Towards Real-time modelchecking using SPIN

SPIN workshop 1997

Bart Knaack,TUE/KUB

Project:AVOCS/VIRES

bknaack@win.tue.nl

Goals of these projects

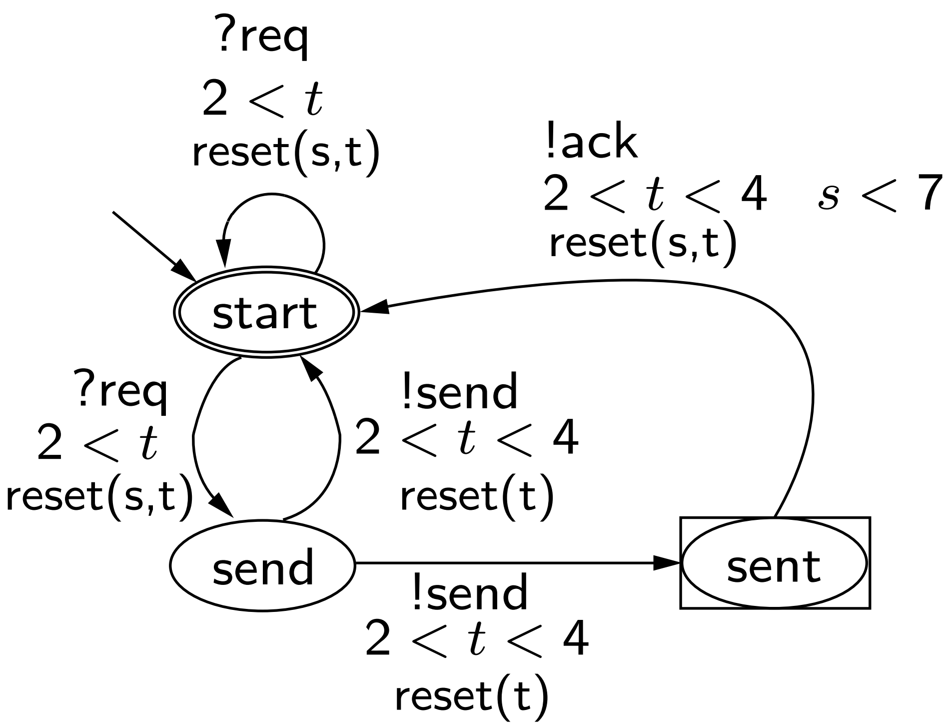
- Real time extension of SPIN
  - Partial order methods
  - bitstate hashing
  - collapsing
- Useable r.t.-input language
- Never Claims
- Acceptance and progress conditions

Outline/Research steps

- Underlying formalism
- Execution Model of the formalism
- Discretisation
- Representation
- Reduction
- Language

Formalism

(based on Timed Graphs)



Lossy Channel

Model

- Based on Timed Graphs [Alur]
- Valid endstates (start)
- Communication Function (?req !send)
- Progress and acceptance labels (sent)
- Urgency

Discretisation Methods

- Region Graphs [Alur,Dill]

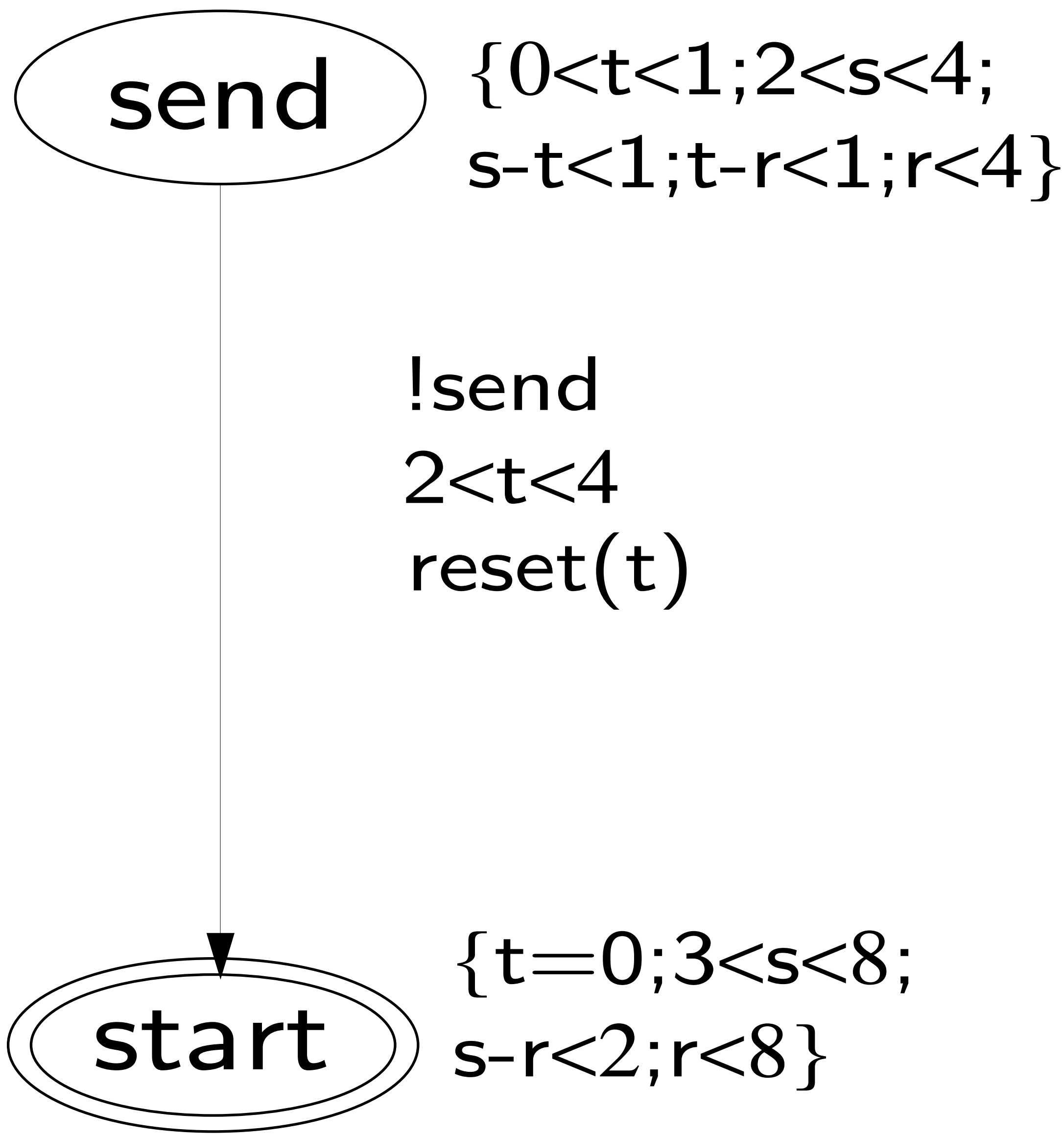
  - Fine-grained equivalence classes

- Sets of Inequalities

  - Usage of model-specific information

$$\begin{array}{cc} x - y > 3 & q - y < 3 \\ z - q < 3 & p - z < 4 \\ 2 < z < 4 & q - y > 2 \\ p - q < 2 & z - x < 6 \end{array}$$

Example: transforming a SOI



Representation

- Important operations
  - inclusion
  - equality
  - emptiness
- Canonical

Candidates:

- Difference bounded Matrices [Dill]
- **Minimal sets**

Minimal sets vs. DBM's

DBM:

$$\begin{array}{c|cccccc} & x & y & z & p & q & \overline{0} \\ \hline x & 0 & \boxed{\mathbf{3}} & 4 & 8 & 6 & 0 \\ y & \infty & 0 & 4 & 5 & 3 & 0 \\ z & \infty & \infty & 0 & 4 & \infty & -2 \\ p & \infty & \infty & 4 & 0 & \infty & 0 \\ q & \infty & -2 & 2 & 2 & 0 & -2 \\ \overline{0} & \infty & \infty & 4 & 8 & \infty & 0 \end{array}$$

$$y - x < 3$$

Minimal Set:

$$x - y > 3 \qquad q - y < 3$$

$$p - q < 2 \qquad p - z < 4$$

$$2 < z < 4 \qquad q - y > 2$$

Reduction

Classical:

- State space explosion

Time:

- Number of time equivalence classes exponential
- storage of polytopes

Solutions

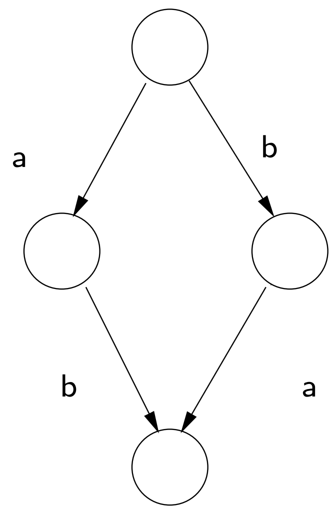
Classical:

- Partial order techniques
  - Dependency relation influenced by clocks

Time:

- Clock minimalisation [Sifakis]

Partial Order techniques

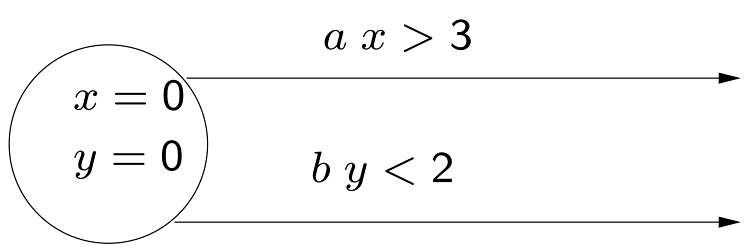


Simple conditions:

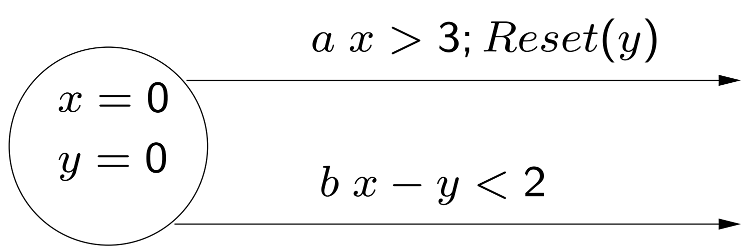
- Untimed SPIN: Global objects
- Timed SPIN: Time as Global object

Dependency

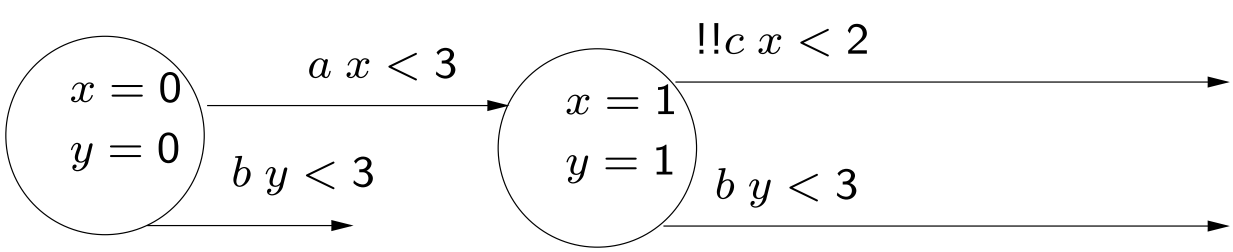
- Time progression



- Resets



- Urgency



Input language

- Intuitive
- Expressive
- Transparent
- Examples:
  - Channel latencies: chan a[n][lb,ub] of int;
  - Delay(8,12)
  - Urgency:
    if
    !! ?req;
    :: delay(12,12)$-$ $>$ break;
    fi

Conclusions

State now:

- Formalism worked out
- Implementation discretisation method
- Study Partial order methods

Extensions:

- Simple clockdrifts
- Dynamic time constraints
- Symbolic time constraints

bknaack@win.tue.nl