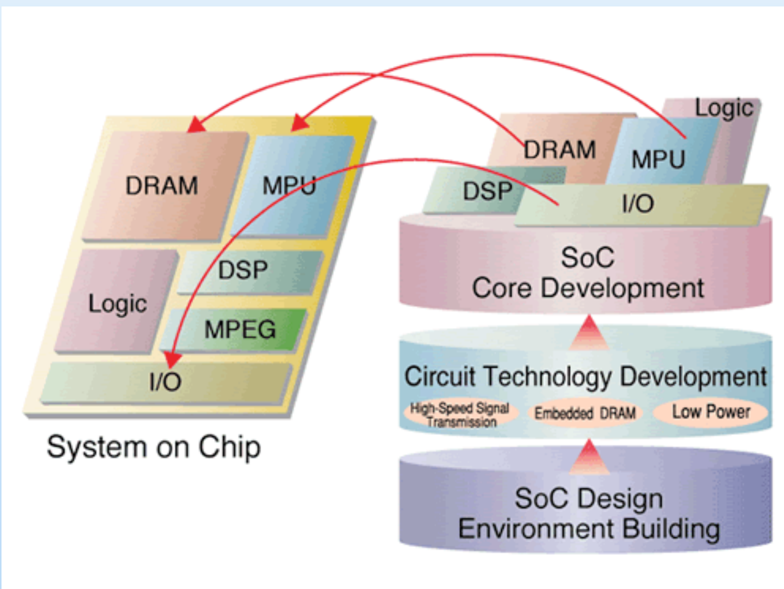
Improving Translation of Live Sequence Charts to Temporal Logic

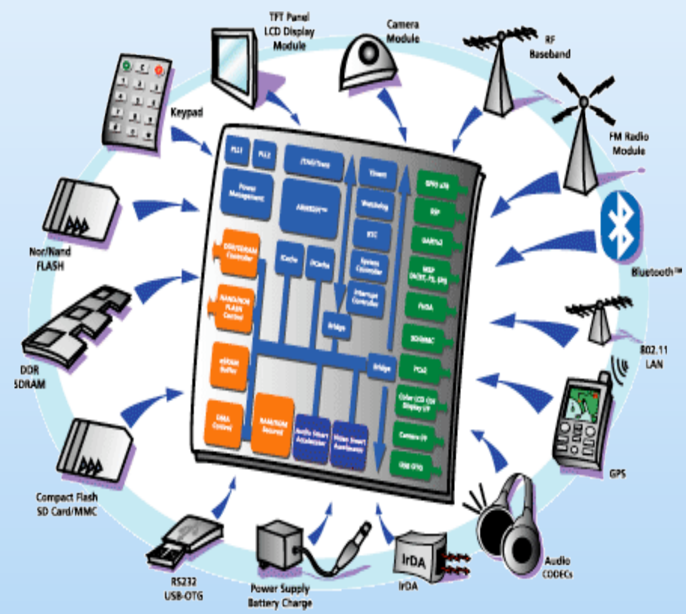
Rahul Kumar Eric Mercer Annette Bunker

AVOCS 2007

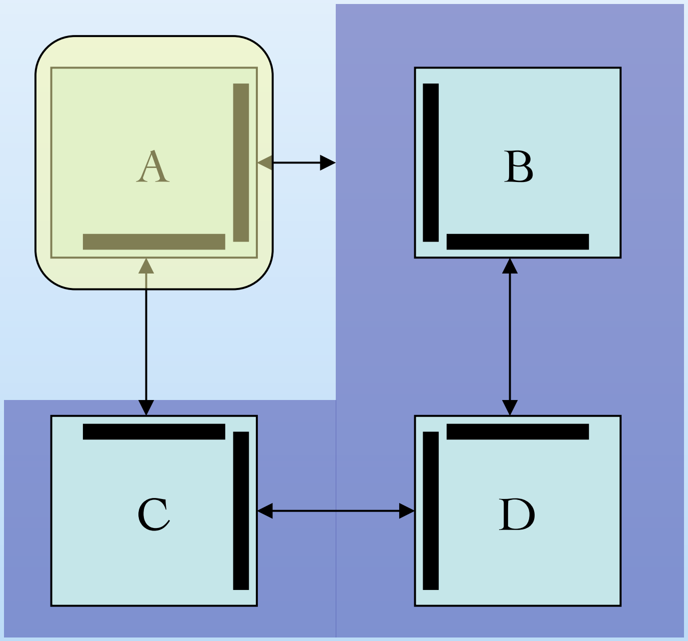
Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Trends: SoC, Multi-agent Systems





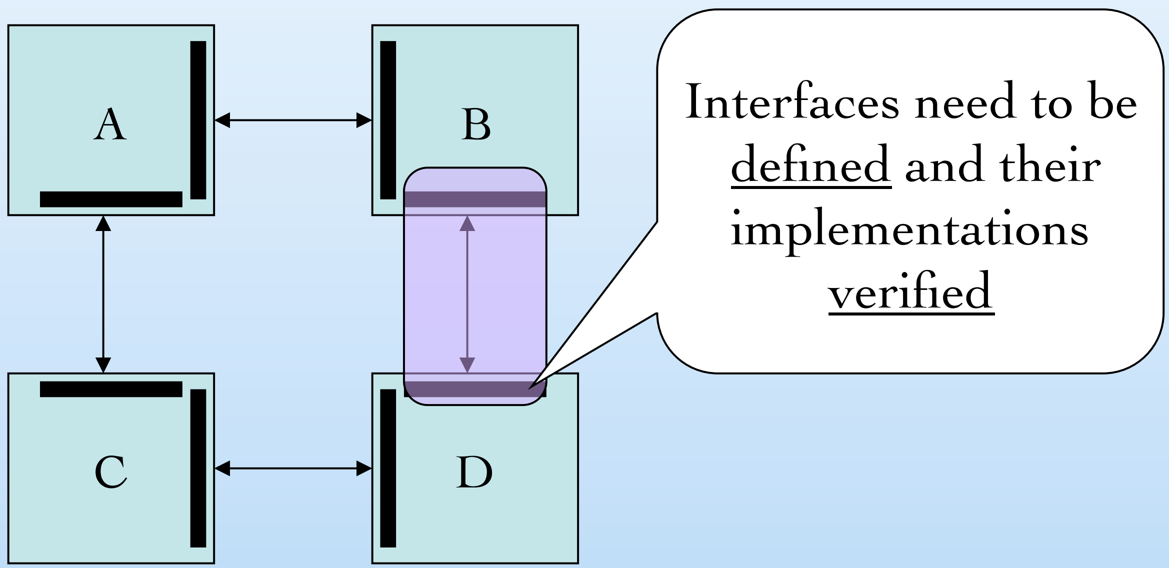
Traditional Testing



Abstracted Environment

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

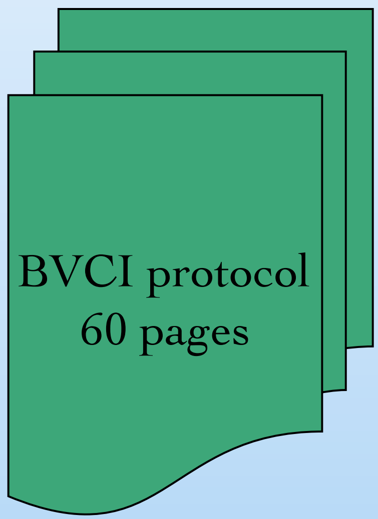
What do IP Core vendors and consumers need?

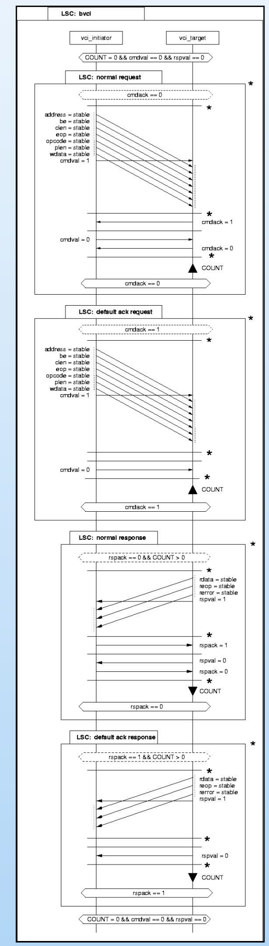


Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Scenario Based Specifications

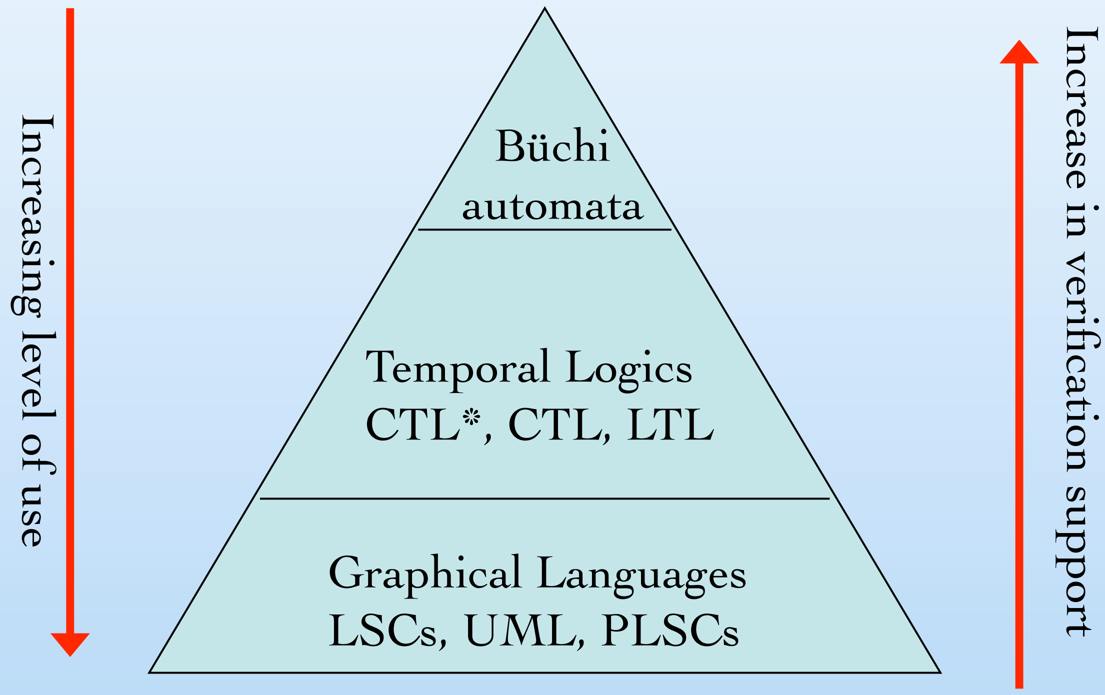
- R.Z. ITU-T 120: Message Sequence Charts
- Damm *et. al.*: Live Sequence Charts
- Bunker *et. al.*: Protocol Live Sequence Charts





Computer Science Department
Brigham Young University
Provo, UT 84606, USA

What do we have so far?



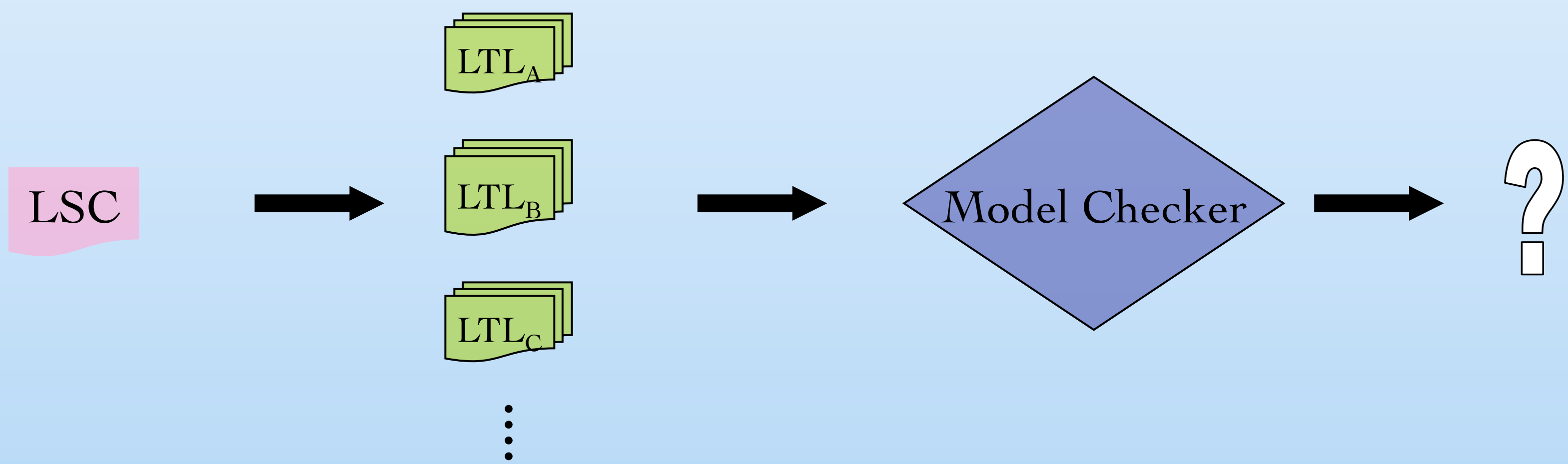
Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Verification Using Scenarios

Theoretically correct
Difficult to use

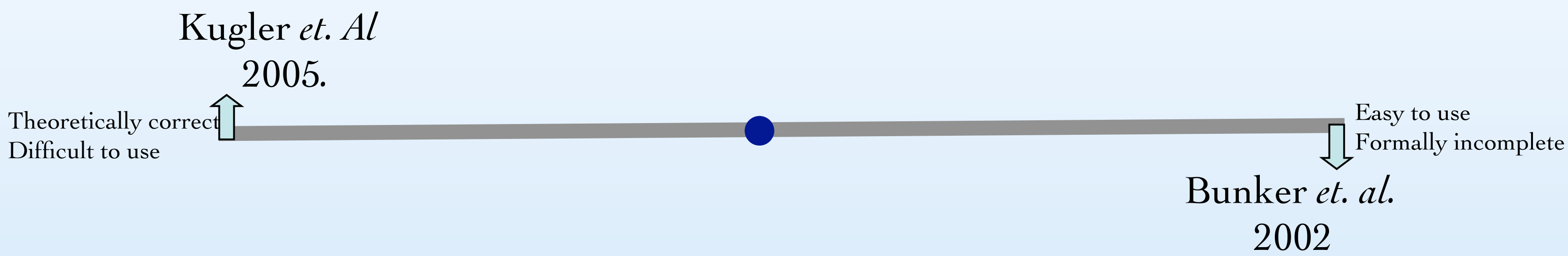
Easy to use
Formally incomplete

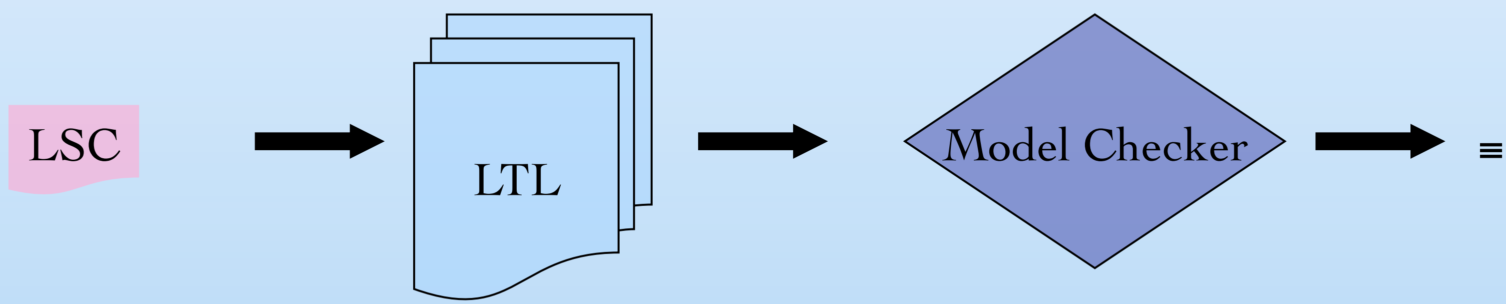
Bunker *et. al.*
2002



Computer Science Department
Brigham Young University
Provo, UT 84606, USA

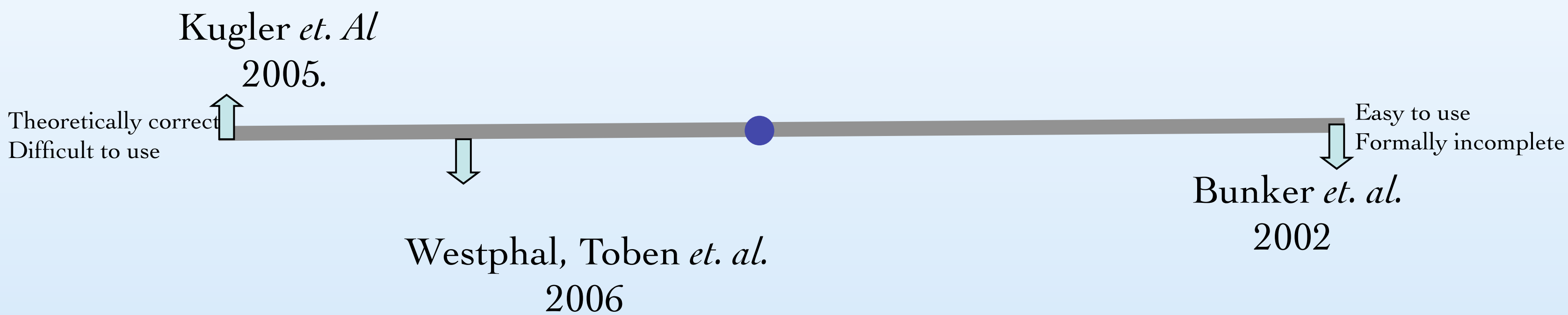
Verification Using Scenarios

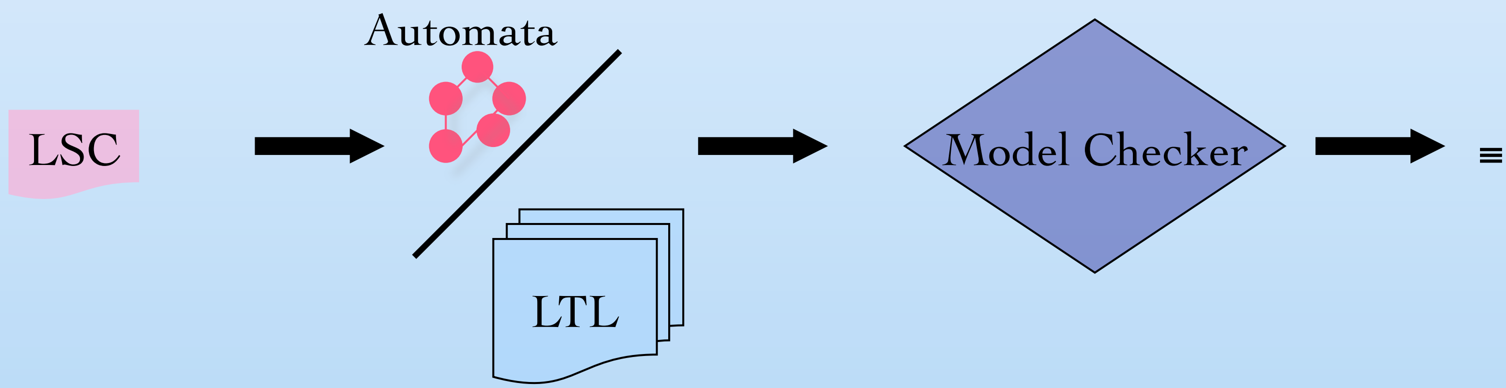




Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Verification Using Scenarios

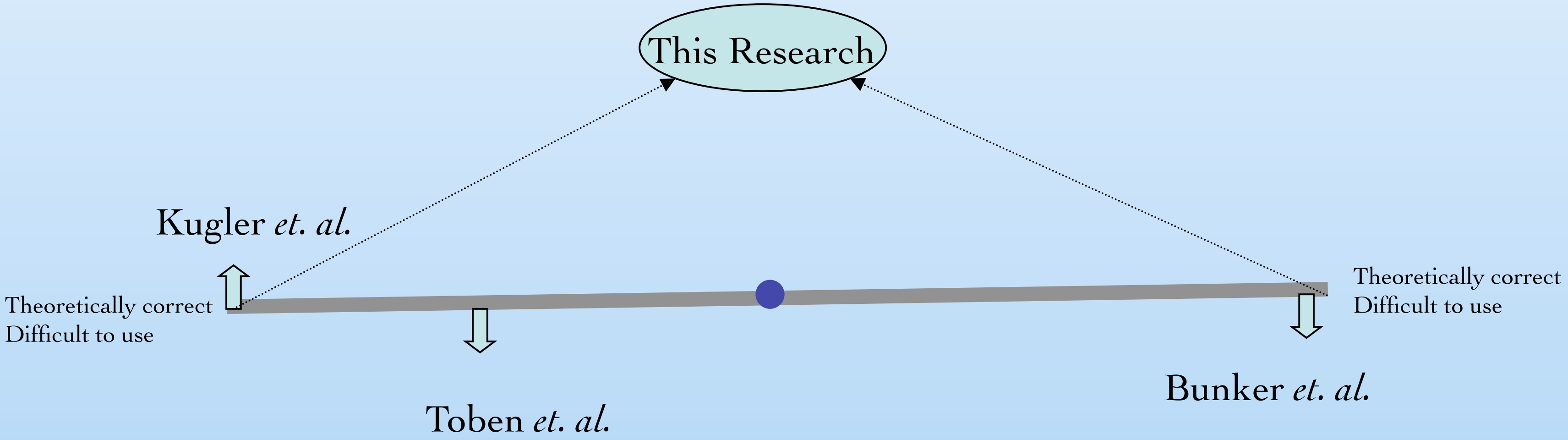




Computer Science Department
Brigham Young University
Provo, UT 84606, USA

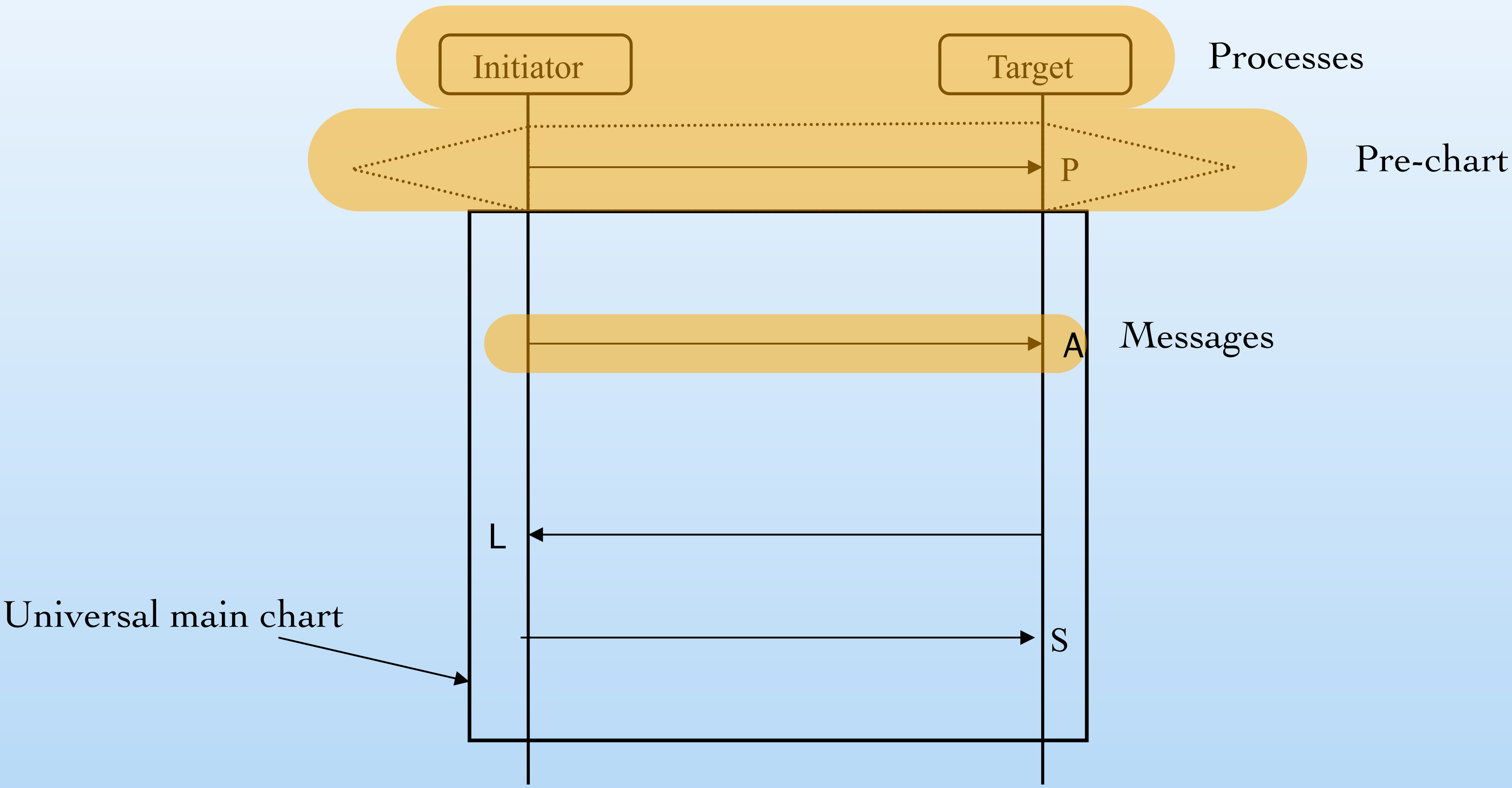
Problems & Solutions

Bridge the gap between graphical specifications and verification methodologies



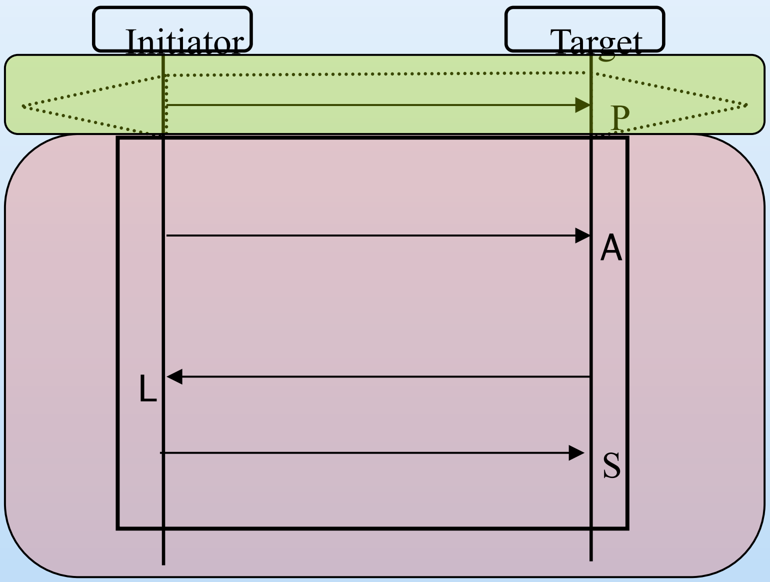
Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Live Sequence Charts



Computer Science Department
Brigham Young University
Provo, UT 84606, USA

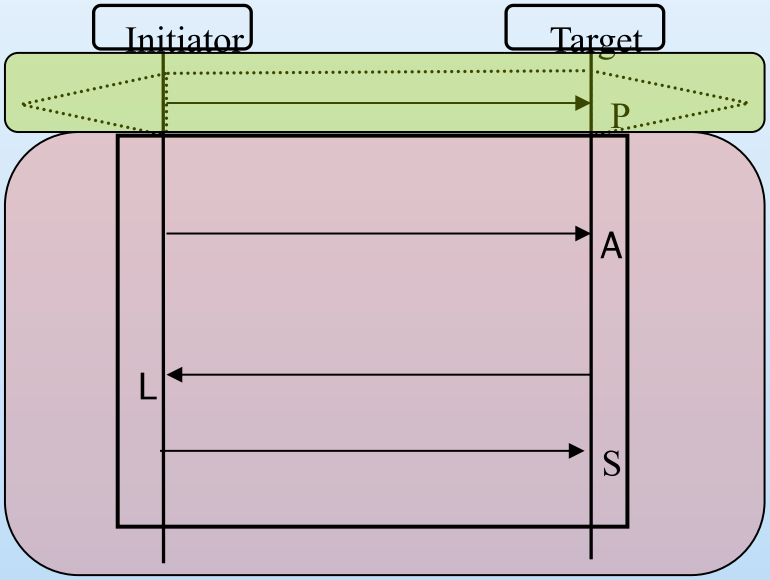
Kugler's Approach



$$G(\ \Theta_{pre} \Rightarrow \Theta_{main}\ )$$

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

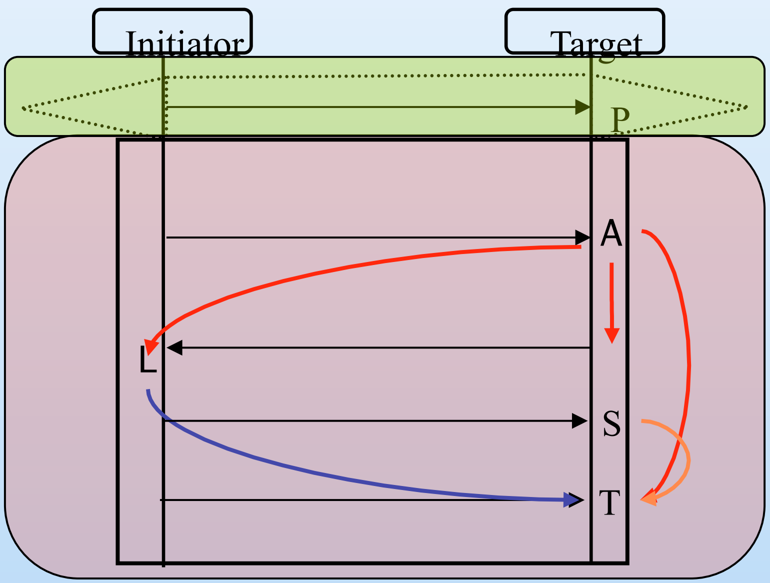
Kugler's Approach



$$G(\ P \Rightarrow \Theta_{main}\ )$$

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

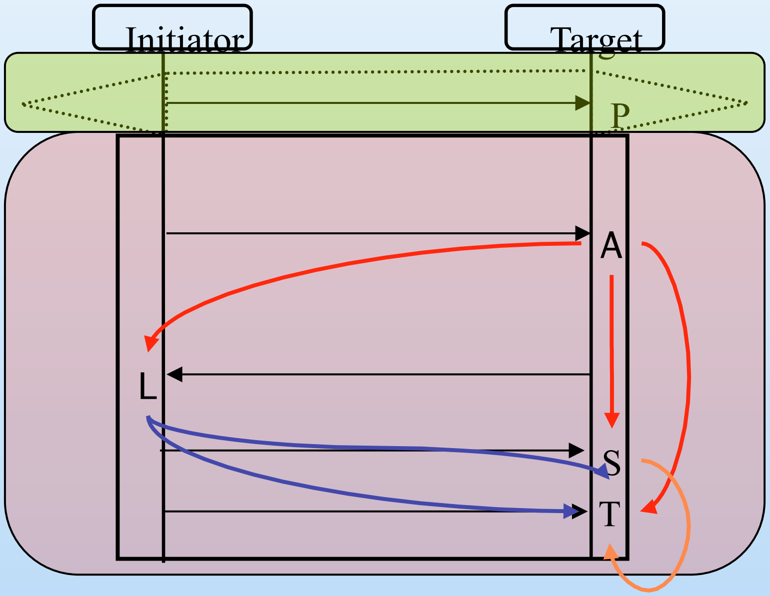
Kugler's Approach - Ordering



$$
\begin{aligned}
G(\ P \Rightarrow\ & (\neg L\ \mathcal{U}\ A) \wedge \\
& (\neg S\ \mathcal{U}\ A) \wedge \\
& (\neg T\ \mathcal{U}\ A) \wedge \\
& (\neg S\ \mathcal{U}\ L) \wedge \\
& (\neg T\ \mathcal{U}\ L) \wedge \\
& (\neg T\ \mathcal{U}\ S) \wedge \\
& (\mathcal{F}\ T))
\end{aligned}
$$

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Kugler's Approach - Uniqueness

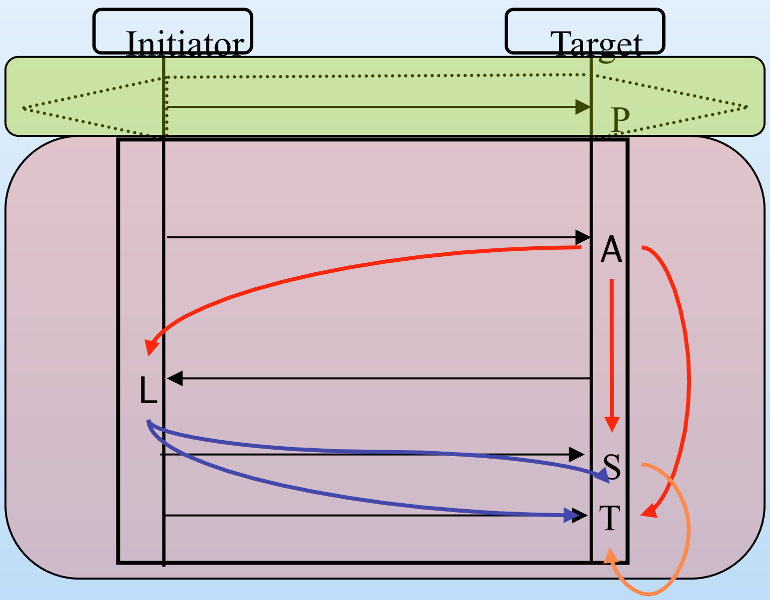


$$G(\ P \Rightarrow \neg\chi_{A,L} \wedge \neg\chi_{A,S} \wedge \neg\chi_{A,T} \wedge$$
$$\neg\chi_{L,S} \wedge \neg\chi_{L,T} \wedge$$
$$\neg\chi_{S,T}\ )$$

$\neg\chi_{a,b}$: $(\neg b \wedge \neg a)\ U\ (a \wedge X((\neg b \wedge \neg a)\ U\ a))$

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Kugler's Approach - Total



$G(\ P \Rightarrow (\neg L\ \boldsymbol{U}\ A) \wedge \neg\chi_{A,L} \wedge \neg\chi_{A,S} \wedge \neg\chi_{A,T} \wedge$

$(\neg S\ \boldsymbol{U}\ A) \wedge \neg\chi_{L,S} \wedge \neg\chi_{L,T} \wedge$

$(\neg T\ \boldsymbol{U}\ A) \wedge \neg\chi_{S,T} \wedge$

$(\neg S\ \boldsymbol{U}\ L) \wedge$

$(\neg T\ \boldsymbol{U}\ L) \wedge$

$(\neg T\ \boldsymbol{U}\ S) \wedge$

$(\boldsymbol{F}\ T))$

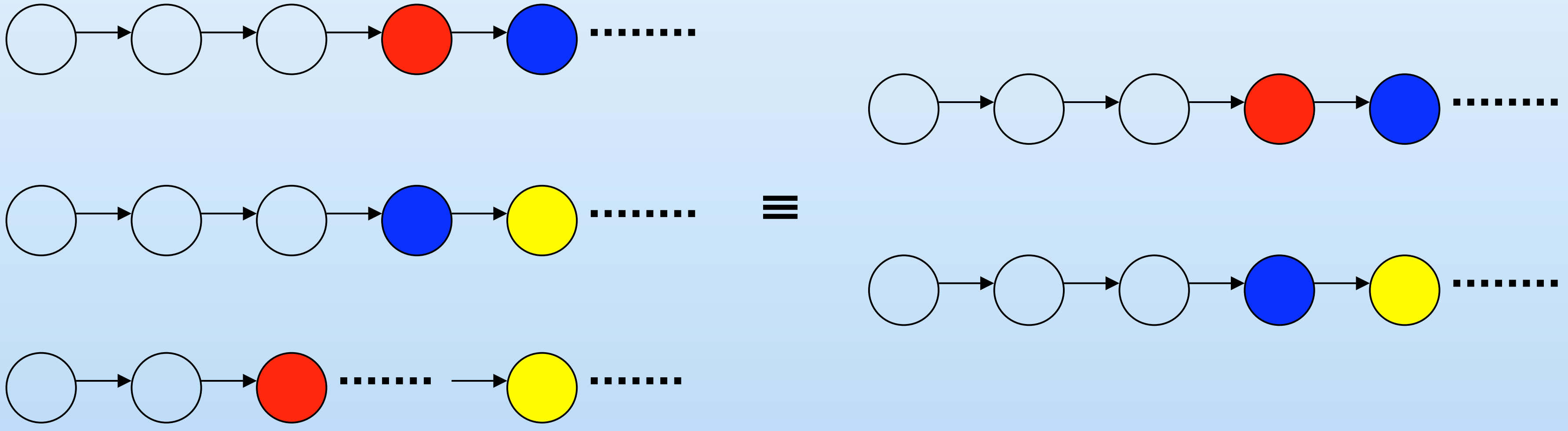
Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Kugler's Approach - Drawbacks

- Very large formulas for small charts
- LTL to automata fails for large charts
- Verification fails for larger charts/models
- Limited set of LSC constructs translated

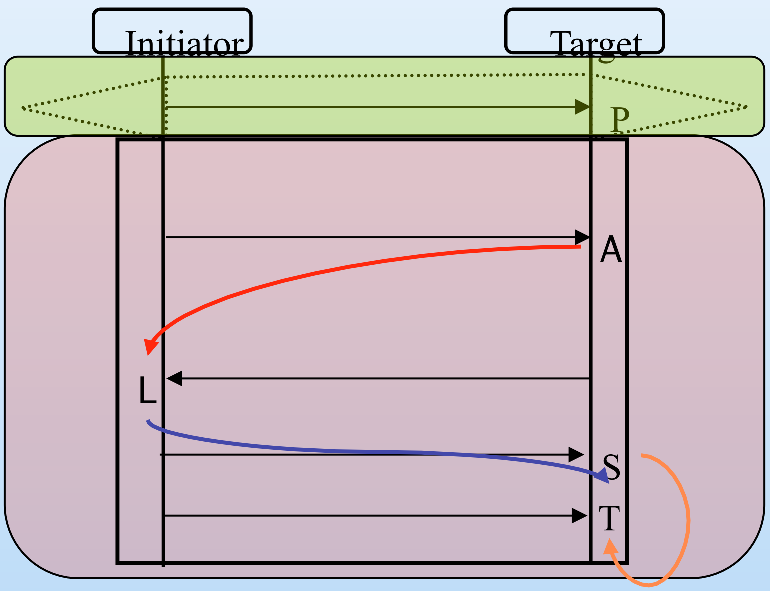
Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Reductions: Until Transitivity



Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Reductions: Using Until Reduction



$G($ pre $\Rightarrow (\neg L\ \mathcal{U}\ A) \wedge$

~~$(\neg S\ \mathcal{U}\ A) \wedge$~~

~~$(\neg T\ \mathcal{U}\ A) \wedge$~~

$(\neg S\ \mathcal{U}\ L) \wedge$

~~$(\neg T\ \mathcal{U}\ L) \wedge$~~

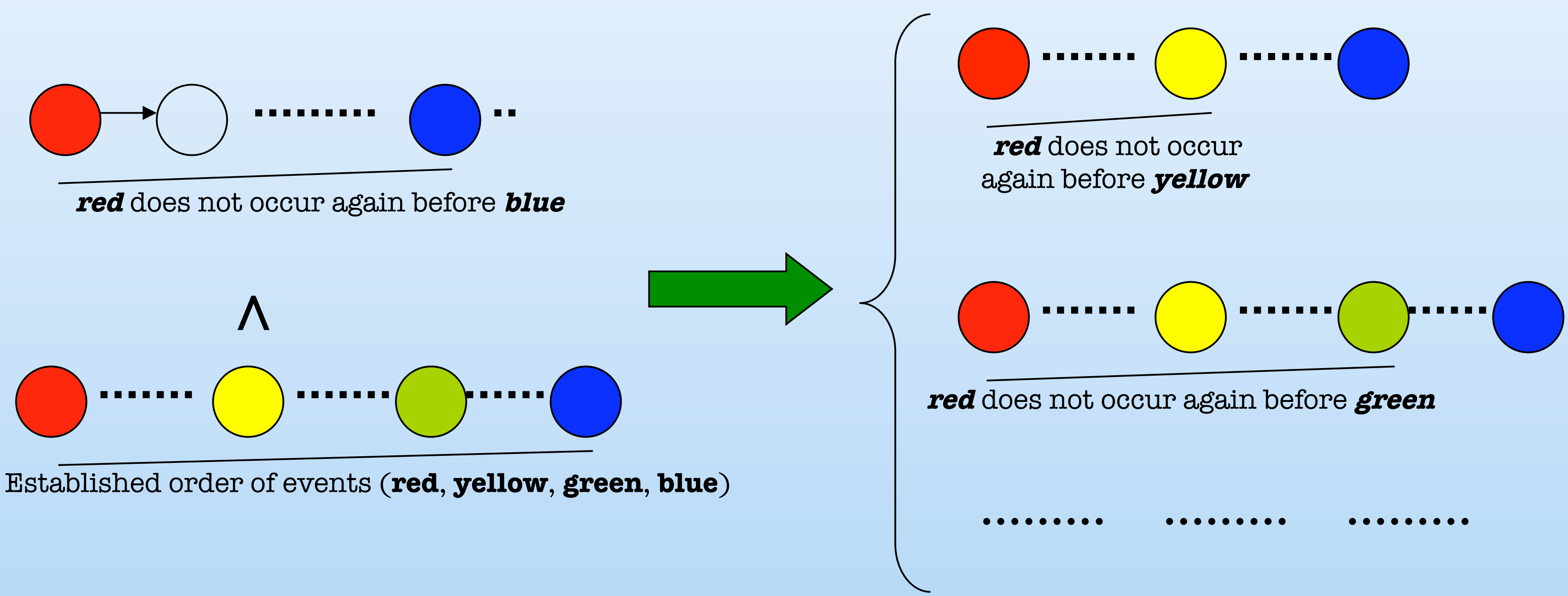
$(\neg T\ \mathcal{U}\ S) \wedge$

$(\mathcal{F}\ T))$

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

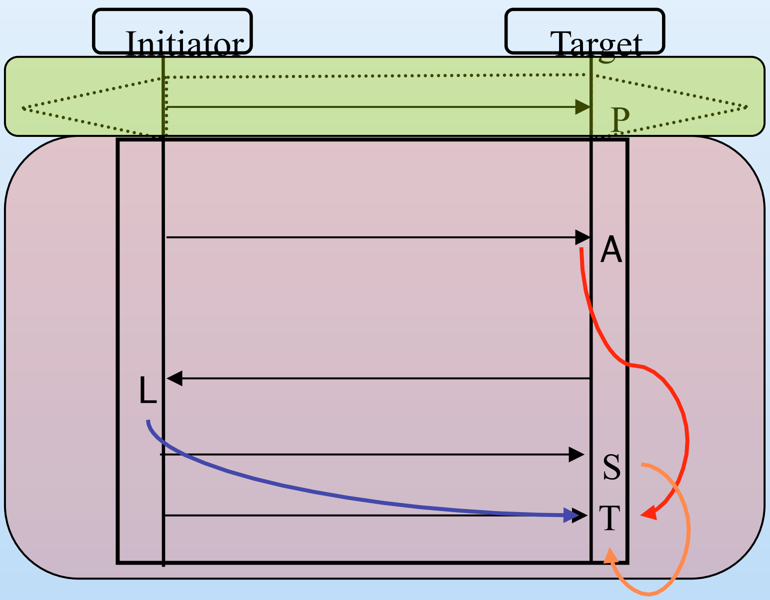
Reductions: Uniqueness

Using Coverage to Specify Uniqueness



Computer Science Department
Brigham Young University
Provo, UT 84606, USA

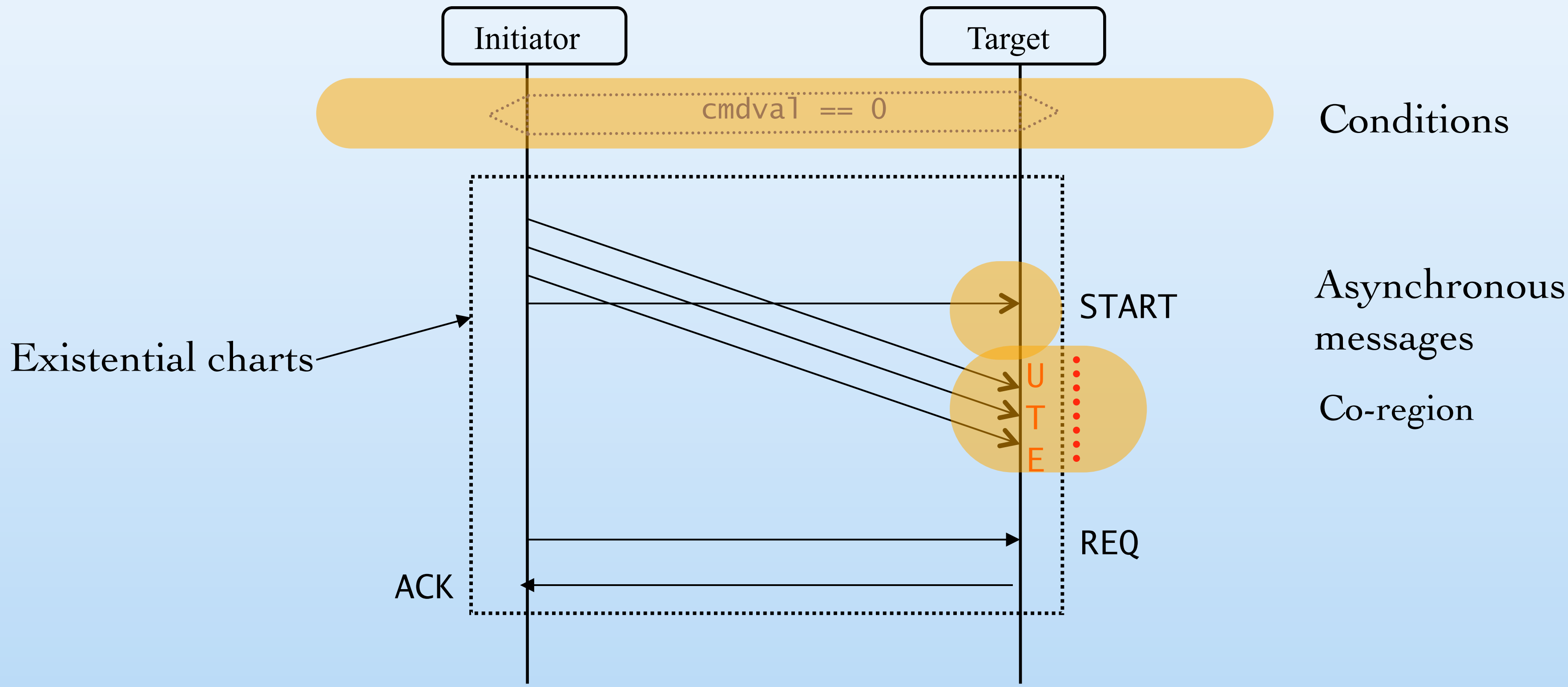
Using Uniqueness Reduction



$$G(\ pre \Rightarrow \neg\chi_{A,L} \wedge \neg\chi_{A,S} \wedge \neg\chi_{A,T} \wedge \neg\chi_{L,S} \wedge \neg\chi_{L,T} \wedge \neg\chi_{S,T}\ )$$

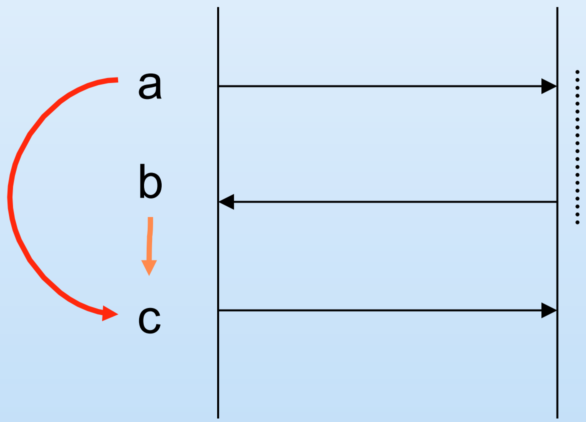
Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Additional Constructs



Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Co-regions

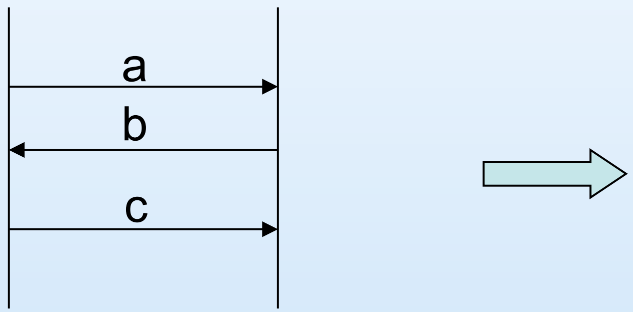


$(\neg c\ \boldsymbol{U}\ a) \wedge$
$(\neg c\ \boldsymbol{U}\ b) \wedge \boldsymbol{F}\ c$

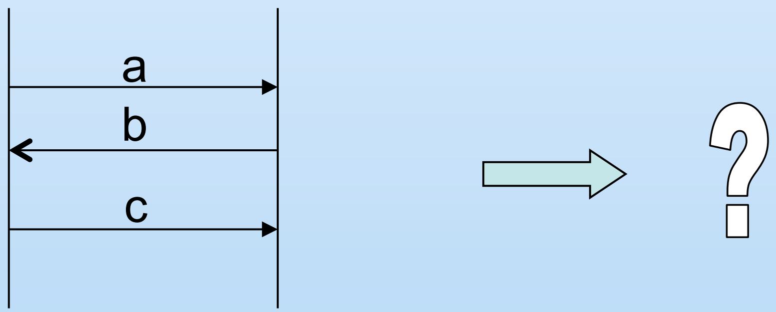
Force a,b to occur but in any order

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Asynchronous Messages



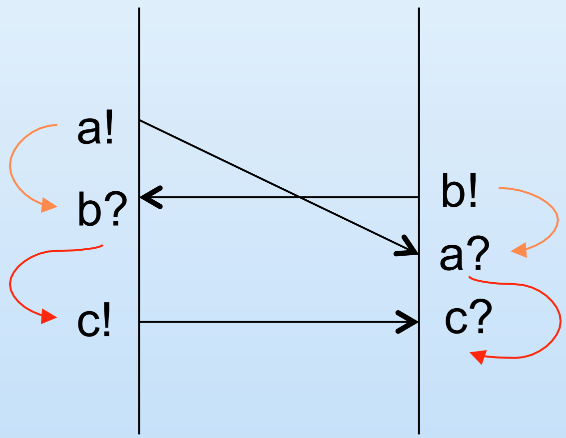
Single letter per message



Describe send and receive events

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Asynchronous Messages



$(\neg b?\ \boldsymbol{U}\ b!) \wedge (\neg a?\ \boldsymbol{U}\ a!) \wedge (\text{assumption})$

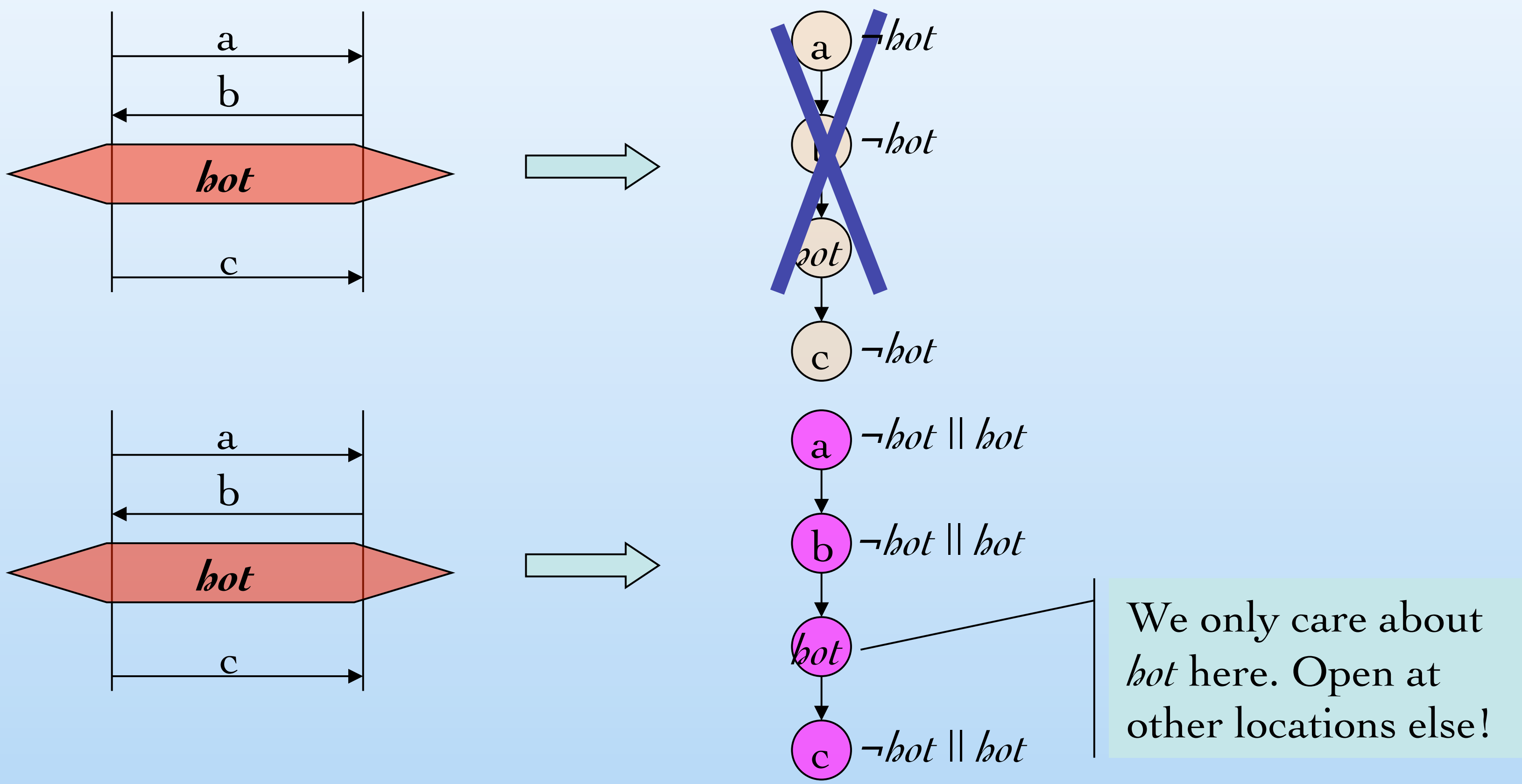
$(\neg b?\ \boldsymbol{U}\ a!) \wedge (\neg a?\ \boldsymbol{U}\ b!) \wedge$

$(\neg c?\ \boldsymbol{U}\ a?) \wedge (\neg c!\ \boldsymbol{U}\ b?) \wedge$

$\boldsymbol{F}\ c? \wedge \boldsymbol{F}\ c!$

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

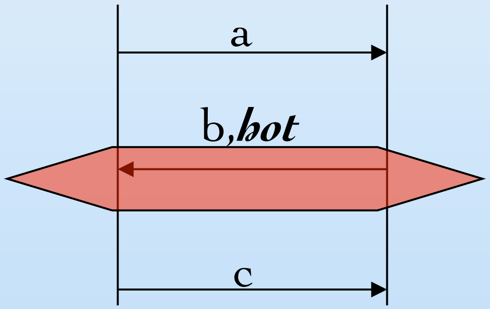
Conditions



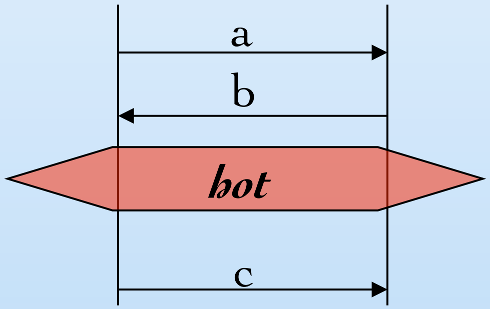
Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Conditions

Bonded Conditions



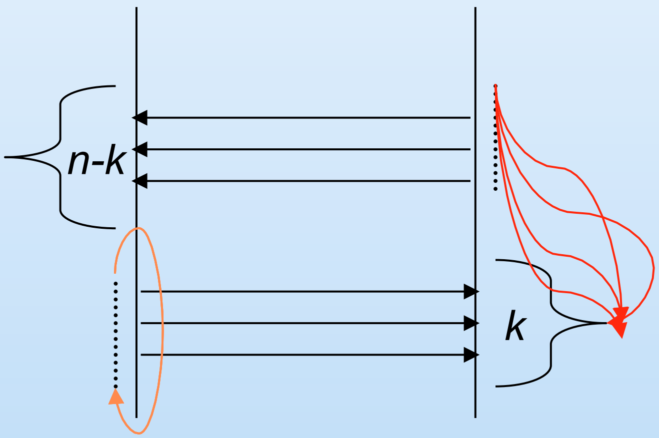
Non-bonded Conditions



Translation undecided

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Analysis



Worst case chart

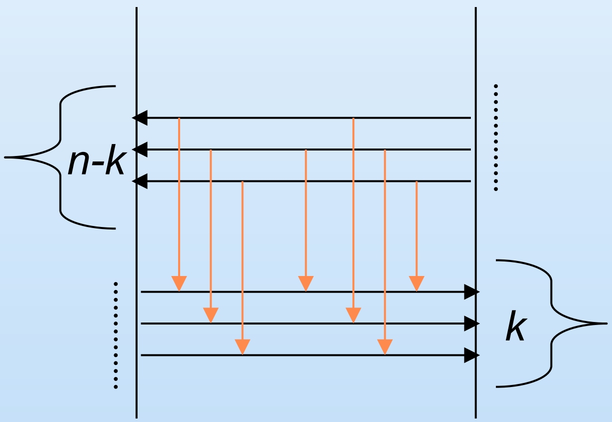
Ordering

n-k properties to order first n messages before *k* messages
k properties for enforcing occurrence of final k messages

n

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Analysis



Worst case chart

<u>Uniqueness</u>

k properties for each of the n messages
(k-1) properties for each of the k messages

$$n*k$$

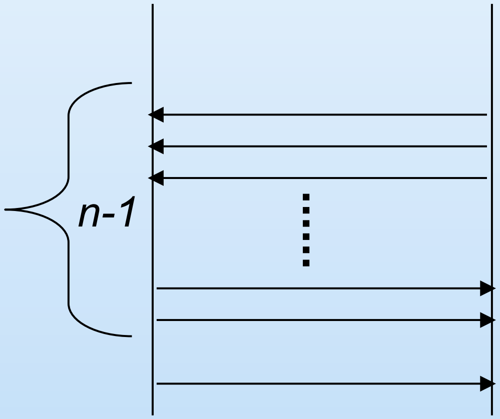
Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Analysis

For chart of size *n* & 1 maximal message:

Ordering: *n* properties

Uniqueness: *n* properties

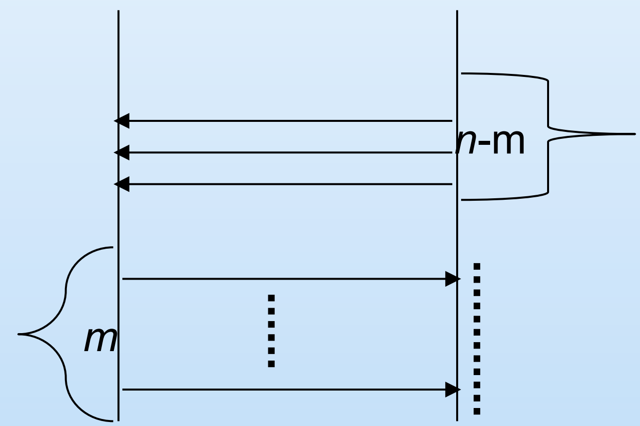


Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Analysis

Multiple maximal messages *(m)*:
Ordering: n
Uniqueness: $n*m$

As $m \rightarrow n$, formula becomes quadratic



Computer Science Department
Brigham Young University
Provo, UT 84606, USA

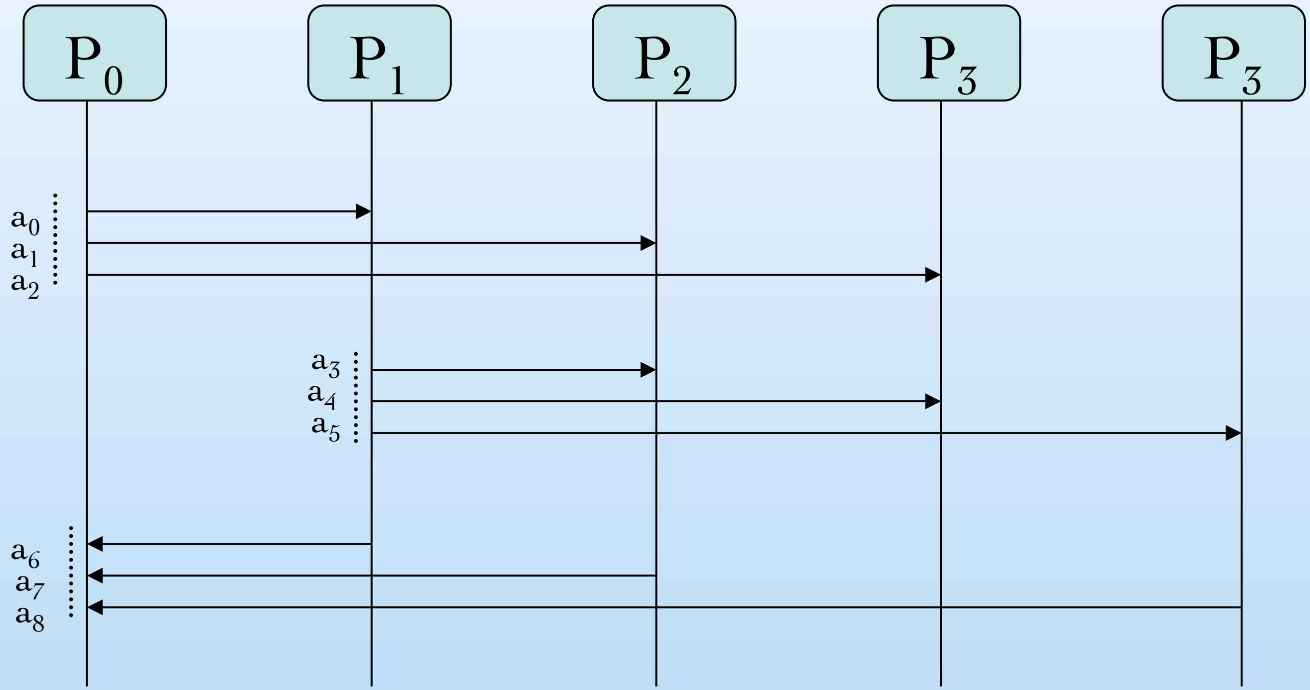
Theoretical Results

- Ordering in linear properties
- Uniqueness in sub-quadratic properties
- Translation at *most* as opposed to at *least* quadratic
- Additional constructs
  - Existential charts
  - Co-regions
  - Asynchronous messages
  - Invariants and bonded conditions

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Experiments - Specifications

<u>A3 specification</u>



Other specifications with 5-7 messages

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Experiments - Models and Verifiers

- Models
  - Promela models with simple message passing
  - Puzzle models followed by messages
  - "**_e**" models contain errors in main chart
- SPIN and NuSMV for model checking
- LTL2BA: explicit state automata generation

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Empirical Results - LTL2BA

Specification	**Messages**		**Kugler's Translation**		**Improved Translation**	
	Total Messages	Maximal Messages	Size	Time (s)	Size	Time (s)
SpecA	5	1	209	59	109	1
SpecB	5	2	175	428	142	2
SpecC	**7**	**2**	**LTL2BA DNF**		**139**	**2**

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Empirical Results - SPIN

Specification	Model	Kugler'sTranslation		Improved Translation	
		States	Time (s)	States	Time (s)
SpecB	SysA	2612	0.02	2158	0.02
	SysA_e	2446	0.07	1965	0.06
SpecC	SysB	-		4175	0.03
	SysB_e	-		4589	0.12
A2	**Soko**	**3847560**	**104**	**1557700**	**36**
	Soko_e	**1479320**	**32**	**620902**	**12**
A3	Soko	-		2840220	69
	Soko_e	-		1031970	22

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Empirical Results - NuSMV

Specification	Model	States	Kugler's Time (s)	Improved Time (s)
A2	bridge	76992	14	5
	Abp4	2236420	30	11
	Bridge_e	76992	29	13
	Abp4_e	2236420	76	27
A3	bridge	76992	22	8
	abp4	2236420	59	20
	Bridge_e	76992	56	20
	Abp4_e	2236420	146	50
A4	**bridge**	**76992**	**49**	**11**
	abp4	2236420	174	29
	Bridge_e	76992	132	26
	Abp4_e	**2236420**	**337**	**67**
A5	bridge	76992	175	26
	abp4	2236420	555	73
	Bridge_e	76992	509	56
	Abp4_e	**2236420**	**1271**	**131**

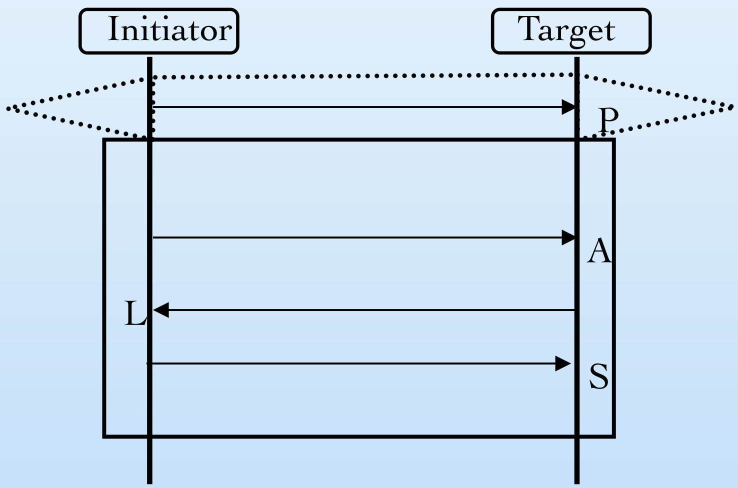
Computer Science Department
Brigham Young University
Provo, UT 84606, USA

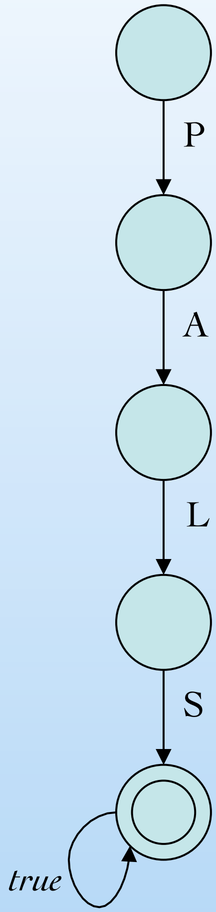
Conclusions

- Reductions produce vast improvement
- Scalability still limited in explicit state
- Translating constructs can be difficult
- Is this translation minimal?
- What about LSC to automata?

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

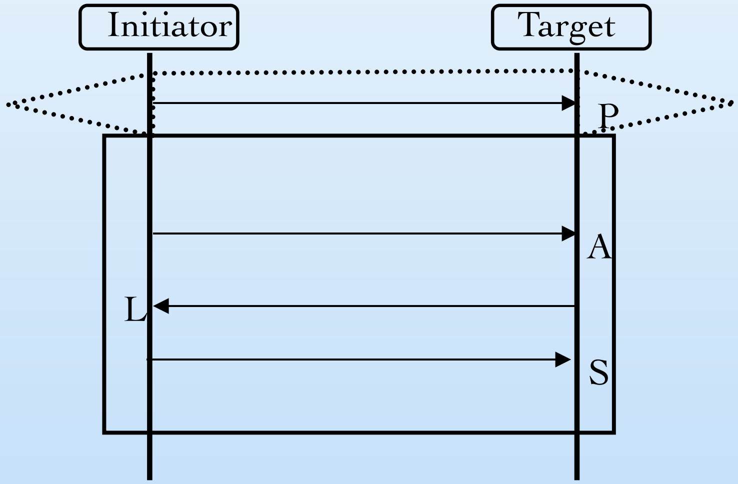
LSC To Automata: Traditional Method



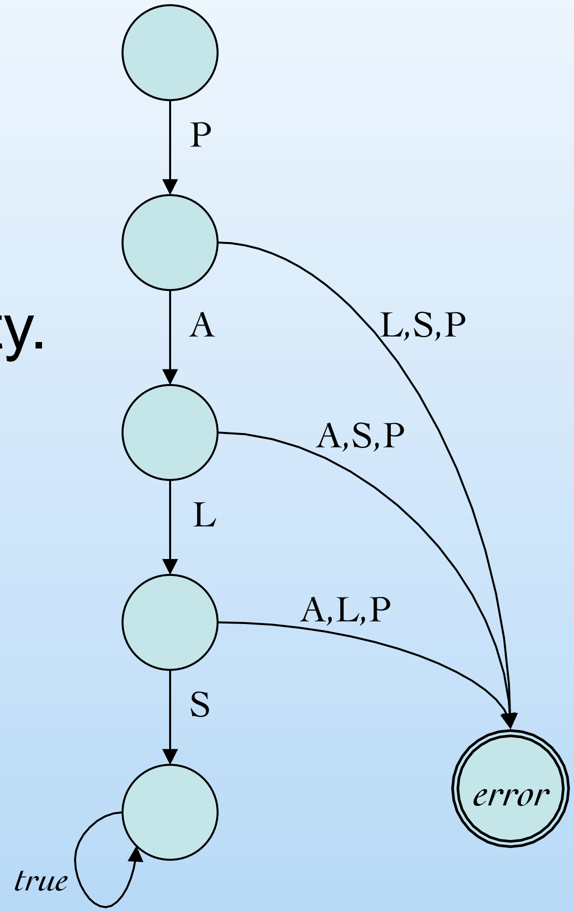


Computer Science Department
Brigham Young University
Provo, UT 84606, USA

LSC To Automata: Reachability

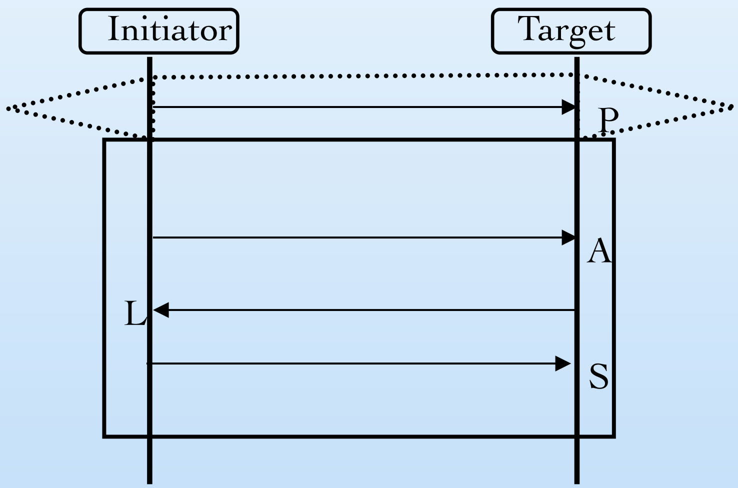


Verify safety.

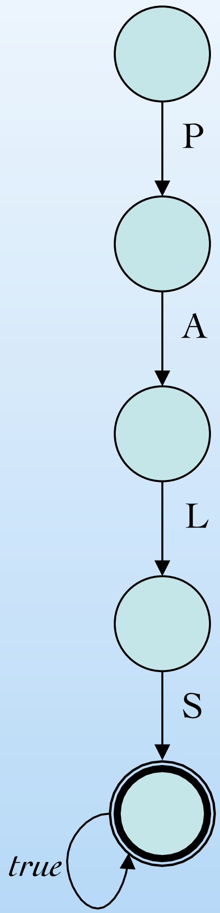


Computer Science Department
Brigham Young University
Provo, UT 84606, USA

LSC To Automata: Liveness

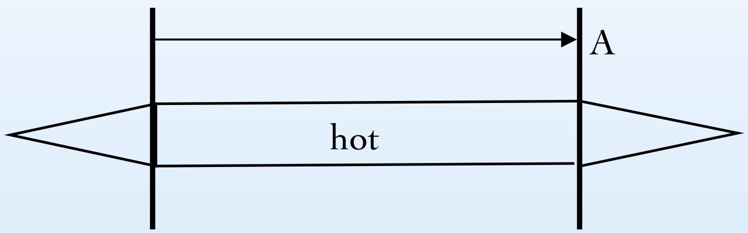


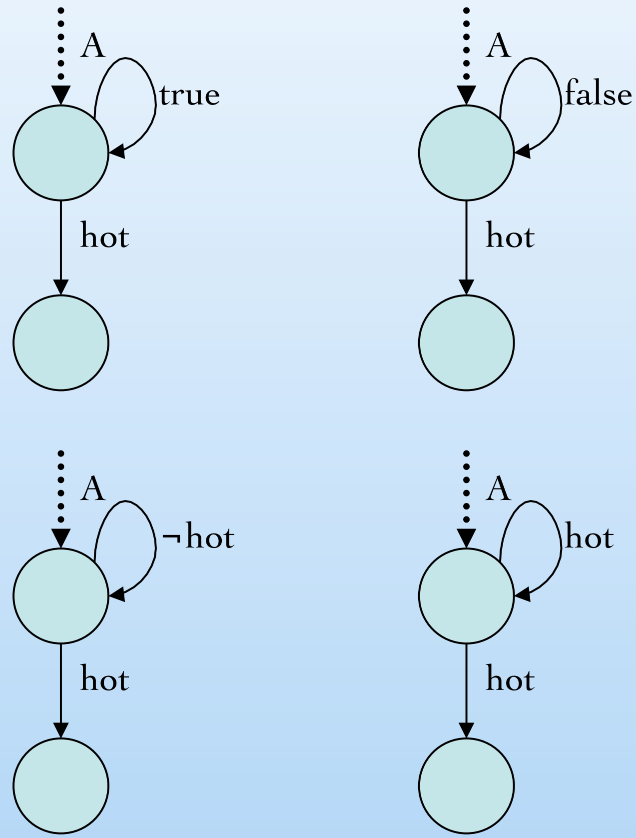
Verify *AGAF(fair)* to enforce progress



Computer Science Department
Brigham Young University
Provo, UT 84606, USA

LSC to Automata: Conditions





How do you detect errors without introducing non-determinism?

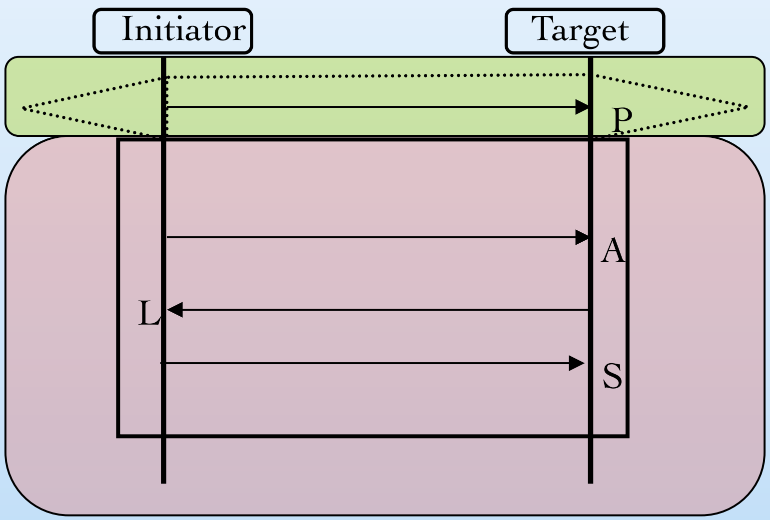
Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Drawbacks

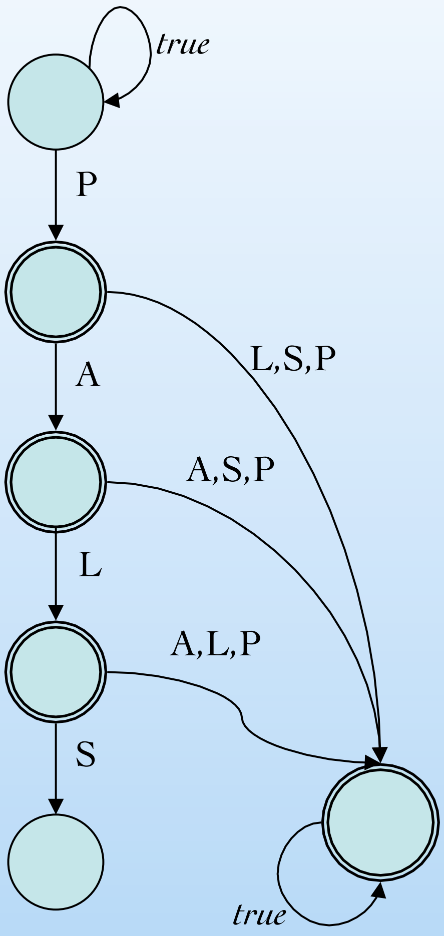
- Safety and progress checking performed in two separate runs
- Non-determinism because of conditions
- Undecided semantics of conditions

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

New Solution

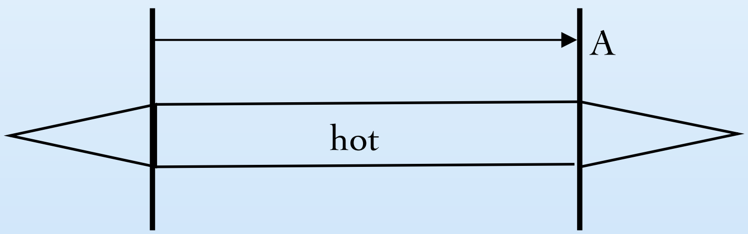


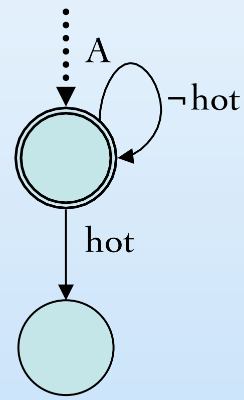
Safety and Liveness in one run by verifying $EGEF(error)$



Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Conditions in New Solution





Placement of error state fixes the problem of non-determinism as well as detecting errors!

Computer Science Department
Brigham Young University
Provo, UT 84606, USA

Advantages

- One shot verification using LSCs
- All constructs supported
- No non-determinism
- More error states means faster detection of errors in system
- Simple unwinding algorithm

Computer Science Department
Brigham Young University
Provo, UT 84606, USA