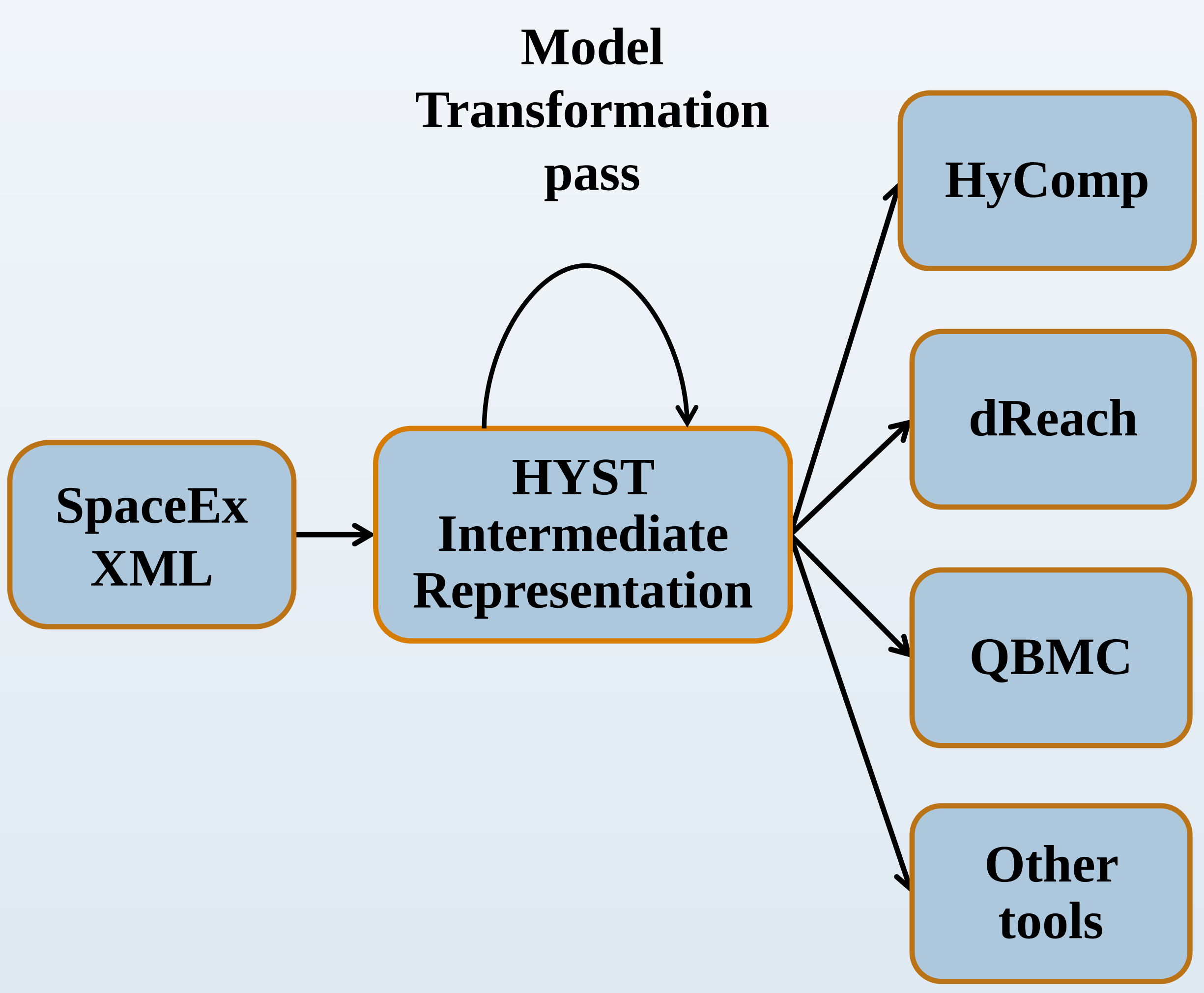
Quantified Bounded Model Checking for Rectangular Hybrid Automata

Luan Nguyen[1], Djordje Maksimovic[2], Taylor T. Johnson[1], Andreas Veneris[2]

[1]University of Texas at Arlington, Arlington, TX USA, [2]University of Toronto, Ontario, Canada

Overview

- **QBMC: a quantified bounded model checking (BMC) for Rectangular Hybrid Automata (RHA)**
  - encodes the BMC problem for RHA in a quantified form
  - performs QBMC by querying the Z3 SMT solver via its Python API and use its quantifier-handling procedures [1]
  - implemented as a module within HyST [2]



Algorithm

- **Quantified free BMC for Hybrid Automata**

$$\Phi(k) \triangleq I(V_0) \wedge \bigwedge_{i=0}^{k-1} T_i(V, V') \wedge (\bigvee_{i=0}^{k} P(V_i))$$

- $I(V_0)$: initial set of states
- $T_i(V, V') \triangleq D_i(V, V') \vee \mathcal{T}_i(V, V')$: transition (discrete or continuous trajectory) between consecutive pairs of sets of states
- $P(V_i)$: a safety specification at iteration i

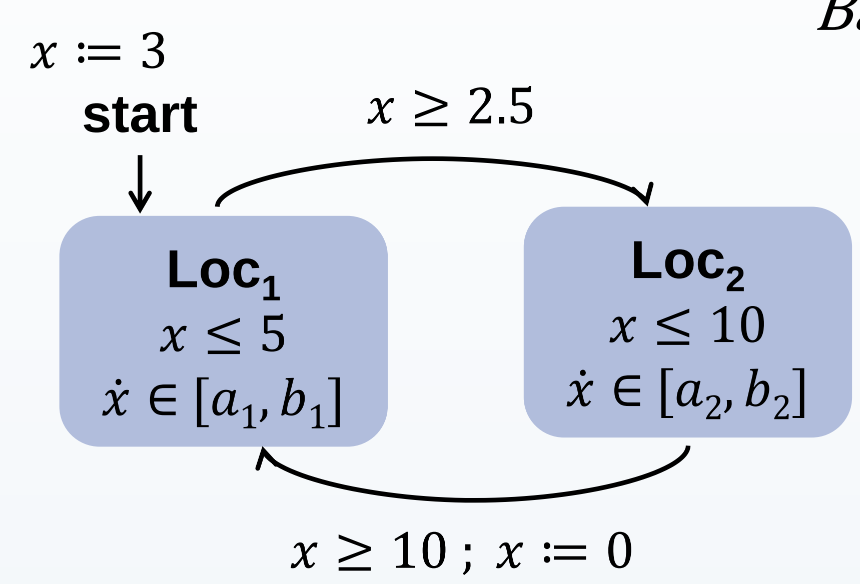
- **QBMC for Hybrid Automata**

$$\Omega(k) \triangleq \exists V_0, V_1, \ldots, V_k, \delta \forall t \exists V, V' \mid I(V_0) \wedge T(V, V') \wedge \bigwedge_{i=0}^{k-1} t_{i+1} \rightarrow [(V = V_i) \wedge (V' = V_{i+1})] \wedge (\bigvee_{i=0}^{k} P(V_i))$$

- δ: the real time elapse in the trajectories
- $t = \langle t_1, t_2, \ldots, t_{\lceil log_2 k \rceil} \rangle$: index each iteration of the BMC of hybrid automata H

Experimental Results

- ***Illustrative Example***



Bad States: $P \triangleq \bigvee_{i=0}^{k} \neg(Loc_i = Loc_2 \rightarrow x \geq 2.5)$

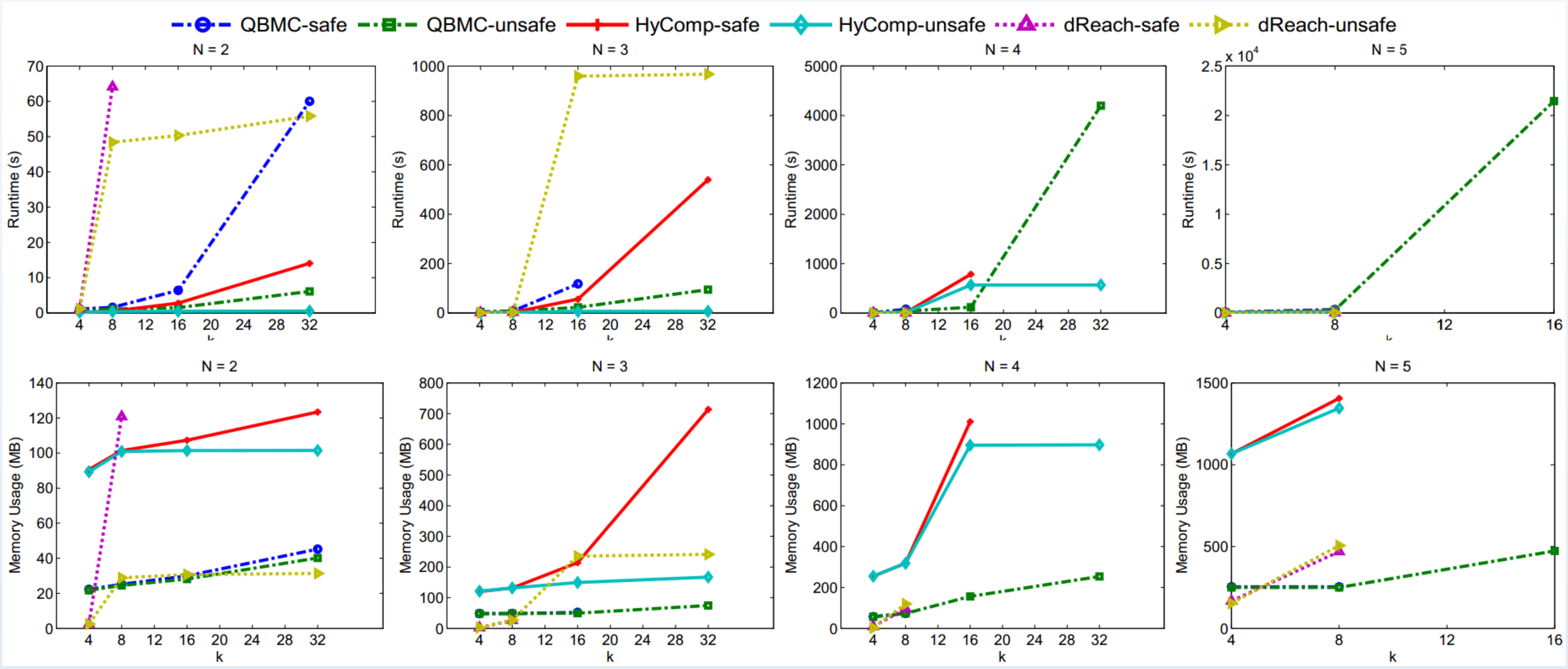
$a_1 = 0, b_1 = 1, a_2 = 0, b_2 = 2$

Tools	L	k ≤ 32		k ≤ 64		k ≤ 128	
		Time (sec)	Mem (MB)	Time (sec)	Mem (MB)	Time (sec)	Mem (MB)
QBMC	2	1.11	27.2	3.68	39.4	19.9	91.2
dReach	2	86.7	102.4	1176.4	284.7	20034	829.2
HyComp	2	0.4	97.3	0.6	101.8	1.44	109.3

- **Fischer mutual exclusion protocol**

Discrete locations: 4^N

Discrete state-spaces: $(N + 1)(4N)^N$



- **Lynch-Shavit mutual exclusion protocol**

Discrete locations: 9^N

Discrete state-spaces: $(N + 1)(9N)^N$

Tools	L	k ≤ 4		k ≤ 8		k ≤ 16	
		Time (sec)	Mem (MB)	Time (sec)	Mem (MB)	Time (sec)	Mem (MB)
QBMC	9^2	3.7	52.2	5.1	52.3	25.9	52.7
	9^3	15.5	65.6	31.3	87.5	1091.5	144.5
	9^4	256.1	702.8	1062.1	708.9	43578	1196.2
HyComp	9^2	0.8	121.9	1.33	132.8	9.5	170.5
	9^3	2.7	307.9	12.81	380.8	192.8	771.4
	9^4	63.9	2655.4	N/A	M/O	N/A	M/O

QBMC & examples are available online at: ***http://www.verivital.com/hyst/cfv2015.zip***

Conclusion

- present a new SMT-based verification technique that encodes the BMC problem for RHA in a quantified form, which also subsumes this encoding for timed automata
- present preliminary experimental results included such as Fischer and Lynch-Shavit mutual exclusion, and compare to dReach and HyComp
- In future, we will investigate more general classes of hybrid automata

References

[1] L. De Moura and N. Bjørner, "Z3: An efficient SMT solver," inProc of 14th International Conference on Tools and Algorithms for the Construction and Analysis of Systems, ser. TACAS '08/ETAPS '08. Springer-Verlag, 2008, pp. 337–340

[2] S. Bak, S. Bogomolov, and T. T. Johnson, "HyST: A source transformation and translation tool for hybrid automaton models," in Proc. of the 18th Intl. Conf. on Hybrid Systems: Computation and Control (HSCC). ACM, 2015.