Shortest Counterexamples for Symbolic Model Checking of LTL with Past

Viktor Schuppan[1], Armin Biere[2]

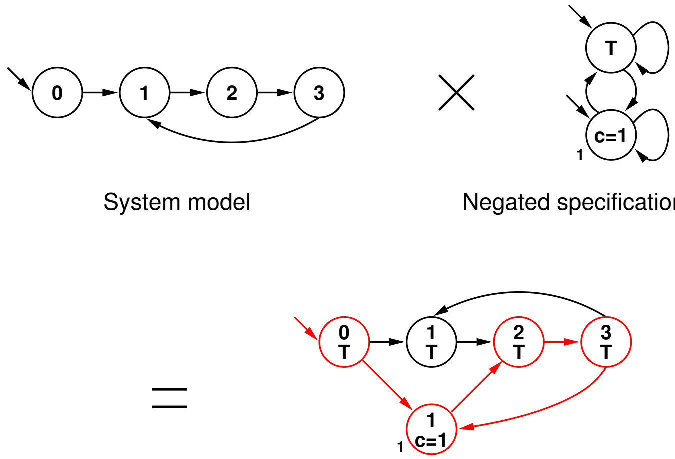
[1]Computer Systems Institute, ETH Zürich

[2]Institute for Formal Models and Verification, JKU Linz

`http://www.inf.ethz.ch/~schuppan/`

TACAS'05, April 4 – 8, 2005, Edinburgh, UK

Shortest Counterexamples for LTL



System model

Negated specification: GF c=1

Find reachable fair lasso–shaped path

To obtain shortest counterexample

1. Find shortest fair lasso-shaped path.

SAT-based BMC	[Biere, Cimatti, Clarke, Zhu (TACAS'99)]
BDD-based symbolic MC	[Schuppan, Biere (STTT'04)]
explicit-state MC	[Gastin, Moro, Zeitoun (SPIN'04)]

2. Have tight automaton/encoding of specification.

SAT-based BMC	[Benedetti, Cimatti (TACAS'03)]
	[Latvala, Biere, Heljanko, Junttila (VMCAI'05)]
BDD-based symbolic MC	this talk
explicit-state MC	(this talk)

Contents

Shortest Infinite Counterexamples

[Clarke, Grumberg, McMillan, Zhao (DAC'95)]

Finite state system with failing LTL property:
$\Rightarrow$ lasso-shaped counterexample $\alpha = \beta\gamma^\omega$

$$\alpha = \underbrace{\underbrace{b_0\, b_1\, b_2 \ldots b_{|\beta|-1}}_{\text{stem } \beta}\ \overbrace{\underbrace{c_0\, c_1\, c_2 \ldots c_{|\gamma|-1}}_{\text{loop } \gamma}\ c_0\, c_1\, c_2 \ldots c_{|\gamma|-1} \quad \ldots}^{\text{loop body } \gamma^\omega}}_{}$$

length of counterexample: |stem β| + |loop γ|

Shortest infinite counterexample $\Rightarrow$ minimal $|\beta| + |\gamma|$.

Tight Büchi Automata — Definition

[Kupferman, Vardi (CAV'99)]:

Automaton on finite words tight

$\Leftrightarrow$

accepts shortest violating prefixes for safety properties.

Extend notion:

Büchi automaton on infinite words tight

$\Leftrightarrow$

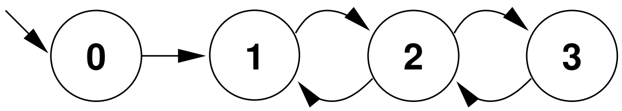
for each lasso-shaped counterexample α there is a fair, lasso-shaped path in the product with α of the same length.

Formally:

$$\forall \alpha \in Lang(B) \,.\, \forall \beta, \gamma \,.\, (\alpha = \beta\gamma^\omega \Rightarrow$$
$$\exists \rho \in Runs(B) \,.\, \exists \lambda, \mu, \nu \,.$$
$$(\rho \models \alpha \;\wedge\; \lambda = \alpha \times \rho = \mu\nu^\omega \;\wedge\; |\mu| + |\nu| = |\beta| + |\gamma|))$$

Tight Büchi Automata — a Criterion

Specification: $\neg(\mathbf{GF}(c = 1) \wedge \mathbf{GF}(c = 3))$

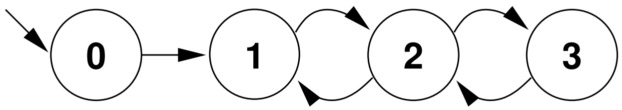
Automaton	Path
	$(0) \quad (1\ 2\ 3\ 2)\ (1\ 2\ 3\ 2)\ (1\ 2\ 3\ 2)\ \ldots$
$\times$	$\times$
?	$(r_0)\ (r_1\ r_2\ r_3\ r_4)\ (r_1\ r_2\ r_3\ r_4)\ (r_1\ r_2\ r_3\ r_4)\ \ldots$
$=$	$=$
?	$\begin{pmatrix} 0 \\ r_0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 2 \\ r_1 & r_2 & r_3 & r_4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 2 \\ r_1 & r_2 & r_3 & r_4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 2 \\ r_1 & r_2 & r_3 & r_4 \end{pmatrix} \ldots$

What do system states of the same color have in common?

$\Rightarrow$ They have the same future. (But different past.)

Tight Büchi Automata — a Criterion

Specification: $\neg(\mathbf{GF}(c=1) \wedge \mathbf{GF}(c=3))$

Automaton	Path
	$(0)\ (1\ 2\ 3\ 2)\ (1\ 2\ 3\ 2)\ (1\ 2\ 3\ 2)\ \ldots$
$\times$	$\times$
?	$(r_0)\ (r_1\, r_2\, r_3\, r_4)\ (r_1\, r_2\, r_3\, r_4)\ (r_1\, r_2\, r_3\, r_4)\ \ldots$
$=$	$=$
?	$\begin{pmatrix} 0 \\ r_0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 2 \\ r_1 & r_2 & r_3 & r_4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 2 \\ r_1 & r_2 & r_3 & r_4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 2 \\ r_1 & r_2 & r_3 & r_4 \end{pmatrix} \ldots$

Büchi automaton must have accepting run that pairs system states with same future with same state.

(Non-) Tightness of Tableau

Tableau following [Kesten, Pnueli, Raviv (ICALP'98)]

– State bits represent subformulae of ϕ.

– If ρ is accepting run on α: formulae in $\rho(i)$ hold at $\alpha(i)$.

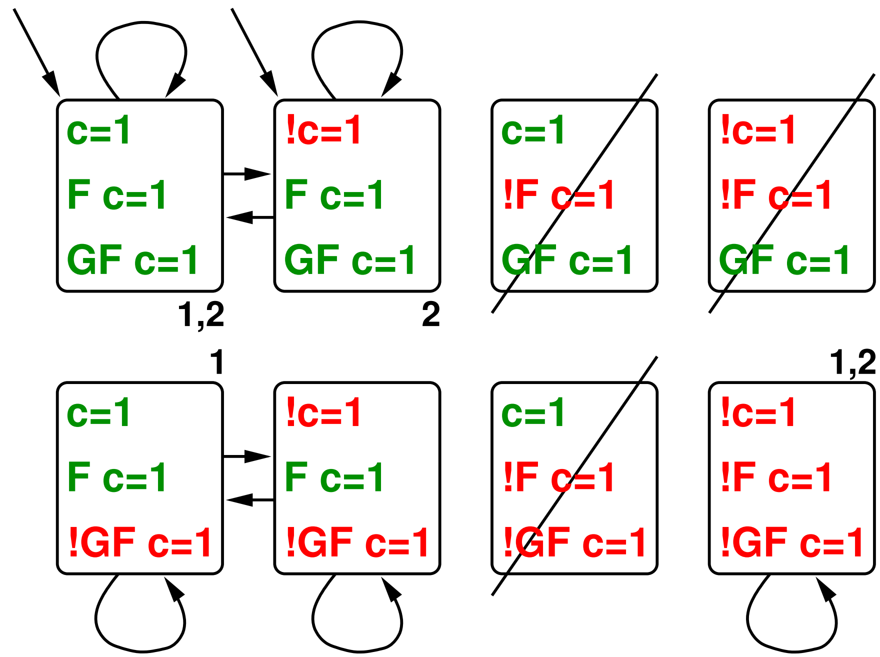
– Each pair of states differs in sign of ≥ 1 formulae:
$\Rightarrow$ different future and/or past.

Tableau is

$\Rightarrow$ tight for future time LTL.

$\Rightarrow$ not tight for LTL with past.

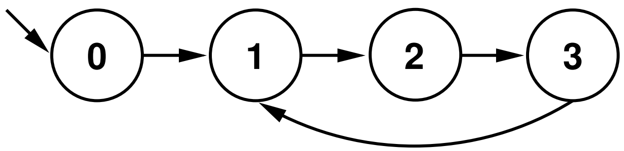
Tableau for $\phi = \mathbf{GF}(c = 1)$



Problem with Past Time Formulae

simplified from [Benedetti, Cimatti ’03]

System model

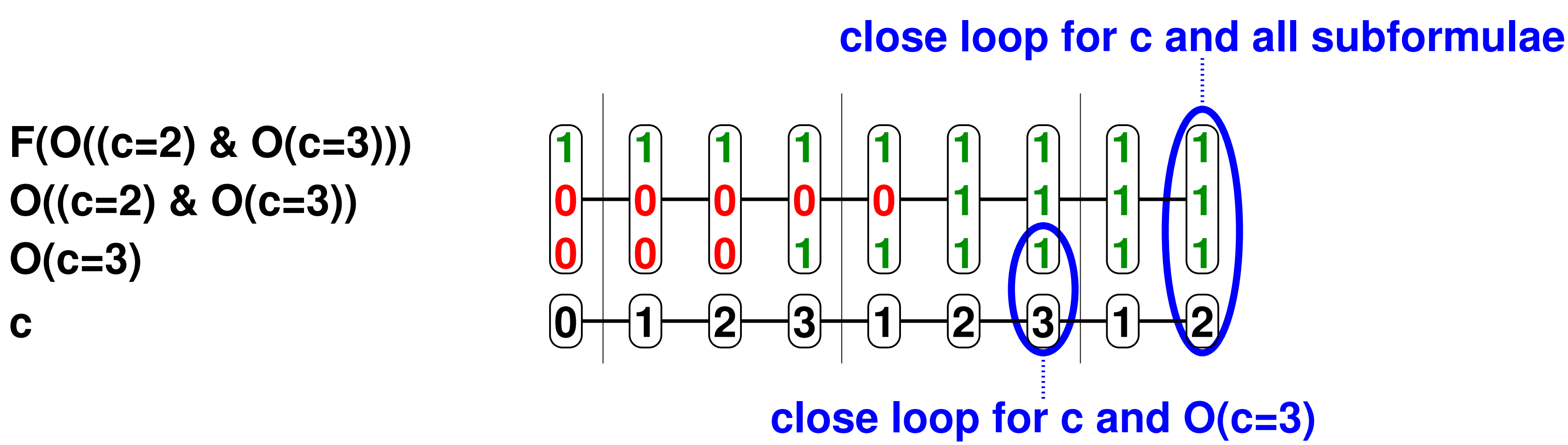


Specification

$$\neg \mathbf{F}(\mathbf{O}((c=2) \wedge \mathbf{O}(c=3)))$$

Shortest counterexample has length 4.

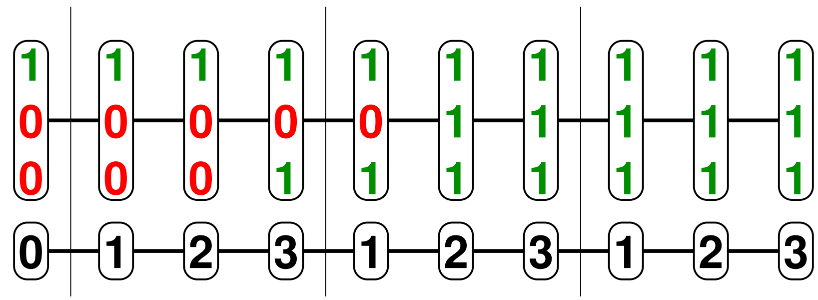
Accepting lasso in tableau



Accepting lasso has length 8.

Excess Length of Tableau Construction

F(O((c=2) & O(c=3)))
O((c=2) & O(c=3))
O(c=3)
c



[Laroussinie, Markey, Schnoebelen (LICS'02)], [Benedetti, Cimatti '03]:

- Let $h(\phi)$ be the maximal number of nested past time operators (past operator depth)
- Truth of past time formula ϕ "stable" after $h(\phi)+1$ loop iterations

Hence:

The length of a shortest counterexample generated by the tableau construction is bounded by $\mathbf{O}(l \cdot h(\phi))$.

(l: length of shortest counterexample)

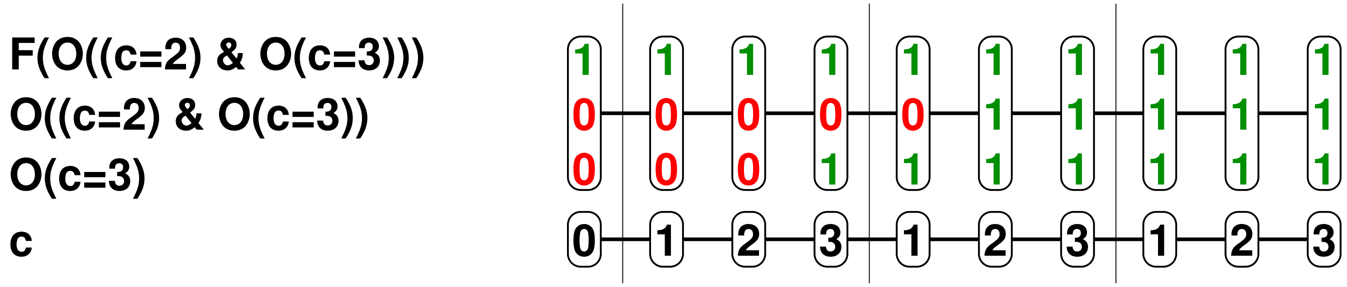
Virtual Unrolling by Example

Same problem faced by bounded model checking of LTL with past

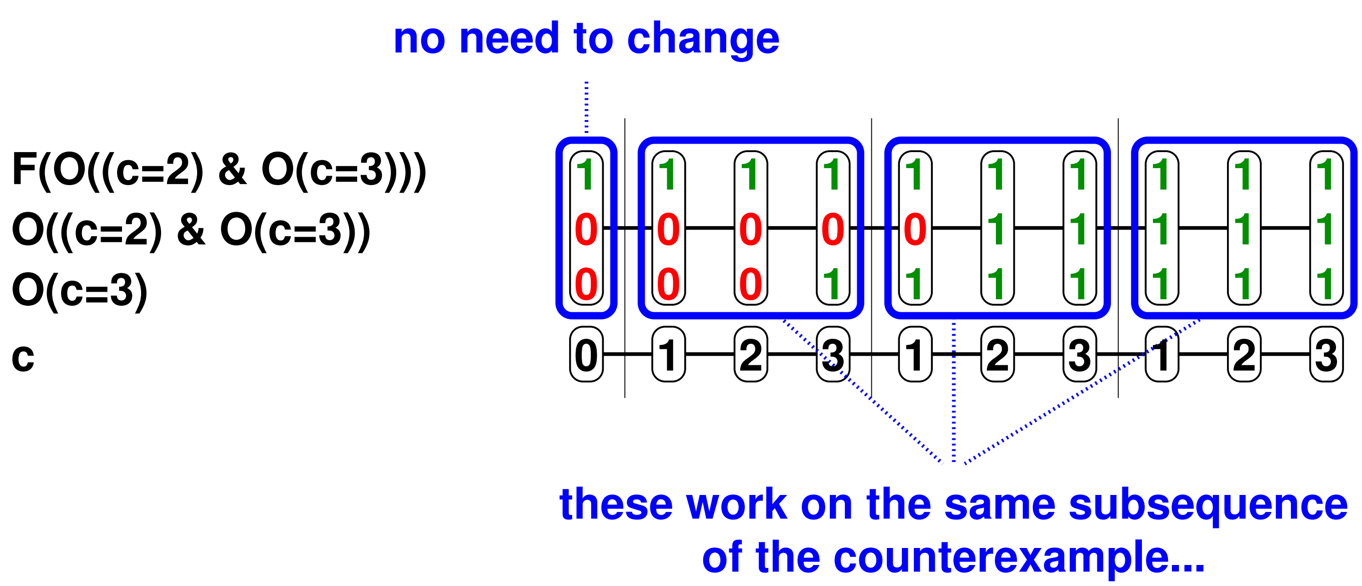
Solution: virtual unrolling of transition relation
[Benedetti, Cimatti ’03], [Latvala et al. ’05]

⇒ Encoding of Latvala et al. can be transformed into Büchi automaton

⇒ Give automata–oriented perspective on virtual unrolling
(some similarity with history transducer
by [Jonsson, Nilsson (TACAS’00)])



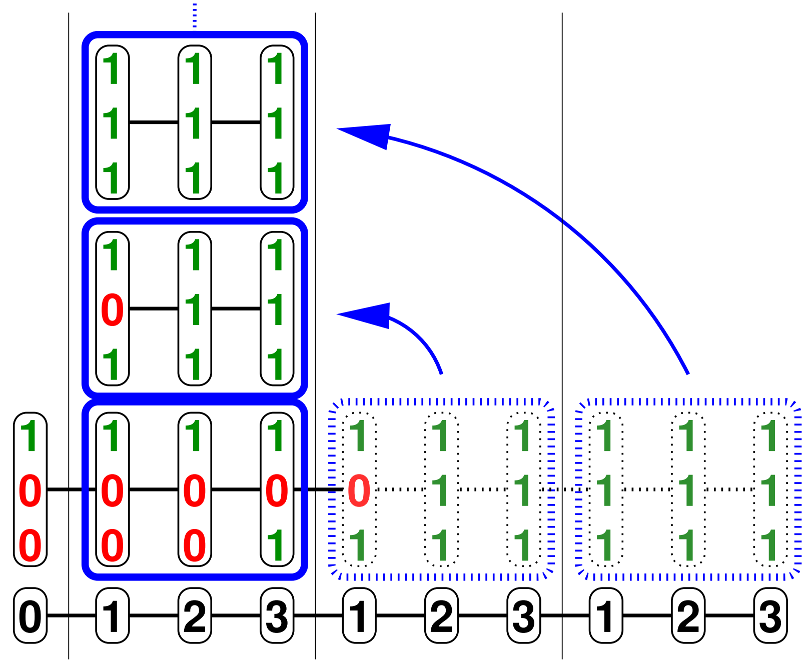
Virtual Unrolling by Example



Virtual Unrolling by Example

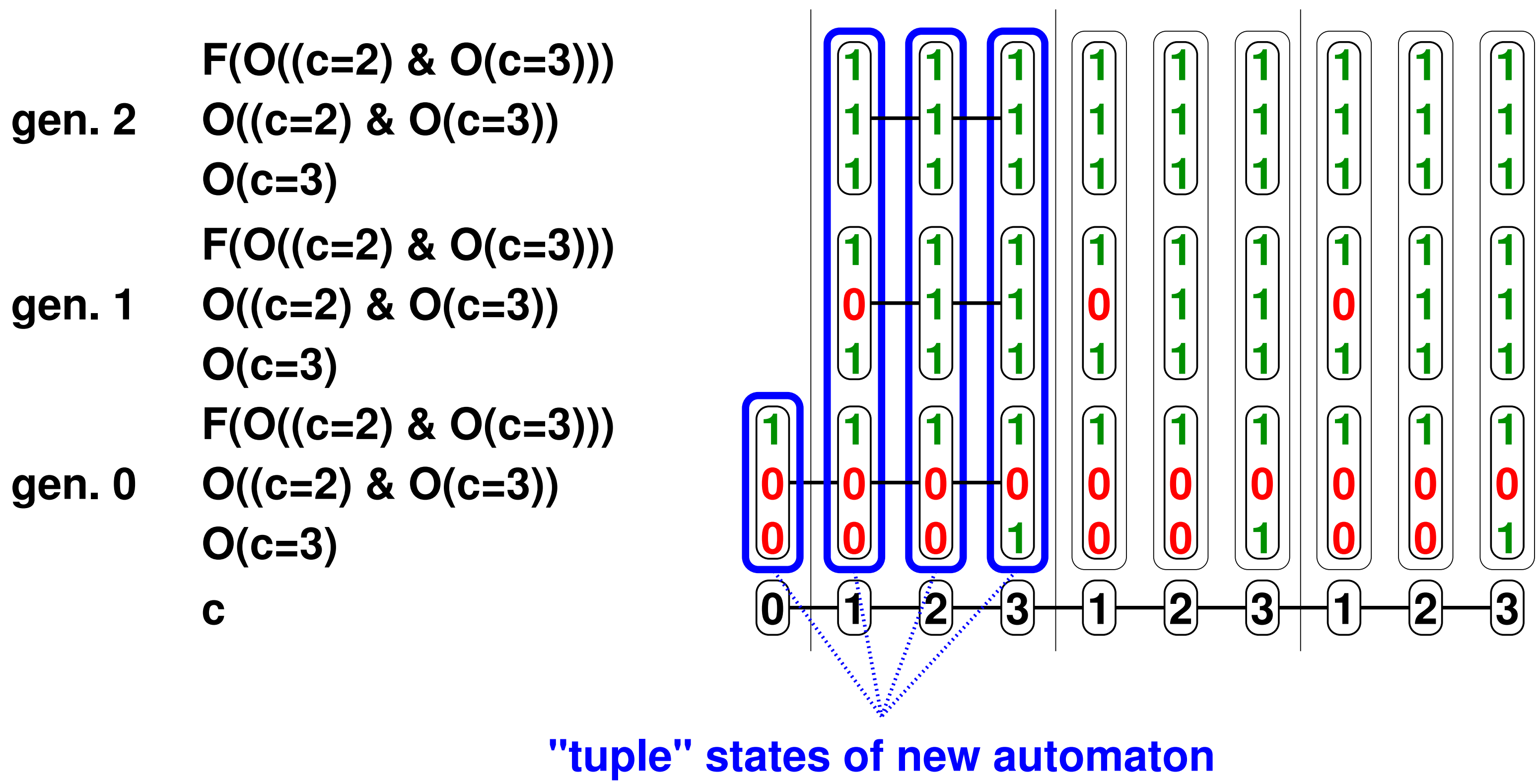
have states of old automaton work in parallel: introduce several generations of variables

F(O((c=2) & O(c=3)))
gen. 2 O((c=2) & O(c=3))
O(c=3)
F(O((c=2) & O(c=3)))
gen. 1 O((c=2) & O(c=3))
O(c=3)
F(O((c=2) & O(c=3)))
gen. 0 O((c=2) & O(c=3))
O(c=3)
c



determined by past operator depth

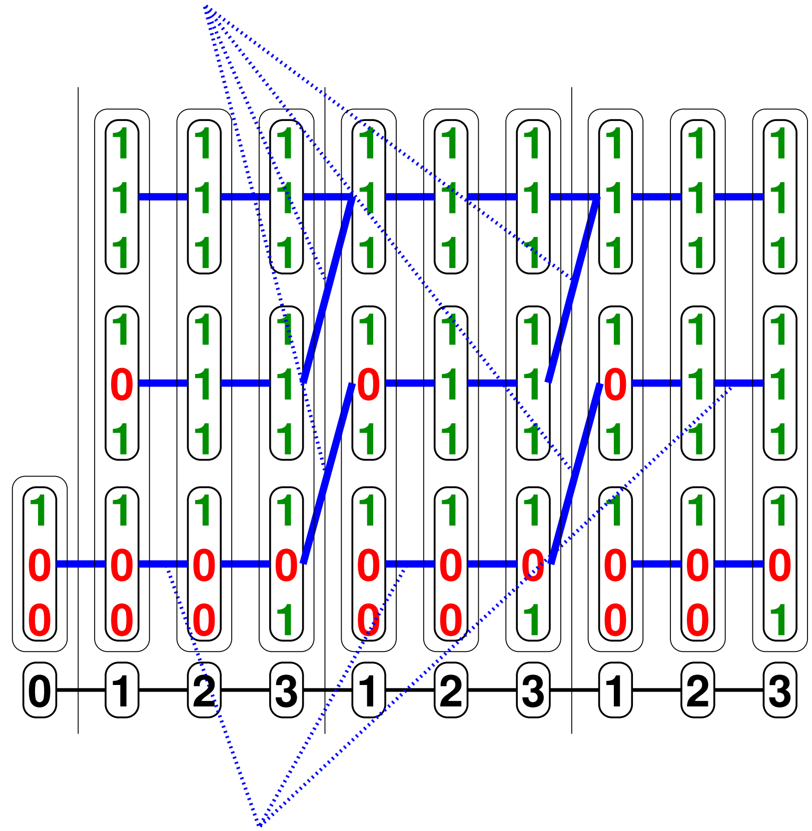
Virtual Unrolling by Example — States



Virtual Unrolling by Example — Transitions

at end of iteration:
constraints between subsequent generations

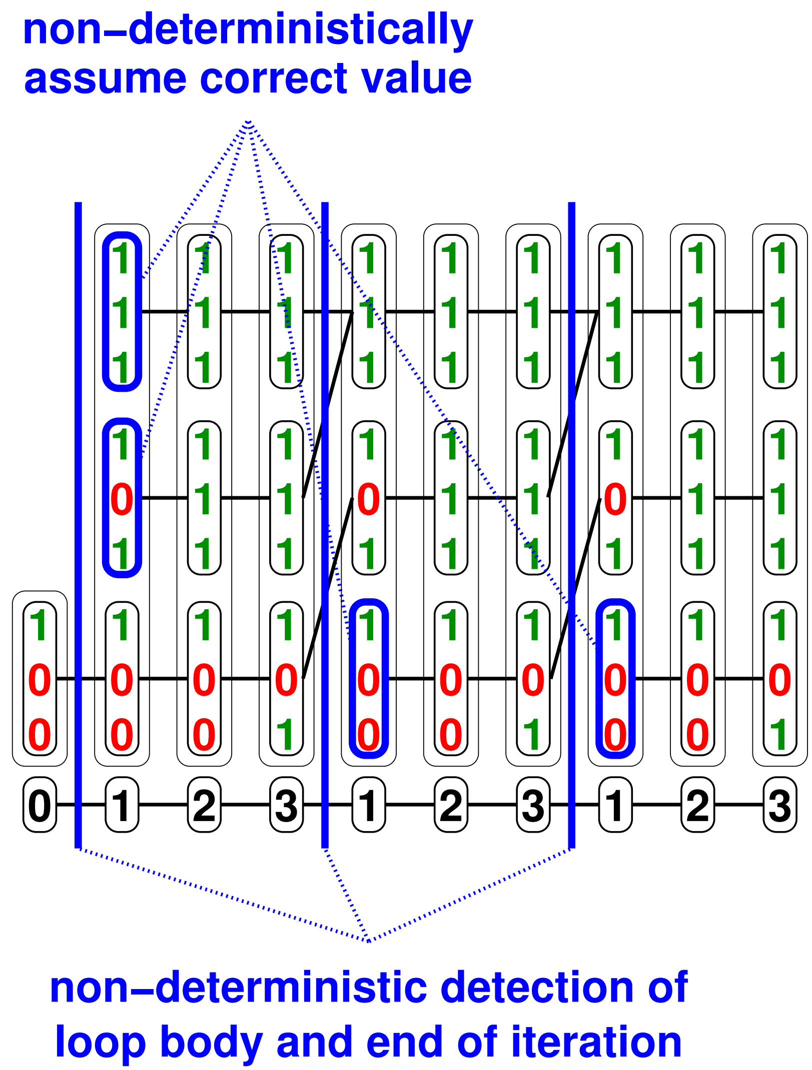
F(O((c=2) & O(c=3)))
gen. 2 O((c=2) & O(c=3))
O(c=3)
F(O((c=2) & O(c=3)))
gen. 1 O((c=2) & O(c=3))
O(c=3)
F(O((c=2) & O(c=3)))
gen. 0 O((c=2) & O(c=3))
O(c=3)
c



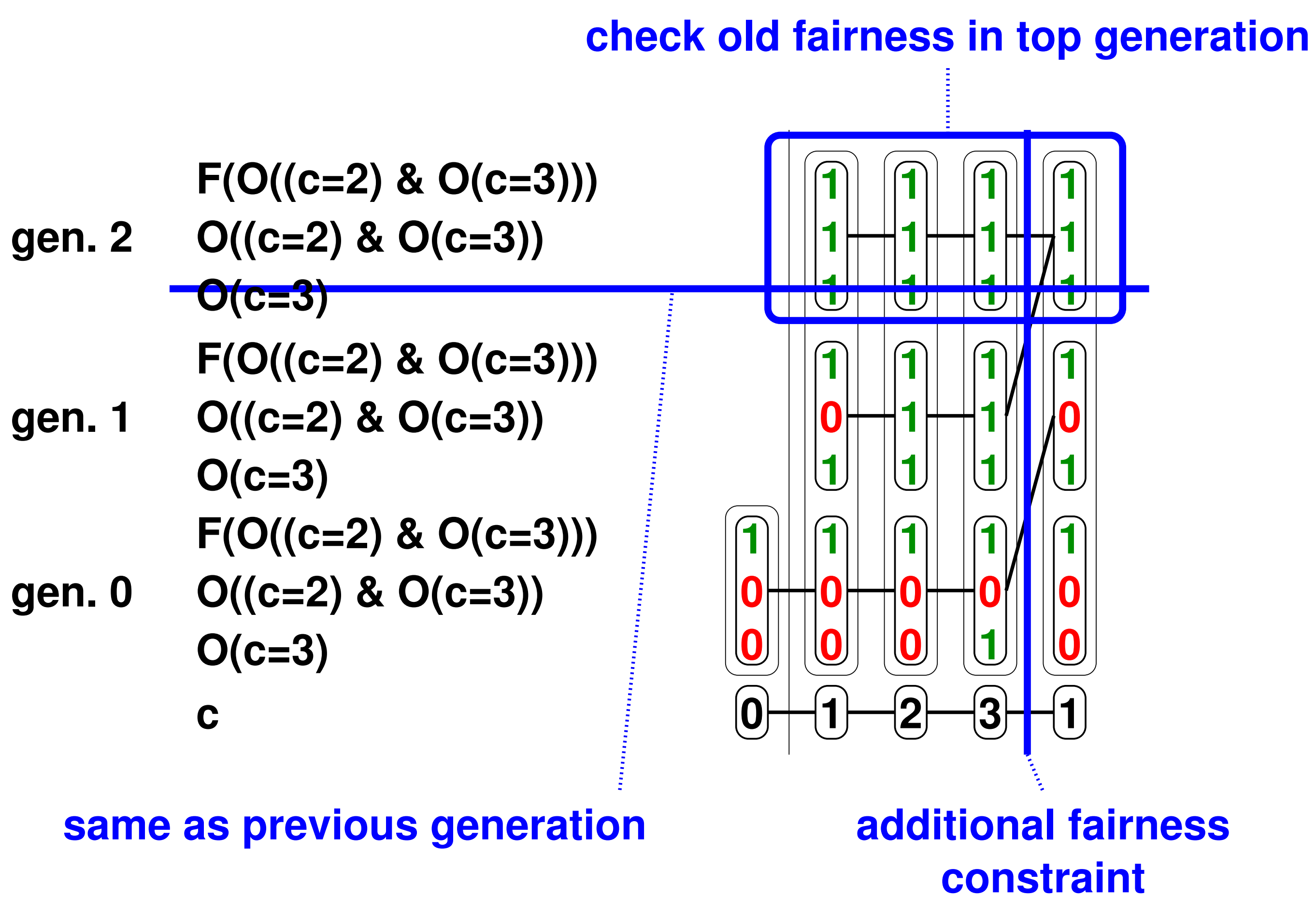
within iteration:
constraints between same generation

Virtual Unrolling by Example — Nondeterminism

	F(O((c=2) & O(c=3)))
gen. 2	O((c=2) & O(c=3))
	O(c=3)
	F(O((c=2) & O(c=3)))
gen. 1	O((c=2) & O(c=3))
	O(c=3)
	F(O((c=2) & O(c=3)))
gen. 0	O((c=2) & O(c=3))
	O(c=3)
	c



Virtual Unrolling by Example — Fine Points



Encoding $\mathbf{O}\psi_1$

	Tableau	Tight Tableau
V^{ψ}	$V^{\psi_1} \cup \{x_\psi\}$	$V^{\psi_1} \cup \bigcup_{i=0}^{h(\psi)} \{x_{\psi,i}\}$
T^{ψ}	T^{ψ_1} $\wedge\ (x'_\psi \leftrightarrow x'_{\psi_1} \vee x_\psi)$	T^{ψ_1} $\wedge\ (\neg lb \longrightarrow (x'_{\psi,\mathbf{0}} \leftrightarrow x'_{\psi_1,\mathbf{0}} \vee x_{\psi,\mathbf{0}}))$ $\wedge\ ((lb \wedge \neg le) \longrightarrow \bigwedge_{i=0}^{h(\psi)-1} (x'_{\psi,\mathbf{i}} \leftrightarrow x'_{\psi_1,\mathbf{i}} \vee x_{\psi,\mathbf{i}}))$ $\wedge\ ((lb \wedge le) \longrightarrow \bigwedge_{i=0}^{h(\psi)-2} (x'_{\psi,\mathbf{i+1}} \leftrightarrow x'_{\psi_1,\mathbf{i+1}} \vee x_{\psi,\mathbf{i}}))$ $\wedge\ (lb \longrightarrow (x'_{\psi,\mathbf{h(\psi)}} \leftrightarrow x'_{\psi_1,\mathbf{h(\psi_1)}} \vee x_{\psi,\mathbf{h(\psi)}}))$
I^{ψ}	$I^{\psi_1} \wedge (x_\psi \leftrightarrow x_{\psi_1})$	$I^{\psi_1} \wedge (x_{\psi,0} \leftrightarrow x_{\psi_1,0})$
F^{ψ}	F^{ψ_1}	F^{ψ_1}

lb is true on the loop body

le is true at the end of a loop iteration

Experiments

Compare finding shortest counterexamples with tight tableau

– SAT-based BMC [Heljanko, Junttila, Latvala, CAV'05]
$\Rightarrow$ preliminary incremental implementation of [Latvala et al. '05] (modified NuSMV 2.2.2, marked incremental BMC)

– BDD-based symbolic loop detection [Schuppan, Biere '04] (on top of NuSMV 2.2.2, marked L2S)

Remarks

– No cone of influence reduction

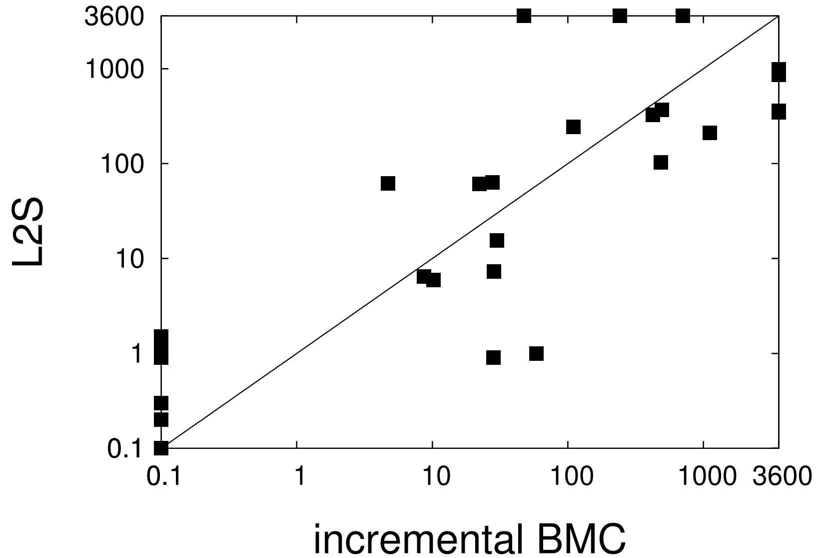
– For BDDs: no dynamic reordering

– For BMC: choice of 2 SAT solvers: zchaff, minisat
$\Rightarrow$ use minimum time/memory

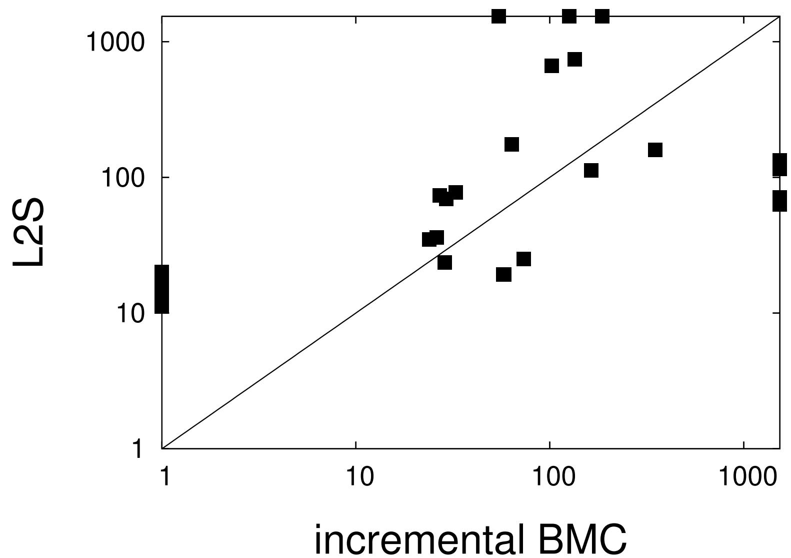
– Examples (all false, resulting in counterexample):
  – [Latvala et al. '05] (some slightly changed)
  – [Schuppan, Biere '04] (some additional properties)

Preliminary Results

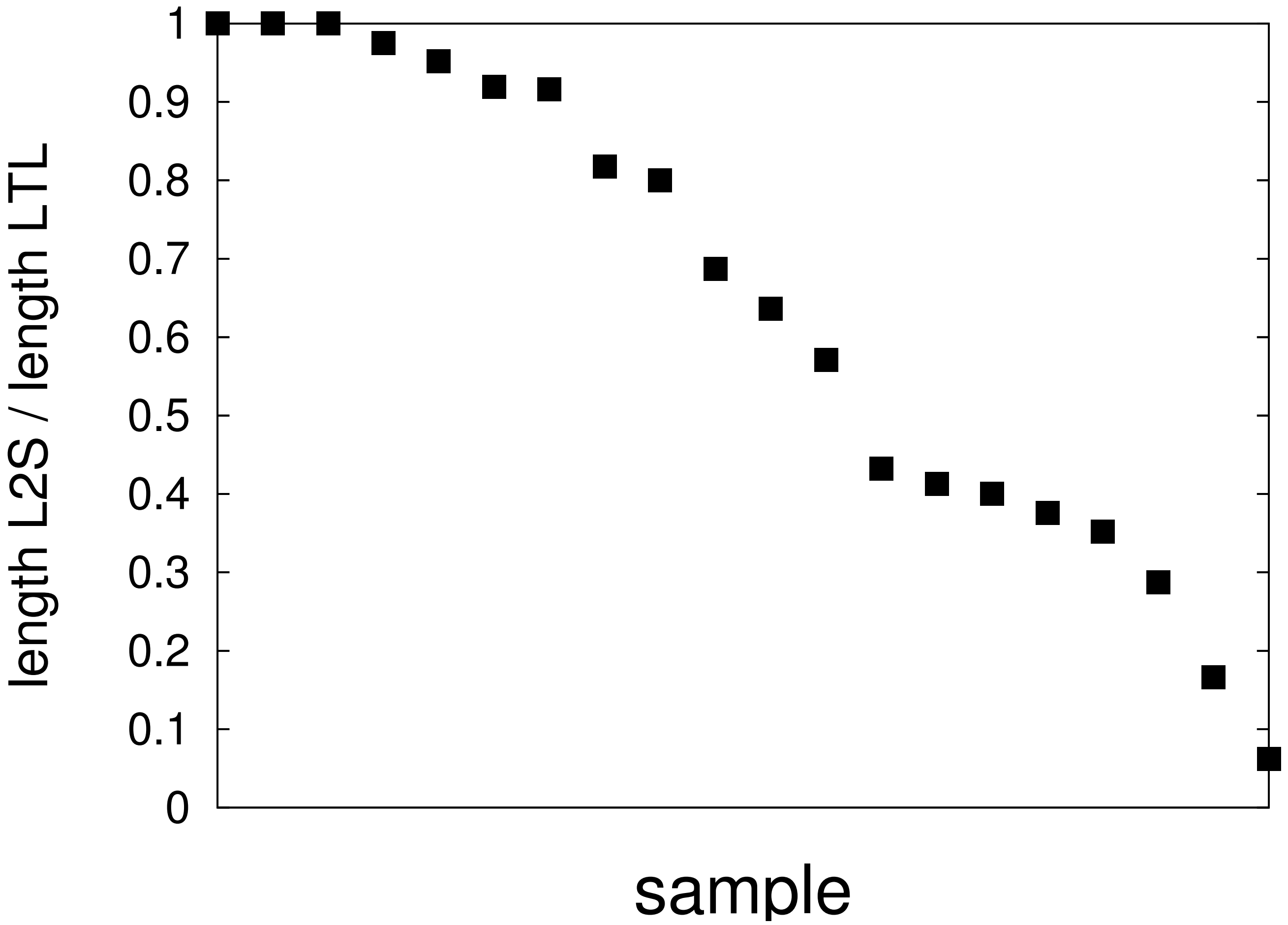
L2S vs incremental BMC
– CPU time [sec]



L2S vs incremental BMC
– Memory [MB]



L2S versus LTL – length counterexample



The End

Summary

– Criteria for Büchi automata to accept shortest counterexamples

– Prove tableau [Kesten et al. '98] tight for future time LTL, not tight for LTL with past

– Practical method to find shortest counterexamples with BDD-based symbolic model checker
$\Rightarrow$ runtime competitive with bounded model checking

Future work

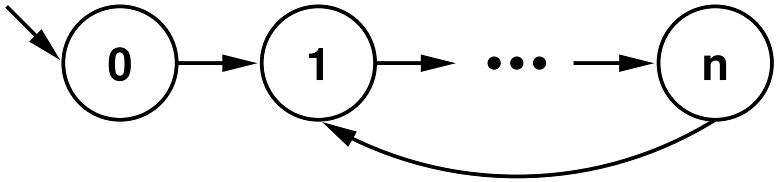
– Explicit-state model checking (size, on-the-fly)

– Lower bounds

Keep out!

Backup slides

Tight Büchi Automata — Where Are We?



$$
\begin{array}{llr}
\neg \mathbf{G}((c \neq n) & \mathbf{U}((c = n) & \wedge \\
\quad ((c \neq n-1) & \mathbf{U}((c = n-1) & \wedge \\
\quad \ldots & & \\
\quad ((c \neq 1) & \mathbf{U}(c = 1)) & \\
\quad \ldots & & \\
\quad)))) & &
\end{array}
$$

automaton of [Gerth, Peled, Vardi, Wolper (PSTV'95)]: counterexample of length $\mathbf{O}(n^2)$.

$$
\begin{array}{l}
\neg(\mathbf{F}(\mathbf{G}(\mathbf{O}((c = 1) \wedge \\
\quad \mathbf{O}((c = 2) \wedge \\
\quad \ldots \\
\quad \mathbf{O}(c = n) \\
\quad \ldots \\
\quad)))))
\end{array}
$$

automaton of [Kesten, Pnueli, Raviv (ICALP'98)]: counterexample of length $\mathbf{O}(n^2)$.

Shortest counterexample has length $n+1$.

Tight Büchi Automata — Equivalent Criteria

The following are equivalent:

1. $\forall\alpha \in \mathit{Lang}(B) \,.\, \forall\beta,\gamma \,.\, (\alpha = \beta\gamma^\omega \Rightarrow$
   $\exists\rho \in \mathit{Runs}(B) \,.\, \exists\lambda,\mu,\nu \,.\, (\rho \models \alpha \;\wedge\; \lambda = \alpha \times \rho = \mu\nu^\omega \;\wedge\; |\mu| + |\nu| = |\beta| + |\gamma|))$

2. $\forall\alpha \in \mathit{Lang}(B) \,.\, \forall\beta,\gamma \,.\, ((\alpha = \beta\gamma^\omega \wedge |\beta| + |\gamma|$ minimal for $\alpha) \Rightarrow$
   $\exists\rho \in \mathit{Runs}(B) \,.\, \exists\lambda,\mu,\nu \,.\, (\rho \models \alpha \;\wedge\; \lambda = \alpha \times \rho = \mu\nu^\omega \;\wedge\; |\mu| + |\nu| = |\beta| + |\gamma|))$

3. $\forall\alpha \in \mathit{Lang}(B) \,.\, ((\exists\beta,\gamma \,.\, \alpha = \beta\gamma^\omega) \Rightarrow$
   $(\exists\rho \in \mathit{Runs}(B) \,.\, (\rho \models \alpha \wedge (\forall i,j \,.\, \alpha[i,\infty] = \alpha[j,\infty] \Rightarrow \rho(i) = \rho(j)))))$

4. $\forall\alpha \in \mathit{Lang}(B) \,.\, \forall\beta,\gamma \,.\, ((\alpha = \beta\gamma^\omega \wedge |\beta| + |\gamma|$ minimal for $\alpha) \Rightarrow$
   $\exists\rho \in \mathit{Runs}(B) \,.\, \exists\sigma,\tau \,.\, (\rho \models \alpha \wedge \rho = \sigma\tau^\omega \wedge |\sigma| = |\beta| \wedge |\tau| = |\gamma|))$

5. $\forall\alpha \in \mathit{Lang}(B) \,.\, \forall\beta,\gamma \,.\, (\alpha = \beta\gamma^\omega \Rightarrow$
   $\exists\rho \in \mathit{Runs}(B) \,.\, \exists\sigma,\tau \,.\, (\rho \models \alpha \wedge \rho = \sigma\tau^\omega \wedge |\sigma| = |\beta| \wedge |\tau| = |\gamma|))$

Encoding: General Part

	Tableau	Tight Tableau
V_{BA}^{ϕ}	V^{ϕ}	$V^{\phi} \cup \{lb, le\}$
T_{BA}^{ϕ}	T^{ϕ}	$T^{\phi} \wedge lb \rightarrow lb'$
I_{BA}^{ϕ}	$I^{\phi} \wedge x_{\phi}$	$I^{\phi} \wedge x_{\phi,0}$
F_{BA}^{ϕ}	F^{ϕ}	$F^{\phi} \cup \{\{lb \wedge le\}\}$

V^{ϕ}, T^{ϕ}, I^{ϕ}, F^{ϕ} are defined recursively on the following slides.

Encoding $\mathbf{X}\psi_1$

	Tableau	Tight Tableau
V^{ψ}	$V^{\psi_1} \cup \{x_{\psi}\}$	$V^{\psi_1} \cup \bigcup_{i=0}^{h(\psi)} \{x_{\psi,i}\}$
T^{ψ}	$T^{\psi_1} \wedge (x_{\psi} \leftrightarrow x'_{\psi_1})$	T^{ψ_1} $\wedge \quad (\neg lb \quad \longrightarrow \quad (x_{\psi,0} \leftrightarrow x'_{\psi_1,0}))$ $\wedge \quad ((lb \wedge \neg le) \quad \longrightarrow \quad \bigwedge_{i=0}^{h(\psi)-1}(x_{\psi,i} \leftrightarrow x'_{\psi_1,i}))$ $\wedge \quad ((lb \wedge le) \quad \longrightarrow \quad \bigwedge_{i=0}^{h(\psi)-1}(x_{\psi,i} \leftrightarrow x'_{\psi_1,i+1}))$ $\wedge \quad (lb \quad \longrightarrow \quad (x_{\psi,h(\psi)} \leftrightarrow x'_{\psi_1,h(\psi_1)}))$
I^{ψ}	I^{ψ_1}	I^{ψ_1}
F^{ψ}	F^{ψ_1}	F^{ψ_1}

Encoding ψ_1 U ψ_2

	Tableau	Tight Tableau
V^{ψ}	$V^{\psi_1} \cup V^{\psi_2} \cup \{x_\psi\}$	$V^{\psi_1} \cup V^{\psi_2} \cup \bigcup_{i=0}^{h(\psi)} \{x_{\psi,i}\}$
T^{ψ}	$T^{\psi_1} \wedge T^{\psi_2}$ $\wedge (x_\psi \leftrightarrow x_{\psi_2} \vee x_{\psi_1} \wedge x'_\psi)$	$T^{\psi_1} \wedge T^{\psi_2}$ $\wedge \quad (\neg lb \quad \rightarrow \quad (x_{\psi,0} \leftrightarrow x_{\psi_2,0} \vee (x_{\psi_1,0} \wedge x'_{\psi,0})))$ $\wedge \quad ((lb \wedge \neg le) \quad \rightarrow \quad \bigwedge_{i=0}^{h(\psi)-1} (x_{\psi,i} \leftrightarrow x_{\psi_2,min(i,h(\psi_2))} \vee (x_{\psi_1,min(i,h(\psi_1))} \wedge x'_{\psi,i})))$ $\wedge \quad ((lb \wedge le) \quad \rightarrow \quad \bigwedge_{i=0}^{h(\psi)-1} (x_{\psi,i} \leftrightarrow x_{\psi_2,min(i,h(\psi_2))} \vee (x_{\psi_1,min(i,h(\psi_1))} \wedge x'_{\psi,i+1})))$ $\wedge \quad (lb \quad \rightarrow \quad (x_{\psi,h(\psi)} \leftrightarrow x_{\psi_2,h(\psi_2)} \vee (x_{\psi_1,h(\psi_1)} \wedge x'_{\psi,h(\psi)})))$
I^{ψ}	$I^{\psi_1} \wedge I^{\psi_2}$	$I^{\psi_1} \wedge I^{\psi_2}$
F^{ψ}	$F^{\psi_1} \cup F^{\psi_2}$ $\cup \{\{\neg x_\psi \vee x_{\psi_2}\}\}$	$F^{\psi_1} \cup F^{\psi_2} \cup \{\{\neg x_{\psi,h(\psi)} \vee x_{\psi_2,h(\psi_2)}\}\}$

Encoding $\mathbf{Y}\psi_1$

	Tableau	Tight Tableau
V^ψ	$V^{\psi_1} \cup \{x_\psi\}$	$V^{\psi_1} \cup \bigcup_{i=0}^{h(\psi)} \{x_{\psi,i}\}$
T^ψ	$T^{\psi_1} \wedge (x'_\psi \leftrightarrow x_{\psi_1})$	T^{ψ_1} $\wedge \quad (\neg lb \quad \rightarrow \quad (x'_{\psi,0} \leftrightarrow x_{\psi_1,0}))$ $\wedge \quad ((lb \wedge \neg le) \quad \rightarrow \quad \bigwedge_{i=0}^{h(\psi)-1}(x'_{\psi,i} \leftrightarrow x_{\psi_1,i}))$ $\wedge \quad ((lb \wedge le) \quad \rightarrow \quad \bigwedge_{i=0}^{h(\psi)-2}(x'_{\psi,i+1} \leftrightarrow x_{\psi_1,i}))$ $\wedge \quad (lb \rightarrow (x'_{\psi,h(\psi)} \leftrightarrow x_{\psi_1,h(\psi_1)}))$
I^ψ	$I^{\psi_1} \wedge (x_\psi \leftrightarrow \bot)$	$I^{\psi_1} \wedge (x_{\psi,0} \leftrightarrow \bot)$
F^ψ	F^{ψ_1}	F^{ψ_1}

Encoding $\psi_1 \, S \, \psi_2$

	Tableau	Tight Tableau
V^{ψ}	$V^{\psi_1} \cup V^{\psi_2} \cup \{x_{\psi}\}$	$V^{\psi_1} \cup V^{\psi_2} \cup \bigcup_{i=0}^{h(\psi)} \{x_{\psi,i}\}$
T^{ψ}	$T^{\psi_1} \wedge T^{\psi_2}$ $\wedge (x'_{\psi} \leftrightarrow x'_{\psi_2} \vee x'_{\psi_1} \wedge x_{\psi})$	$T^{\psi_1} \wedge T^{\psi_2}$ $\wedge \quad (\neg lb \quad \longrightarrow \quad (x'_{\psi,0} \leftrightarrow x'_{\psi_2,0} \vee (x'_{\psi_1,0} \wedge x_{\psi,0})))$ $\wedge \quad ((lb \wedge \neg le) \quad \longrightarrow \quad \bigwedge_{i=0}^{h(\psi)-1} (x'_{\psi,i} \leftrightarrow x'_{\psi_2,min(i,h(\psi_2))} \vee (x'_{\psi_1,min(i,h(\psi_1))} \wedge x_{\psi,i})))$ $\wedge \quad ((lb \wedge le) \quad \longrightarrow \quad \bigwedge_{i=0}^{h(\psi)-1} (x'_{\psi,i+1} \leftrightarrow x'_{\psi_2,min(i+1,h(\psi_2))} \vee (x'_{\psi_1,min(i+1,h(\psi_1))} \wedge x_{\psi,i})))$ $\wedge \quad (lb \quad \longrightarrow \quad (x'_{\psi,h(\psi)} \leftrightarrow x'_{\psi_2,h(\psi_2)} \vee (x'_{\psi_1,h(\psi_1)} \wedge x_{\psi,h(\psi)})))$
I^{ψ}	$I^{\psi_1} \wedge I^{\psi_2} \wedge (x_{\psi} \leftrightarrow x_{\psi_2})$	$I^{\psi_1} \wedge I^{\psi_2} \wedge (x_{\psi,0} \leftrightarrow x_{\psi_2,0})$
F^{ψ}	$F^{\psi_1} \cup F^{\psi_2}$	$F^{\psi_1} \cup F^{\psi_2}$

Preliminary Exp.s w/ Incremental BMC — Raw Data

		L2S		BMC			
				zchaff		minisat	
model	spec	time [sec]	mem [MB]	time [sec]	mem [MB]	time [sec]	mem [MB]
1394-3-2	0	6.5	34.9	9.8	34.1	8.7	23.9
	1	5.9	35.9	11.3	35.7	10.2	26.2
1394-4-2	0	382.3	665.9	430.6	122.4	423.4	102.6
	1	366.8	742.6	527.2	199.2	493.4	134.8
abp4	L	7.3	23.6	30.2	30.4	28.6	28.8
brp	¬ L	0.3	13.5	0.1	1.0	0.1	1.0
	¬ L, nv	102.5	112.9	486.5	163.2	t.o.	t.o.
dme2	L	1.0	19.3	58.7	58.1	484.4	119.2
	¬ L	0.2	11.4	0.1	1.0	0.1	1.0
	¬ L, nv	0.9	19.3	28.2	57.4	355.2	102.5
dme5	L	348.7	71.0	t.o.	t.o.	t.o.	t.o.
	¬ L	1.0	17.3	0.1	1.0	0.1	1.0
	¬ L, nv	360.8	63.2	t.o.	t.o.	t.o.	t.o.
dme6	L	983.6	133.4	t.o	t.o.	t.o	t.o.
	¬ L	1.5	18.3	0.1	1.0	0.1	1.0
	¬ L, nv	866.8	115.5	t.o.	t.o.	t.o.	t.o.
pci	L	m.o.	m.o.	47.5	54.6	104.5	72.8
	F L	m.o.	m.o.	701.6	126.2	2480.2	478.8
	¬ L	0.9	17.1	0.1	13.8	0.1	1.0
prod-cons	0	243.4	175.7	109.7	63.8	299.9	158.2
	1	61.1	69.6	22.2	33.6	25.1	29.2
	2	61.8	73.8	4.7	27.1	103.7	53.5
	3	63.0	77.3	27.9	32.7	25.6	29.4
production-cell	0	15.5	25.0	30.0	73.5	511.1	111.2
	1	t.o.	t.o	241.8	187.0	559.9	130.4
bc57-sensors	0	211.2	159.6	1112.8	349.2	2306.6	300.1
srg5	¬ L	0.1	11.2	0.1	1.0	0.1	1.0
	¬ L, nv	1.2	20.0	0.1	1.0	0.1	1.0

red: best overall   blue: best BMC

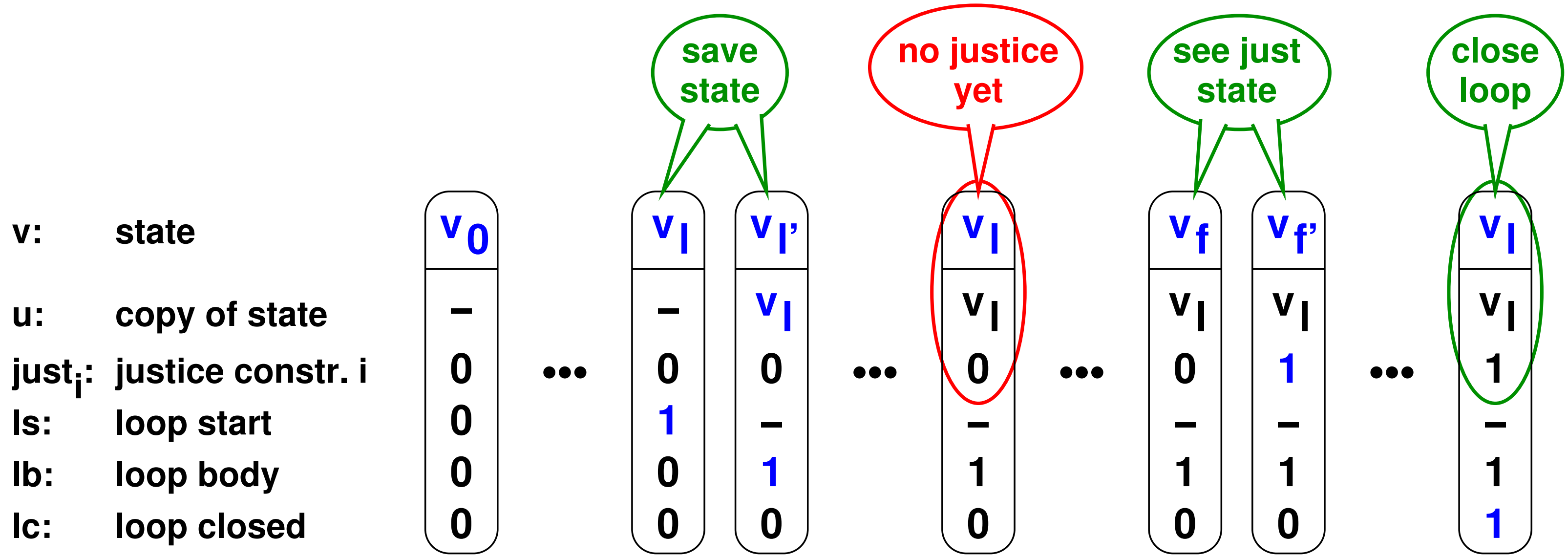
Templates of Properties

model	prop	template
1394-3/4-2	0	$\neg((\mathbf{F}(\mathbf{G}(p))) \rightarrow (\neg((q)\ \mathbf{S}\ (r))))$
	1	$\neg(\mathbf{F}((p) \mid ((q \mid (r))))$
abp4	L	$\mathbf{G}((p) \rightarrow (Y(H(q))))$
brp	¬ L	$\neg(\mathbf{F}(\mathbf{G}((p) \rightarrow (\mathbf{O}((q) \rightarrow (O(r)))))))$
	¬ L, nv	$\neg((\mathbf{F}(\mathbf{G}((p) \rightarrow (\mathbf{O}((q) \rightarrow (\mathbf{O}(r))))))) \wedge ((\mathbf{G}(\mathbf{F}(p))) \wedge (\mathbf{G}(\mathbf{F}(q)))))$
dme2/5/6	(L)	$\mathbf{G}((p) \rightarrow ((p)\ \mathbf{T}\ ((\neg(p))\ \mathbf{T}\ (\neg(q)))))$
	¬ L	$\neg\mathbf{G}((p) \rightarrow ((p)\ \mathbf{T}\ ((\neg(p))\ \mathbf{T}\ (\neg(q)))))$
	¬ L, nv	$\neg((\mathbf{G}((p) \rightarrow ((p)\ \mathbf{T}\ ((\neg(p))\ \mathbf{T}\ (\neg(q)))))) \wedge (\mathbf{G}(\mathbf{F}(p))))$
pci	(L)	$\mathbf{G}((p) \rightarrow (\mathbf{G}(((q) \wedge (\mathbf{Y}((r) \wedge (\mathbf{O}((s) \wedge (\mathbf{O}((t) \wedge (\mathbf{O}(u))))))))) \rightarrow$ $(\mathbf{O}((v) \wedge (\mathbf{O}((w) \wedge (\neg(\mathbf{O}(x))))))))))$
	F L	$\mathbf{F}(\mathbf{G}((p) \rightarrow (\mathbf{G}(((q) \wedge (\mathbf{Y}((r) \wedge (\mathbf{O}((s) \wedge (\mathbf{O}((t) \wedge (\mathbf{O}(u))))))))) \rightarrow$ $(\mathbf{O}((v) \wedge (\mathbf{O}((w) \wedge (\neg(\mathbf{O}(x)))))))))))$
	(¬ L)	$\neg(\mathbf{G}((p) \rightarrow (\mathbf{G}(((q) \wedge (\mathbf{Y}((r) \wedge (\mathbf{O}((s) \wedge (\mathbf{O}((t) \wedge (\mathbf{O}(u))))))))) \rightarrow$ $(\mathbf{O}((v) \wedge (\mathbf{O}((w) \wedge (\neg(\mathbf{O}(x)))))))))))$
prod-cons	0	$\neg(((\mathbf{G}(\neg(p))) \wedge (\mathbf{G}(\mathbf{F}((q) \wedge ((q)\ \mathbf{S}\ (r)))))) \wedge (\mathbf{G}(\mathbf{F}(((q) \wedge ((q)\ \mathbf{S}\ (r))) \rightarrow ((s)\ \mathbf{S}\ (t))))))$
	1	$\neg((\mathbf{G}((p) \rightarrow ((p)\ \mathbf{S}\ ((q)\ \mathbf{S}\ ((r)\ \mathbf{S}\ ((s)\ \mathbf{S}\ (t))))))) \wedge (\mathbf{G}(\mathbf{F}(p))))$
	2	$\mathbf{G}((p) \rightarrow (\mathbf{F}(((q) \wedge (r)) \wedge (s))))$
	3	$\mathbf{G}((p) \rightarrow (\mathbf{F}(q)))$
production -cell	0	$\neg(\mathbf{G}(\mathbf{F}(((p) \vee (q)) \wedge (\mathbf{O}((r) \wedge (\mathbf{O}(((s) \vee (t)) \wedge (\mathbf{O}((u) \wedge$ $(\mathbf{O}(((v) \vee (w)) \wedge (\mathbf{O}(((x) \vee (y)) \wedge (\mathbf{O}(z))))))))))))))$
	1	$\neg(\mathbf{G}(\mathbf{F}(((p) \vee (q)) \wedge (\mathbf{Y}(\mathbf{O}((r) \wedge (\mathbf{Y}(\mathbf{O}(((s) \vee (t)) \wedge (\mathbf{Y}(\mathbf{O}((u) \wedge$ $(\mathbf{Y}(\mathbf{O}(((v) \vee (w)) \wedge (\mathbf{Y}(\mathbf{O}(((x) \vee (y)) \wedge (\mathbf{Y}(\mathbf{O}(z))))))))))))))))))))$
bc-57 -sensors	0	$\neg(\mathbf{G}(\mathbf{F}((p) \wedge (\mathbf{O}((q) \wedge (\mathbf{F}((r) \wedge (\mathbf{O}(s)))))))))$
srg5	¬ L	$\neg((((\mathbf{F}(\mathbf{G}(\neg(p)))) \wedge (\mathbf{G}(\mathbf{F}(q)))) \wedge (\mathbf{G}(\mathbf{F}(r)))) \rightarrow (\mathbf{F}((s)\ \mathbf{S}\ ((t)\ \mathbf{S}\ ((u)\ \mathbf{S}\ ((v)\ \mathbf{S}\ (w)))))))$
	¬ L, nv	$\neg(((((\mathbf{F}(\mathbf{G}(\neg(p)))) \wedge (\mathbf{G}(\mathbf{F}(q)))) \wedge (\mathbf{G}(\mathbf{F}(r)))) \rightarrow (\mathbf{F}((s)\ \mathbf{S}\ ((t)\ \mathbf{S}\ ((u)\ \mathbf{S}\ ((v)\ \mathbf{S}\ (w))))))) \wedge$ $(((\mathbf{F}(\mathbf{G}(\neg(p)))) \wedge (\mathbf{G}(\mathbf{F}(q)))) \wedge (\mathbf{G}(\mathbf{F}(r)))))$

(Blue): only for preliminary experiments w/ incremental BMC.

Symbolic Loop Detection

[Schuppan, Biere '04]



$$V^L = V \cup \{u, just_i, ls, lb, lc\}$$

$$\begin{aligned} T^L = T & \wedge (lb' \leftrightarrow ls \vee lb) \wedge (ls \rightarrow u' = v) \wedge (lb \rightarrow u' = u) \\ & \wedge (just_i' \rightarrow (just_i \vee (ls \vee lb) \wedge just_i(v))) \\ & \wedge (lc \rightarrow (lb \wedge u = v \wedge just_i)) \end{aligned}$$

$$I^L = I \wedge \neg lb \wedge \neg just_i$$

There exists a just loop in K $\Leftrightarrow$ there is a reachable state with $lc = 1$ in K^L.