TReX

TReX
A Tool for Reachability Analysis of CompleX Systems

Ahmed Bouajjani, Aurore Collomb, and Mihaela Sighireanu

http://www.liafa.jussieu.fr/~sighirea/trex/

Outline

- Motivation
- Aims
- Methodology
- TReX core techniques
  - Symbolic representations
  - Extrapolation of reached configurations
- New open architecture
- Future work

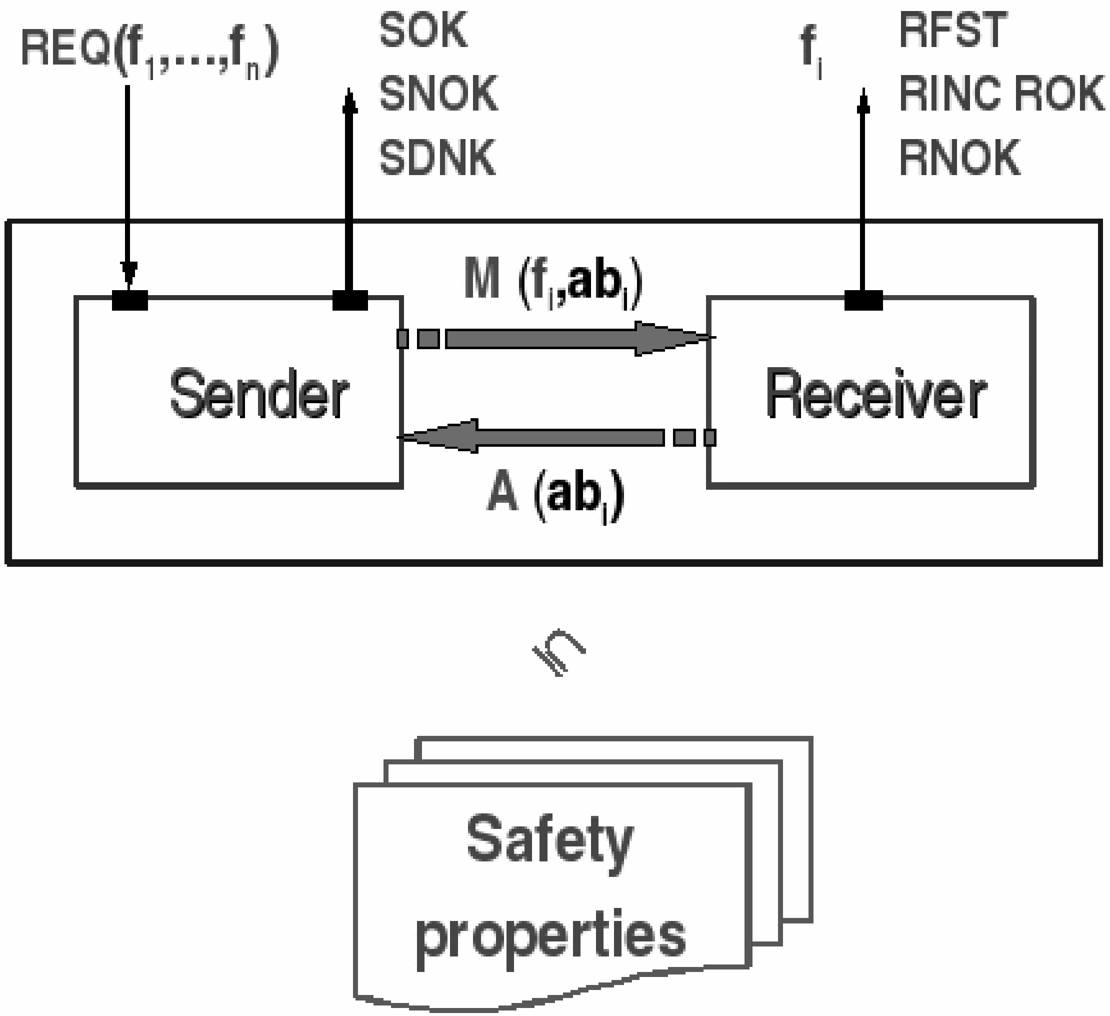
Motivation: Verification of Communication Protocols

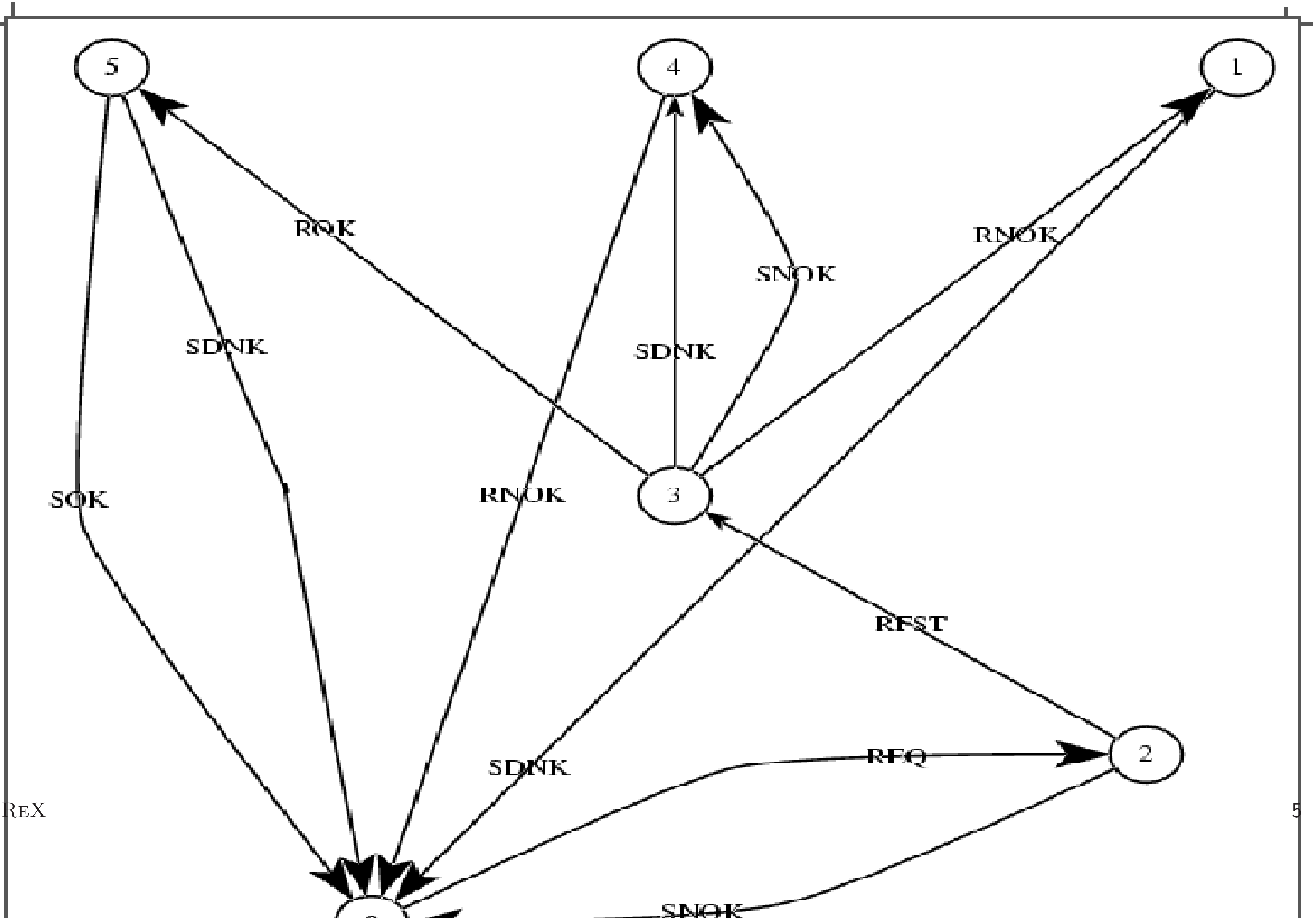
New generation of communication protocols (e.g., BRP, IEEE 1394, PGM) uses:

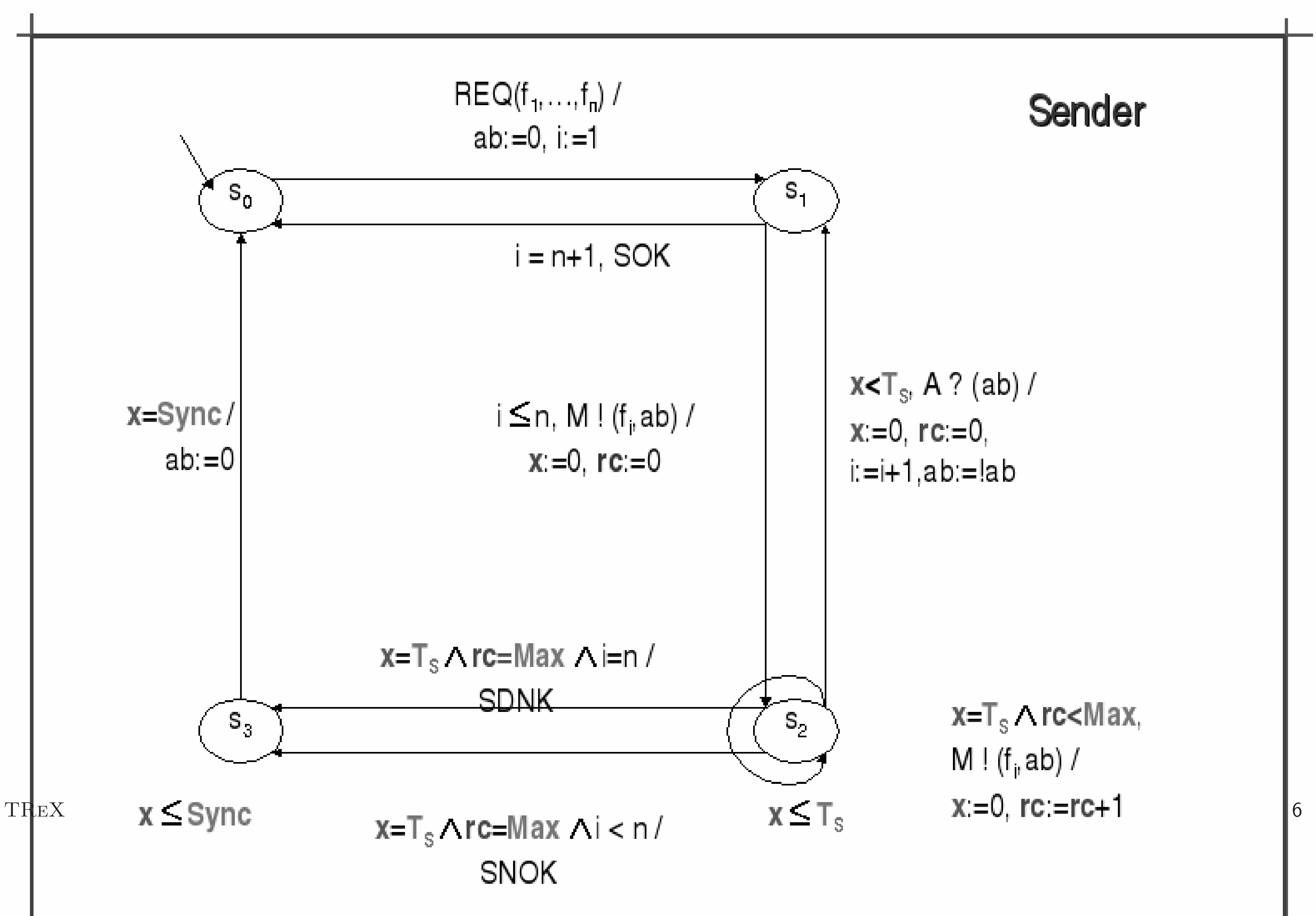
- real-time constraints
- data of larger (infinite) domains, e.g., counters
- channels with unreliable service and larger (infinite) capacity
- dynamic architectures
- ...

... and are (re)used in different environments: parameterized specifications.

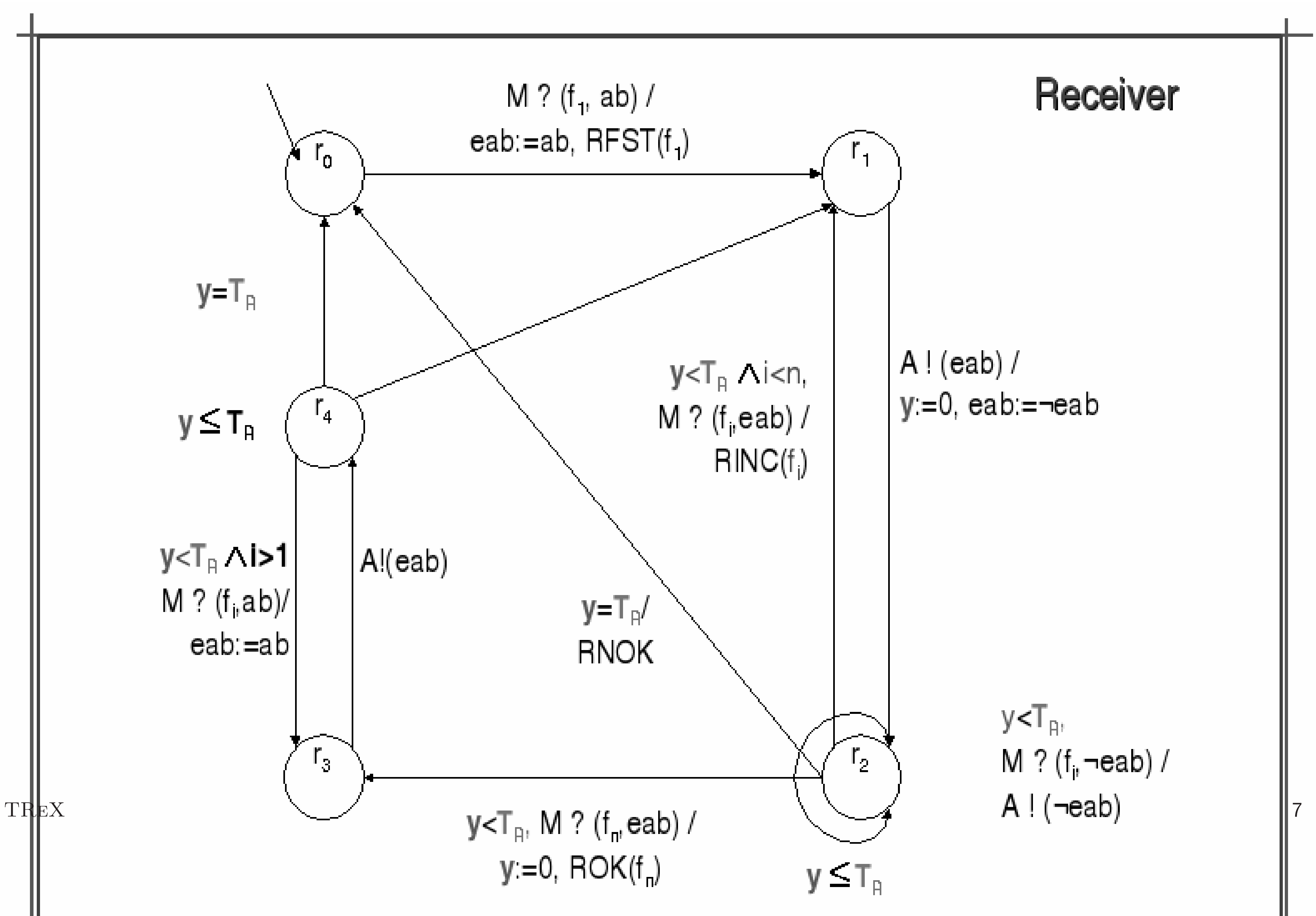
Bounded Retransmission Protocol of Philips




5
4
L
ROK
RNOK
SNOK
SDNK
SDNK
SOK
RNOK
3
RFST
SDNK
RFQ
2
SNOK



Sender
REQ(f1,...,fn) /
ab:=0, i:=1
s0
s1
i = n+1, SOK
x=Sync /
ab:=0
i ≤ n, M ! (fi,ab) /
x:=0, rc:=0
x<TS, A ? (ab) /
x:=0, rc:=0,
i:=i+1,ab:=!ab
x=TS ∧ rc=Max ∧ i=n /
SDNK
s3
s2
x=TS ∧ rc<Max,
M ! (fi,ab) /
x:=0, rc:=rc+1
x ≤ Sync
x=TS ∧ rc=Max ∧ i < n /
SNOK
x ≤ TS


Receiver
r0
r1
r2
r3
r4
M ? (f1, ab) /
eab:=ab, RFST(f1)
y=TR
y ≤ TR
y<TR ∧i<n,
M ? (fi,eab) /
RINC(fi)
A ! (eab) /
y:=0, eab:=¬eab
y<TR ∧i>1
M ? (fi,ab)/
eab:=ab
A!(eab)
y=TR/
RNOK
y<TR,
M ? (fi,¬eab) /
A ! (¬eab)
y<TR, M ? (fn,eab) /
y:=0, ROK(fn)
y ≤ TR

TReX's Aims

Verify complex systems which can be modelized by
automata extended
with variables of heterogenous, infinite domains
and parameters.

Examples BRP, PGM, IEEE 1394,... $=$
extended automata with counters, clocks, parameters, lossy FIFO channels, ...

TReX's Methodology

Input: (network of communicating) extended automata.

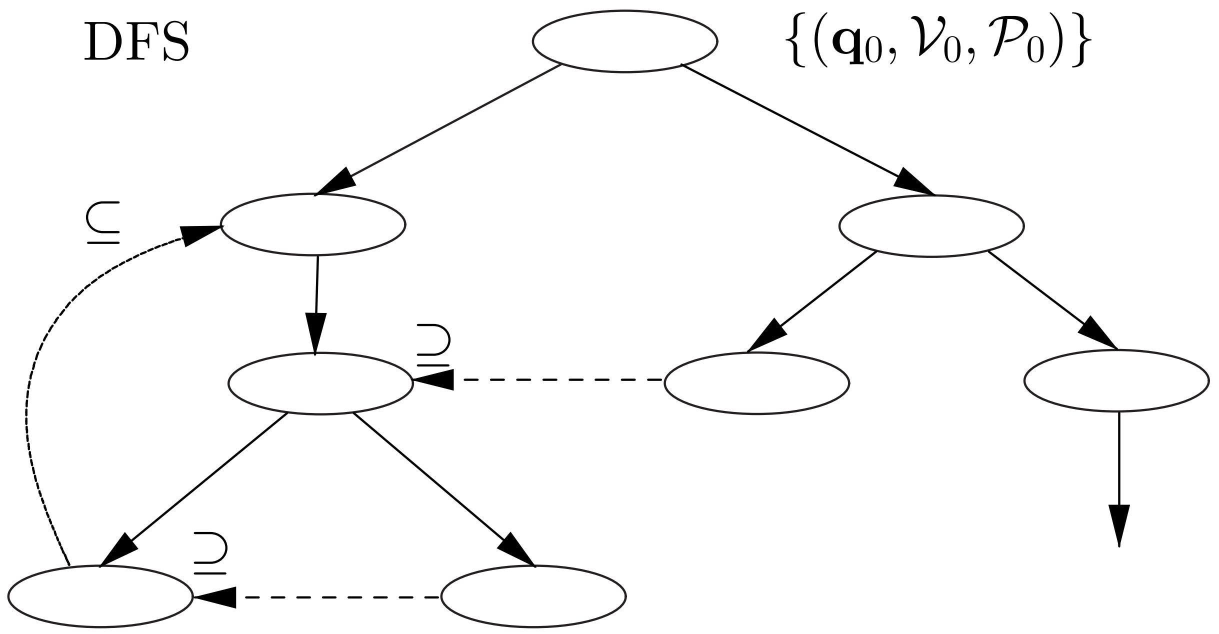
Analysis: by (forward, backward) reachability using:

- symbolic representation of (sets of) configurations,
- extrapolation strategies to help termination.

Output: (abstract) symbolic graph of reachable configurations used to:

- finite model-check,
- synthesize constraints on parameters.

TReX core techniques: Symbolic Reachability Analysis



Termination is not guaranteed!

TReX core techniques: Extrapolation of control loops

Principle:

- work on configuration sets obtained by reachability analysis
- refine the principle of widening [Cousot-Halbwachs-79] for generalisation of reachable sets, e.g., by searching periodicity

Example:

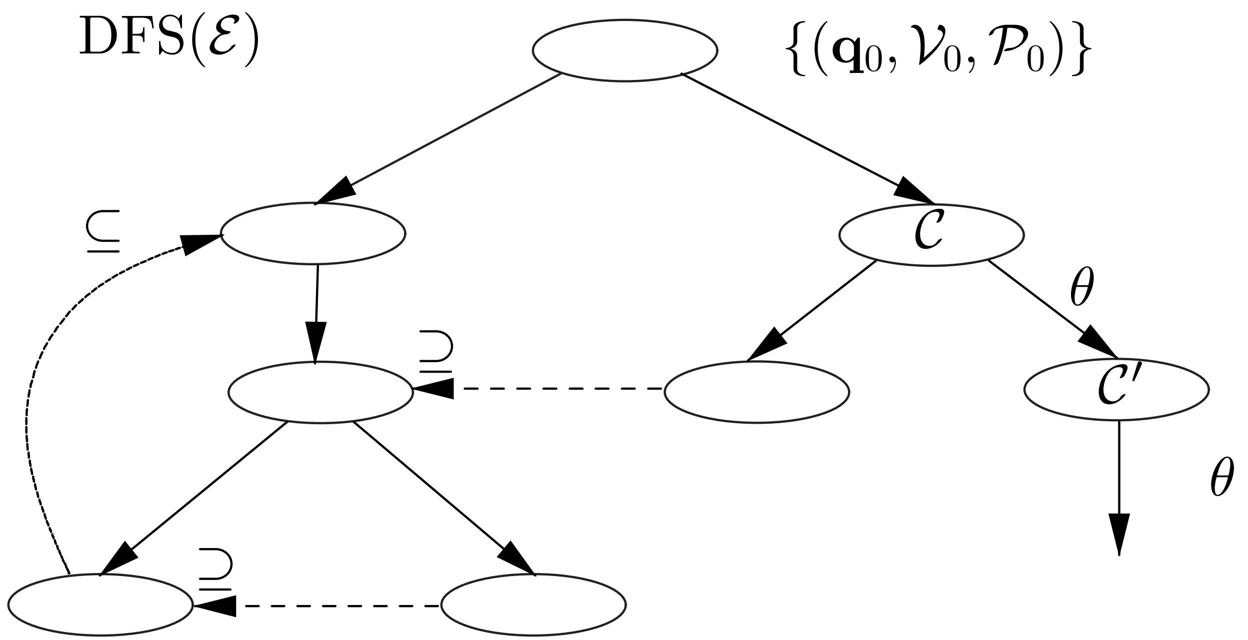
$\mathcal{C} = \{2 \leq x \leq 6, 1 \leq y \leq 4\}$

$post_\theta(\mathcal{C}) = \{2 \leq x \leq 6, 1 \leq y \leq 6\}$ $post^2_\theta(\mathcal{C}) = \{2 \leq x \leq 6, 1 \leq y \leq 8\}$

$\Longrightarrow$

$$post^*_\theta(\mathcal{C}) = \begin{cases} \{2 \leq x \leq 6, 1 \leq y\} & \text{using widening} \\ \{2 \leq x \leq 6, 1 \leq y \leq 4 + 2n\} & \text{using periodicity} \end{cases}$$

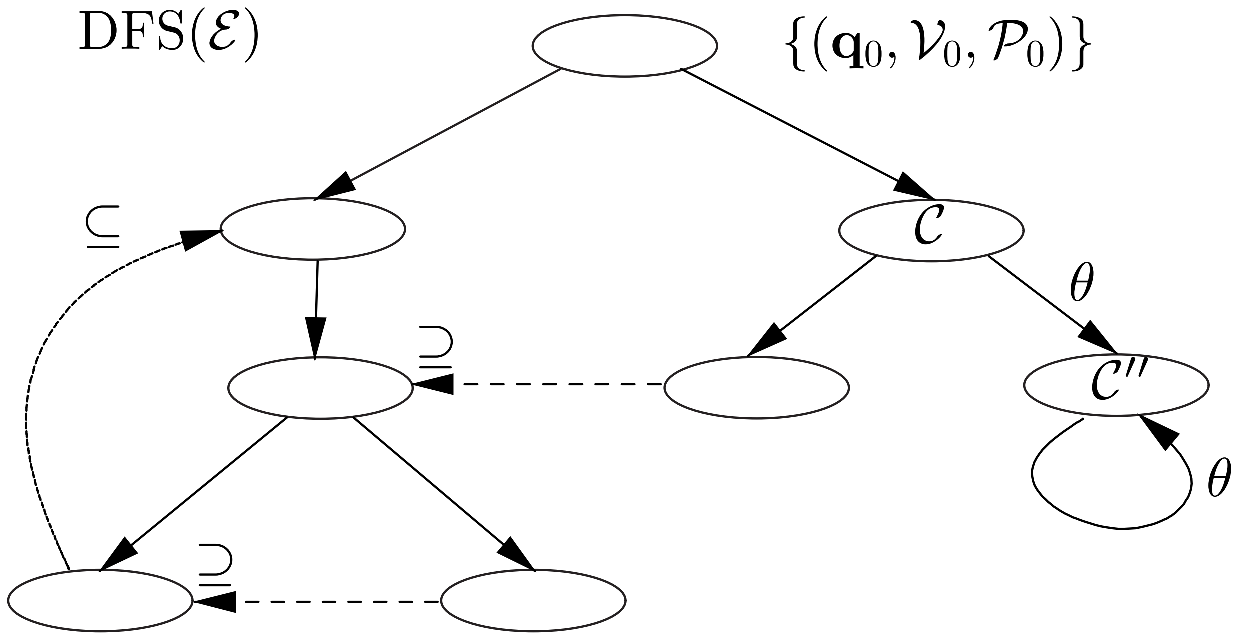
TReX core techniques: Extrapolation of control loops



If $\mathcal{C}, \mathcal{C}', \theta \vdash \mathcal{E}$ then ...

e.g., $\mathbf{q}_{\mathcal{C}} = \mathbf{q}_{\mathcal{C}'}$ and $\mathcal{C}' - \mathcal{C} = \theta(\mathcal{C}') - \mathcal{C}' = \Delta$ and $(|\theta| \leq \mathrm{cycle\_depth}_{\mathcal{E}}$ or $\mathbf{q}_{\mathcal{C}} \in \mathcal{E})$

TReX core techniques: Extrapolation of control loops



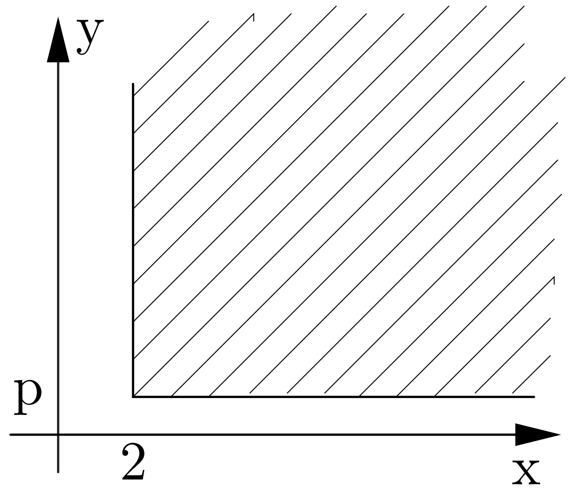
If $\mathcal{C}, \mathcal{C}', \theta \vdash \mathcal{E}$ then $\mathcal{C}'' = post^*_\theta$

e.g., $\mathbf{q}_\mathcal{C} = \mathbf{q}_{\mathcal{C}'}$ and $\mathcal{C}' - \mathcal{C} = \theta(\mathcal{C}') - \mathcal{C}' = \Delta$ and $(|\theta| \leq \mathrm{cycle\_depth}_\mathcal{E}$ or $\mathbf{q}_\mathcal{C} \in \mathcal{E})$

where $\mathcal{C}'' = \theta(\mathcal{C} + \mathbf{n}\Delta) \wedge \mathbf{n} \geq 0$

TReX core techniques: Constrained Parameterized DBM [Asarin-Annichini-Bouajjani-00]

$$\wedge_{i,j}(x_i - x_j \prec_{ij} t_{ij}) \wedge \phi(\mathcal{P})$$



$$(x \geq 2 \wedge y \geq p) \wedge p > 1)$$

$$\left(\begin{bmatrix} (\prec_{00}, t_{00}) & & (\prec_{0n}, t_{0n}) \\ & \dots & \\ (\prec_{n0}, t_{n0}) & & (\prec_{nn}, t_{nn}) \end{bmatrix}, \phi(\mathcal{P}) \right)$$

TReX core techniques: Basic Operations on Constrained PDBM

- intersection with (simple) guard $(x_i - x_j \prec t)$:

$$(M, \phi) \cap (x_i - x_j \prec t) = \begin{cases} \{(M, \phi)\} & \text{if } \phi \supseteq (M_{ij} \prec t) \\ \{(M[ij \leftarrow t], \phi)\} & \text{if } \phi \supseteq \neg(M_{ij} \prec t) \\ \{(M, \phi \wedge M_{ij} \prec t), & \\ \quad (M[ij \leftarrow t], \phi \wedge \neg(M_{ij} \prec t))\} & \text{otherwise} \end{cases}$$

- canonical representation, emptiness test by parameterized Floyd-Warshall

$$\mathrm{cf}(M, \phi) = \{(M^1, \phi^1), ..., (M^n, \phi^n)\}$$

- inclusion test and its safe extension to sets of PDBM

$$(M^1, \phi^1) \subseteq (M^2, \phi^2) \ \text{ iff } \ \forall P \ . \ \forall i, j \ . \ \phi^1 \rightarrow \phi^2 \wedge M^1_{ij} \leq M^2_{ij}$$

TReX core techniques: Evolved Operations on Constrained PDBM

- extrapolation of loops

  If $post_\theta(M) - M = post^2_\theta(M) - post_\theta(M) = \Delta$

  Then $post^n_\theta(M) = post_\theta(M + n\Delta)$

- assignment of variables:
  - exact computation iff $x_i = x_j + t$
  - approximate iff $\vec{x} = M\vec{x} + \vec{b}$

Case studies

About ten in the distribution: ABP, Fischer, Lift Ctrl, Bakery, BRP, IEEE 1394, etc.

New case studies:

- Parameterized version of bridge scheduling problem (Uppaal)
- Pragmatic Multicast Protocol
- Nuclear Reactor Controller (Farn Wang)

Why a New Open Architecture?

Limitation of the TReX 1.xx:

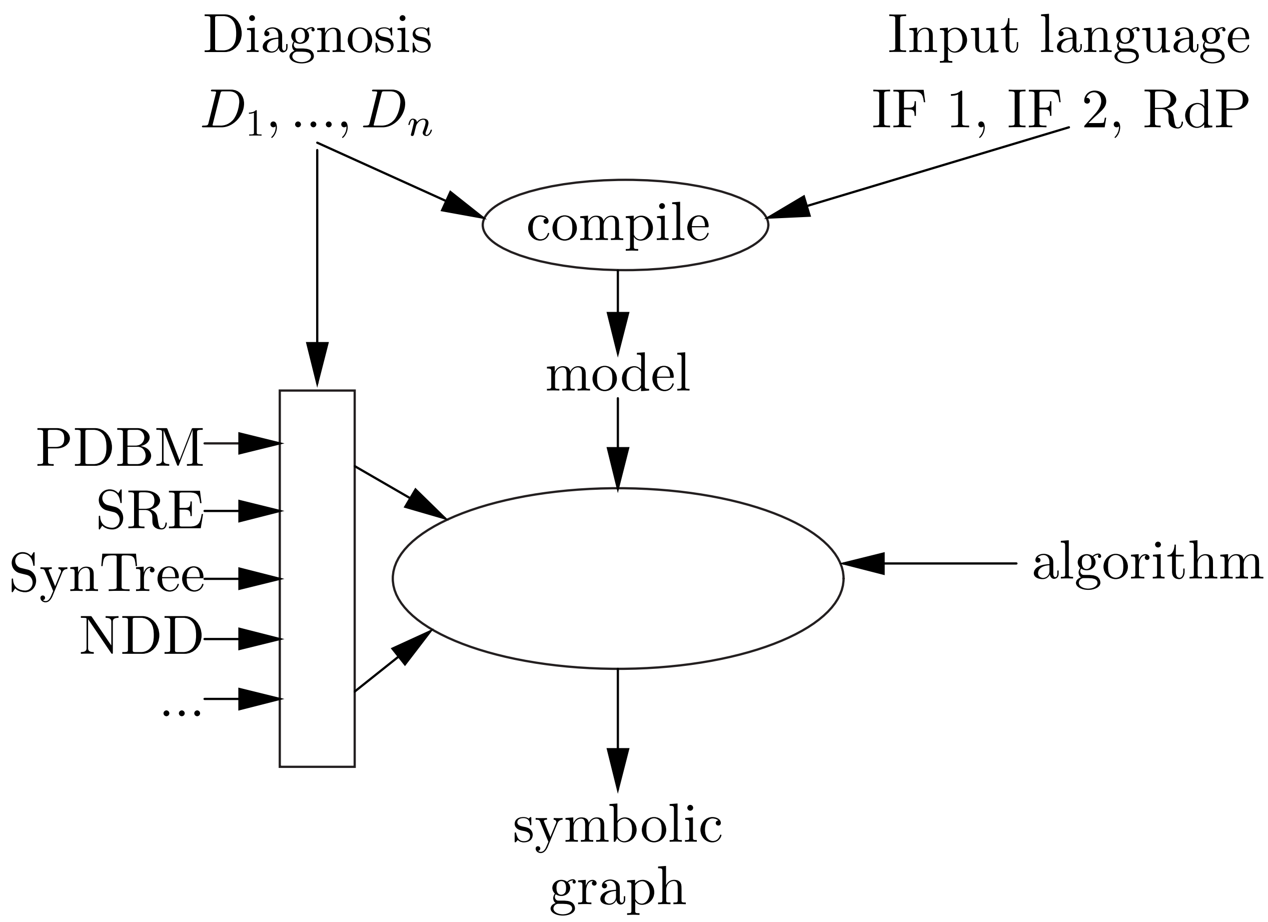
- input language for extended automata: fixed (IF 1.0)
- symbolic representations: fixed (SRE, CPDBM, SynTree)
- strategy for extrapolation: fixed

Our aim: remove fixed above.

New Open Architecture: TReX 2

- allow several input languages compiled to a simple input model
  - used only for code generation
  - may be extended easily
- user choice (guided or free+checked) of symbolic representations
  - SRE, CPDBM, SynTree
  - octagons, itervals
  - NDD, RVA
  - polyhedra, ...
- choice of extrapolation strategy
  - depending on symbolic representation

New Open Architecture: TReX 2



Future Work

- export/import available symbolic representations and their algorithms

- develop new symbolic representations

- extend the input model in order to deal with quantitative properties