neq \emptyset\}$
- $\mathcal{F}_{\mathfrak{Z} \to \mathfrak{D}} = \{f : \mathfrak{Z} \longrightarrow \mathfrak{D} \mid \text{supp}(f) \text{ is finite}\}$

Integer-Decimal Functions (IDF)

- We represent a set $R = \bigcup_{i=1}^{p} (Z_i + D_i)$ by a function :

$$\begin{aligned} f : \mathfrak{Z} &\longrightarrow \mathfrak{D} \\ Z_i &\longmapsto D_i \end{aligned}$$

- Its support of f is defined by : $\text{supp}(f) = \{Z \mid f(Z) \neq \emptyset\}$
- $\mathcal{F}_{\mathfrak{Z} \to \mathfrak{D}} = \{f : \mathfrak{Z} \longrightarrow \mathfrak{D} \mid \text{supp}(f) \text{ is finite}\}$

Definition (interpretation)

$$\forall f \in \mathcal{F}_{\mathfrak{Z} \to \mathfrak{D}},\ [\![f]\!] = \bigcup_{Z \in supp(f)} \Big(Z + f(Z)\Big)$$

Integer-Decimal Functions (IDF)

Definition (IDF)

An IDF is a function $f \in \mathcal{F}_{\mathfrak{Z} \to \mathfrak{D}}$ *such that* $Z \neq Z'$ *implies* $f(Z) \cap f(Z') = \emptyset$

Integer-Decimal Functions (IDF)

Definition (IDF)

An IDF is a function $f \in \mathcal{F}_{\mathfrak{Z}\to\mathfrak{D}}$ such that $Z \neq Z'$ implies $f(Z) \cap f(Z') = \emptyset$

Let $IDF_{\mathfrak{Z}\to\mathfrak{D}} = \{f \in \mathcal{F}_{\mathfrak{Z}\to\mathfrak{D}} \mid f \text{ is an IDF}\}$
Let $[\![IDF_{\mathfrak{Z}\to\mathfrak{D}}]\!] = \{[\![f]\!] \mid f \in IDF_{\mathfrak{Z}\to\mathfrak{D}}\}$

Proposition (IDF $\equiv$ Finite Unions of Sums)

$\mathfrak{Z} \uplus \mathfrak{D} = [\![IDF_{\mathfrak{Z}\to\mathfrak{D}}]\!]$

Integer-Decimal Functions (IDF)

Definition (IDF)

An IDF is a function $f \in \mathcal{F}_{\mathfrak{Z}\to\mathfrak{D}}$ such that $Z \neq Z'$ implies $f(Z) \cap f(Z') = \emptyset$

Let $IDF_{\mathfrak{Z}\to\mathfrak{D}} = \{f \in \mathcal{F}_{\mathfrak{Z}\to\mathfrak{D}} \mid f \text{ is an IDF}\}$
Let $[\![IDF_{\mathfrak{Z}\to\mathfrak{D}}]\!] = \{[\![f]\!] \mid f \in IDF_{\mathfrak{Z}\to\mathfrak{D}}\}$

Proposition (IDF $\equiv$ Finite Unions of Sums)

$\mathfrak{Z} \uplus \mathfrak{D} = [\![IDF_{\mathfrak{Z}\to\mathfrak{D}}]\!]$

Proposition (Canonicity)

For any $f_1, f_2 \in IDF_{\mathfrak{Z}\to\mathfrak{D}}$, $[\![f_1]\!] = [\![f_2]\!]$ implies $f_1 = f_2$

Conclusion

Contribution

Conclusion

Contribution

- Representation of subsets of $\mathbb{R}^n$ as finite unions

Conclusion

Contribution

- Representation of subsets of $\mathbb{R}^n$ as finite unions
- Decomposition of 3 decidable logics,
  each into 2 separated fragments (*integer* + *decimal*)

Conclusion

Contribution

- Representation of subsets of $\mathbb{R}^n$ as finite unions
- Decomposition of 3 decidable logics,
  each into 2 separated fragments (*integer* + *decimal*)
- Bases for an implementation, as a GENEPI plugin

Conclusion

Future work

Conclusion

Future work

- Implementation/optimisation of the GENEPI plugin

Conclusion

Future work

- Implementation/optimisation of the GENEPI plugin
- Verification of infinite-state systems with counters and clocks

Conclusion

Future work

- Implementation/optimisation of the GENEPI plugin
- Verification of infinite-state systems with counters and clocks
- Extension to other logics decompositions

References

Aurore Annichini, Eugene Asarin, and Ahmed Bouajjani.
Symbolic Techniques for Parametric Reasoning about Counter and Clock Systems.
In CAV, volume 1855 of Lecture Notes in Computer Science, pages 419–434. Springer, 2000.

Gerd Behrmann, Patricia Bouyer, Emmanuel Fleury, and Kim Guldstrand Larsen.
Static Guard Analysis in Timed Automata Verification.
In TACAS, volume 2619 of Lecture Notes in Computer Science, pages 254–277. Springer, 2003.

Bernard Boigelot, Stéphane Rassart, and Pierre Wolper.
On the Expressiveness of Real and Integer Arithmetic Automata (extended abstract).
In ICALP, volume 1443 of Lecture Notes in Computer Science, pages 152–163. Springer, 1998.

Jérôme Leroux and Gérald Point.
The GENEPI Framework, 2006.
http://altarica.labri.fr/wiki/tools:tapas:genepi.

Volker Weispfenning.
Mixed Real-Integer Linear Quantifier Elimination.
In ISSAC, pages 129–136. ACM, 1999.