Combination of accelerations.

Sébastien Bardin

Joint work with Alain Finkel

LSV - CNRS & ENS de Cachan

Laboratoire Spécification et Vérification

Model-checking protocols

Difficult because of

1. data ranging over infinite domains (integers, clocks, queues, parameters, . . .)
2. heterogeneous data types (example: Bounded Retransmission Protocol)

Existing solutions

1. infiniteness:
   - symbolic representation,
   - acceleration or widening.
2. heterogeneity: ??

So when we know acceleration for data type $\mathcal{D}_1$ and acceleration for data type $\mathcal{D}_2$, we do not know anything about $\mathcal{D}_1 \times \mathcal{D}_2$!!

Related work on heterogeneity

- specific approach (counters and clocks, stacks and counters) with *dedicated* acceleration
- upper approximation of post^* by Cartesian product (TReX)
- the Composite Symbolic Library, or algebraic BDDs: nice methods for post, but does not work for acceleration.

Our objective

$\mathcal{D}$ is a domain, $\mathcal{S}$ a symbolic representation and post^* an acceleration.

Given $(\mathcal{D}_1, \mathcal{S}_1, \mathsf{post}^*{}_1)$ and $(\mathcal{D}_2, \mathcal{S}_2, \mathsf{post}^*{}_2)$, we want to deduce a symbolic representation and an acceleration for $\mathcal{D}_1 \times \mathcal{D}_2$.

Transition systems

Definition 1 (transition system) *A transition system is a pair $(D, \rightarrow)$ where D is a set (the domain) and $\rightarrow \subseteq D \times D$ is the transition relation.*

Definition 2 (finitely presented transition system) *A transition system $(D, \rightarrow)$ is finitely presented if there exist $m \geq 0$ recursive relations $r_i \subseteq \mathcal{D} \times \mathcal{D}$ such that $\rightarrow = (r_1, \ldots, r_m)^*$. Let $\mathcal{R} = \{r_1, \ldots, r_m\}$. We write $(D, \mathcal{R})$ for $(D, \rightarrow)$.*

Definition 3 (heterogeneous system) *A heterogeneous system is a transition system $\mathcal{H} = (D, \rightarrow)$ such that there exist $n \geq 2, k_1, \ldots, k_n \in \mathbb{N}$ and n sets $\mathcal{D}_i$ such that $\mathcal{D} = \mathcal{D}_1^{k_1} \times \ldots \times \mathcal{D}_n^{k_n}$ written $\times \mathcal{D}_i^{k_i}$.*

In the following, the transition systems we consider are all finitely presented heterogeneous systems, written $(\times \mathcal{D}_i^{k_i}, \mathcal{R})$

Symbolic representations

Definition 4 (symbolic representation) *A symbolic representation for a finitely presented transition system $\mathcal{H} = (D, \mathcal{R})$ is a 5-uplet $\mathcal{S} = (\mathsf{S}, \gamma, \sqcup, \sqsubseteq, \mathsf{post})$ verifying:*

1. $\gamma(\mathsf{s}_1 \sqcup \mathsf{s}_2) = \gamma(\mathsf{s}_1) \cup \gamma(\mathsf{s}_2)$ *(consistancy of union);*
2. $\gamma(\mathsf{post}(r, \mathsf{s})) = r(\gamma(\mathsf{s}))$ *(consistancy of* post*);*
3. $\mathsf{s}_1 \sqsubseteq \mathsf{s}_2 \Rightarrow \gamma(\mathsf{s}_1) \subseteq \gamma(\mathsf{s}_2)$ *(consistancy of inclusion).*

Some examples

- UBAs, NDDs and RVAs for $\mathbb{N}, \mathbb{Z}$, and $\mathbb{R}$.
- CPDBM for clocks and counters.
- QDDs , SLRE and CQDDs for perfect FIF0 queues or stacks.
- SRE for lossy FIFO channels.
- SMS for pointers.

Acceleration

Definition 5 (symbolic reachability set problem)

- *Input*
  - *a finitely presented transition system* $\mathcal{H} = (\mathcal{D}, \mathcal{R})$,
  - $\mathcal{S} = (\mathsf{S}, \gamma, \sqcup, \sqsubseteq, \mathsf{post})$ *a symbolic representation for* $\mathcal{H}$,
  - *an initial symbolic state* $\mathsf{s}_0 \in \mathsf{S}$,
- *Output:* $\mathsf{s}' \in \mathsf{S}$ *such that* $\mathcal{R}^*(\gamma(\mathsf{s}_0)) = \gamma(\mathsf{s}')$.

Definition 6 (acceleration function) *Consider* $\mathcal{H} = (\mathcal{D}, \mathcal{R})$ *a finitely presented transition system and* $\mathcal{S} = (\mathsf{S}, \gamma, \sqcup, \sqsubseteq, \mathsf{post})$ *a symbolic representation for* $\mathcal{H}$. *An acceleration function for* $(\mathcal{H}, \mathcal{S})$ *is a computable totally defined function* $\mathsf{post}^* : \mathcal{R}^* \times \mathsf{S} \to \mathsf{S}$ *such that*

$$\forall r, \mathsf{s} \in \mathcal{R}^* \times \mathsf{S}, \gamma(\mathsf{post}^*(r, \mathsf{s})) = r^*(\gamma(\mathsf{s}))$$

.

Weak heterogeneous systems

Definition 7 (weak heterogeneous systems) *Let $\mathcal{H} = (\times \mathcal{D}_i^{k_i}, \mathcal{R})$ be a finitely presented heterogeneous system. $\mathcal{H}$ is weakly heterogeneous if there exist n $\mathcal{R}_i$ finite sets of relations over $\mathcal{D}_i^{k_i} \times \mathcal{D}_i^{k_i}$ such that $\mathcal{R} \subseteq \times \mathcal{R}_i$. We write $\mathcal{H} = (\times \mathcal{D}_i^{k_i}, \mathcal{R}, \times \mathcal{R}_i)$.*

- *Data types are strongly encapsulated*. Each data has its own operations, and the whole system is built combining these operations.
- *Consistent with modular or object oriented design*.
- Can model communication protocols using channels with finite sets of messages, (parameterized) maximum number of reemissions and clocks for abortion (ABP,BRP,...)
- Cannot model writing the value of a counter into a queue, since it implies *mixing the structures of the data types, and not only their operations*.

In the following, we want to derive algorithms or properties on the whole system $\mathcal{H}$ from the study of projected systems $(\mathcal{D}_i^{k_i}, \mathcal{R}_i)$.

First results

We define the Cartesian product of $\mathcal{S}_1 = (\mathsf{S}_1, \gamma_1, \sqcup_1, \sqsubseteq_1, \mathsf{post}_1)$ and $\mathcal{S}_2 = (\mathsf{S}_2, \gamma_2, \sqcup_2, \sqsubseteq_2, \mathsf{post}_2)$ by $\mathcal{S}_1 \times \mathcal{S}_2 = (\mathcal{P}_f(\mathsf{S}_1 \times \mathsf{S}_2), \gamma_1 \times \gamma_2, \sqcup, \sqsubseteq_1 \times \sqsubseteq_2, \mathsf{post}_1 \times \mathsf{post}_2)$.

Theoreme 1 *If $\mathcal{S}_1$ is a symbolic representation for $(\mathcal{D}_1^{k_1}, \mathcal{R}_1)$ and $\mathcal{S}_2$ is a symbolic representation for $(\mathcal{D}_2^{k_2}, \mathcal{R}_2)$ then $\mathcal{S}_1 \times \mathcal{S}_2$ is a symbolic representation for all weak heterogeneous systems $(\mathcal{D}_1^{k_1} \times \mathcal{D}_2^{k_2}, \mathcal{R}, \mathcal{R}_1 \times \mathcal{R}_2)$.*

Result used in the Composite Symbolic Library (ALV).

Does not hold for acceleration.

- $r_1^*(d_1) \times r_2^*(d_2) = \bigcup_{i\in\mathbb{N}} \bigcup_{j\in\mathbb{N}} r_1^i(d_1) \times r_2^j(d_2)$ (1)
- $(r_1 \times r_2)^*(d_1, d_2) = \bigcup_{k\in\mathbb{N}} r_1^k(d_1) \times r_2^k(d_2)$ (2)
- (2) $\subseteq$ (1).

Ideas

The previous proof relies on the non synchronization of the number of iteration.

Idea:

- hypothesis on the transition system: weak heterogeneous;
- hypothesis on the symbolic representation: must have a *counting* part;
- hypothesis on the acceleration function: must use the counting part to model explicitly the number of iterations.

Then we want to define a variant of Cartesian product, synchronizing the representations of iterations.

Presburger symbolic representation

Definition 8 (Presburger symbolic representation) *Let $\mathcal{H} = (\mathcal{D}, \mathcal{R})$ be a finitely presented transition system. A Presburger symbolic representation for $\mathcal{H}$ is an effective symbolic representation $\mathcal{S}p = (\mathsf{Sp}, \gamma, \sqcup, \sqsubseteq, \mathsf{post})$ such that:*

- Sp *is a set of 2-uplets* $\mathsf{sp} = (w, \Phi(\overline{w}))$ *with:*
  - w *is a word over a language* $\mathcal{L}$*,*
  - $\overline{w}$ *is a finite set of variables associated to* $w \in \mathcal{L}$*,*
  - $\Phi(\overline{w})$ *is a Presburger formula whose free variables are in* $\overline{w}$*.*
- *the concretization function* γ *is defined as follow:*
  - *there exists a function* $\gamma_a : (w : \mathcal{L}) \times \mathbb{N}^{|\overline{w}|} \to \mathcal{D}$
  - $\gamma((w, \Phi(\overline{w}))) = \bigcup_{v \in \Phi} \gamma_a(w, v)$
- $\mathsf{post}(r, (w, \Phi(\overline{w}))) = (w', \exists \overline{w}.\Phi(\overline{w}) \wedge \varphi(\overline{w}, \overline{w}'))$ *where* w' *and* φ *depend only of* r *and* w*.*

Counting acceleration

Definition 9 (Counting acceleration) *Let $\mathcal{H} = (\mathcal{D}, \mathcal{R})$ be a finitely presented transition system and $\mathcal{S}p = (\mathsf{Sp}, \gamma, \sqcup, \sqsubseteq, \mathsf{post})$ a Presburger symbolic representation for $\mathcal{H}$. A counting acceleration for $(\mathcal{H}, \mathcal{S}p)$ is an acceleration function post^* for $(\mathcal{H}, \mathcal{S}p)$ such that $\forall \mathsf{sp} = (w, \Phi(\overline{w})) \in \mathsf{Sp}, \forall r \in \mathcal{R}$,*

- $\mathsf{post}^*(r, (w, \Phi(\overline{w}))) = (w', \exists \theta \in \mathbb{N}. \exists \overline{w}. \Phi(\overline{w}) \wedge \varphi(\overline{w}, \overline{w}', \theta))$ *where* (w', φ) *depends only of* r *and* w *;*
- $\gamma((w', \exists \theta \in \mathbb{N}. \exists \overline{w}. \Phi(\overline{w}) \wedge \varphi(\overline{w}, \overline{w}', \theta) \wedge \theta = i)) = r^i(\gamma(w, \Phi(\overline{w})))$.

Synchronized product

Synchronized product of Presburger symbolic representations

- Input: $(w_1, \Phi_1(\overline{w_1}))$ and $(w_2, \Phi_2(\overline{w_2}))$
- Output: $(w_1, w_2, \Phi(\overline{w_1}, \overline{w_2}))$.

We can define an acceleration for it.

- Input:
  - ➤ $\text{post}^*_1 : (r, w_1) \to (w_1', \varphi_1(\overline{w_1}, \overline{w_1}', \theta))$,
  - ➤ $\text{post}^*_2 : (r, w_2) \to (w_2', \varphi_2(\overline{w_2}, \overline{w_2}', \theta))$
- Output: $\text{post}^*_:(r, (w_1, w_2)) \to ((w_1', w_2'), \varphi_1(\overline{w_1}, \overline{w_1}', \theta) \wedge \varphi_2(\overline{w_2}, \overline{w_2}', \theta))$

Theoreme 2 *Let $\mathcal{H} = (\times \mathcal{D}_i^{k_i}, \mathcal{R} \subseteq \times \mathcal{R}_i)$ a weak heterogeneous system. Assume that for all i, there exists $\mathcal{S}p_i$ a Presburger symbolic representation for $\mathcal{H}_i = (\mathcal{D}_i^{k_i}, \mathcal{R}_i)$ and post^*_i a counting acceleration for $(\mathcal{H}_i, \mathcal{S}p_i)$. Then*

- *$\bigotimes \mathcal{S}p_i$ is a Presburger symbolic representation for $\mathcal{H}$,*
- *there exists a counting acceleration for $(\mathcal{H}, \mathcal{S}p_i)$.*

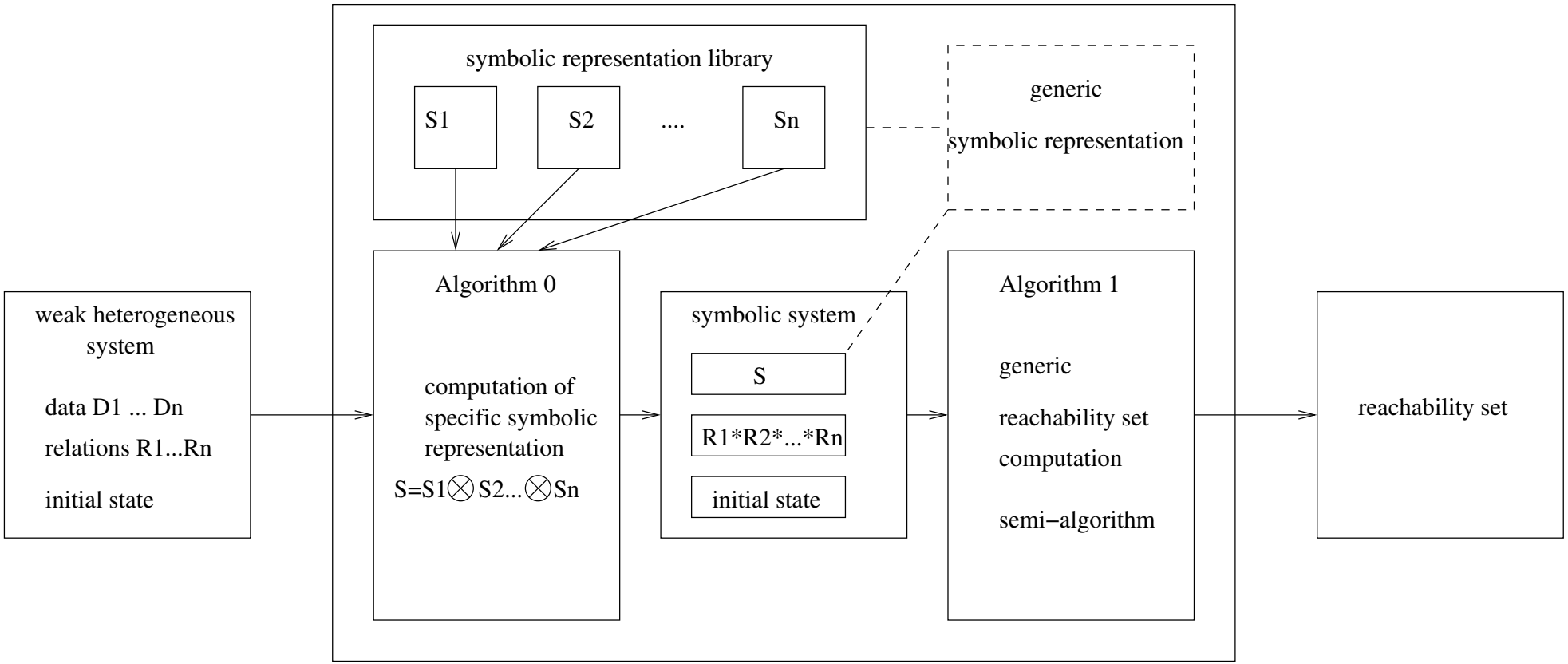
Laboratoire Spécification et Vérification

Existing symbolic representations

	data	effective symbolic representation	post*/ counting
SRE	lossy queues	yes	yes/no
QDD	queues/stacks	yes	yes/no
SLRE	queues/stacks	yes	yes/no
CQDD	**queues/stacks**	**yes**	**yes**
UBA/NDD	**counters**	**yes**	**yes**
RVA	**clocks and counters**	**yes**	**yes**
SMS	pointers	yes	?
CPDBMs	clocks and counters	$\sqsubseteq$ semi-decidable	semi-decidable

Theoreme 3 *A symbolic representation and an acceleration function can be computed automatically for weak heterogeneous systems manipulating counters, clocks, perfect FIFO queues and stacks.*

Toward a generic tool



Laboratoire Spécification et Vérification

Perspective

- heuristics and termination results from the projections on each data type,
- theoretical work on getting more efficient combinations,
- a tool.