Automated Theory Formation and Refinement Based Modelling

Maria Teresa Llano[1] Andrew Ireland[1] Alison Pease[2]

[1]School of Mathematical and Computer Sciences
Heriot-Watt University

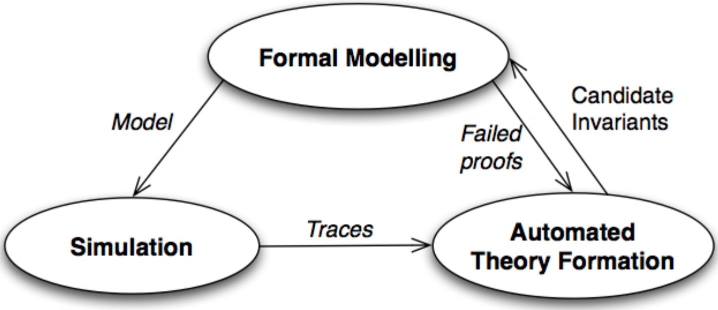
[2]School of Informatics
University of Edinburgh

June, 2011

Motivation

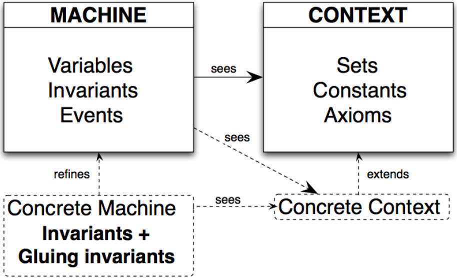
- The identification of invariants is a key aspect of the verification of formal models and the development of reliable systems.
- Discovering correct and meaningful invariants for a model represents a significant challenge.
- Increasing the level of automation in discovering invariants will:
  - Ripe productivity gains.
  - Increase the accessibility of formal modelling platforms.
- We have experimented the use of Automated Theory Formation (ATF) techniques to reason about software requirements and suggest candidate invariants.
- Aim is to use experimental results as the basis for future tool design.
- Funding: "A Cognitively Based Model of Theory Formulation and Reformulation" – EP/F035594, EP/F037058, EP/F036647; BAE Systems Studentship (Warton).

Our Approach



Event-B

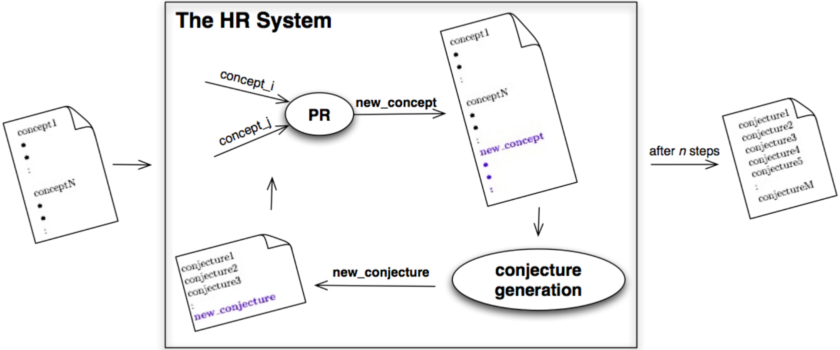
- A formalism that supports modelling and reasoning of discrete event systems.
- Based on the B-method developed by *Jean-Raymond Abrial*.
- Uses first order logic and set theory to represent models.
- An Event-B model is composed of *machines* and *contexts*.



- Promotes the evolution of models through *refinement*.
- Uses mathematical proof to verify the consistency between refinement levels.

ATF and HR

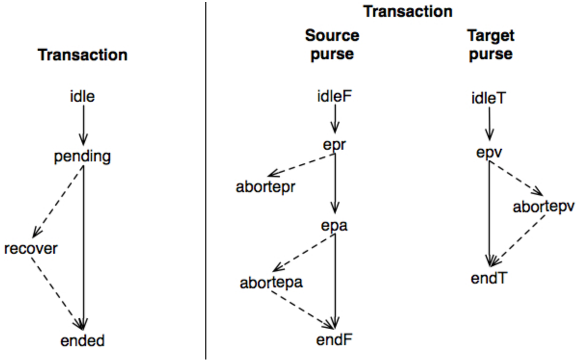
- ATF is a machine learning technique that builds theories about objects of interest within a given domain.
- HR[1] is a system that implements ATF.



[1] http://www.doc.ic.ac.uk/~sgc/hr/

Case study: The Mondex system

Abstract model | **Concrete model**



Mondex refinement step

TransferFail $\widehat{=}$
  any
    t
  where
    $t \in pending$
  then
    $recover := recover \cup \{t\}$
    $pending := pending \setminus \{t\}$
end

XOR

Abortepv$_1$ $\widehat{=}$
  any
    t
  where
    $t \in epv$
    $t \in abortepa$
  then
    $abortepv := abortepv \cup \{t\}$
    $epv := epv \setminus \{t\}$
end

Abortepa$_1$ $\widehat{=}$
  any
    t
  where
    $t \in epa$
    $t \in abortepv$
  then
    $abortepa := abortepa \cup \{t\}$
    $epa := epa \setminus \{t\}$
end

Abortepv1 GRD PO:
$t \in epv$
$t \in abortepa$
$\stackrel{?}{\vdash}$
$t \in pending$

Abortepa1 GRD PO:
$t \in epa$
$t \in abortepv$
$\stackrel{?}{\vdash}$
$t \in pending$

Missing invariants:
$\mathbf{epv \cap (epa \cup abortepa) \subseteq pending}$
$\mathbf{epa \cap (epv \cup abortepv) \subseteq pending}$

Mondex animation trace - 100 steps

	Variables				
State	**pending**	**epa**	**epv**	**abortepa**	**abortepv**
s00	-	-	-	-	-
s01	-	-	-	-	-
:	:	:	:	:	:
s20	t5	t5	t5,t9	-	-
s21	t5	t5	t5,t9	-	-
s22	t5	t5	t5,t9	-	-
s33	t9	t9	t4,t7,t9	-	t6
s34	t9	t9	t4,t7	-	t6, t9
s35	t9	t9	t3,t4,t7	-	t6, t9
s36	t9	t9	t3,t4	-	t6, t7, t9
s47	t10	t10	t10	-	t1, t3, t4, t6, t7
s48	t10	t10	t10	-	t1, t3, t4, t6, t7
s49	t10	-	t10	t10	t1, t3, t4, t6, t7
s50	t10	-	t10	t10	t1, t3, t4, t6, t7
s51	t10	-	t8, t10	t10	t1, t3, t4, t6, t7
s52	t3,t10	t3	t8, t10	t10	t1, t3, t4, t6, t7
:	:	:	:	:	:

HR core concepts for the mondex system

For each state, we supply HR with the concepts of pending, epa, epv, abortepa and abortepv.

state(A)
s00
s01
:
s20
s21
s22
s33
s34
s35
s36
s47
s48
s49
s50
s51
s52
:

pending(A,B)	
s00	-
s01	-
:	:
s20	t5
s21	t5
s22	t5
s33	t9
s34	t9
s35	t9
s36	t9
s47	t10
s48	t10
s49	t10
s50	t10
s51	t10
s52	t3
s52	t10
:	:

epa(A,B)	
s00	-
s01	-
:	:
s20	t5
s21	t5
s22	t5
s33	t9
s34	t9
s35	t9
s36	t9
s47	t10
s48	t10
s49	-
s50	-
s51	-
s52	t3
:	:

abortepa(A,B)	
s00	-
s01	-
:	:
s20	-
s21	-
s22	-
s33	-
s34	-
s35	-
s36	-
s47	-
s48	-
s49	t10
s50	t10
s51	t10
s52	t10
:	:

epv(A,B)	
s00	-
s01	-
:	:
s20	t5
s20	t9
s21	t5
s21	t9
s22	t5
s22	t9
s33	t4
s33	t7
s33	t9
s34	t4
s34	t7
s35	t3
s35	t4
s35	t7
s36	t3
s36	t4
s47	t10
s48	t10
s49	t10
s50	t10
s51	t8
s51	t10
s52	t8
s52	t10
:	:

abortepv(A,B)	
s00	-
s01	-
:	:
s20	-
s21	-
s22	-
s33	t6
s34	t6
s34	t9
s35	t6
s35	t9
s36	t6
s36	t7
s36	t9
s47	t1
s47	t3
s47	t4
s47	t6
s47	t7
s48	t1
s48	t3
s48	t4
s48	t6
s48	t7
s49	t1
s49	t3
s49	t4
:	:

Disjunct production rule

epa(A,B)	
s00	-
s01	-
:	:
s20	t5
s21	t5
s22	t5
s33	t9
s34	t9
s35	t9
s36	t9
s47	t10
s48	t10
s49	-
s50	-
s51	-
s52	t3
:	:

abortepa(A,B)	
s00	-
s01	-
:	:
s20	-
s21	-
s22	-
s33	-
s34	-
s35	-
s36	-
s47	-
s48	-
s49	t10
s50	t10
s51	t10
s52	t10
:	:

$\xrightarrow{disjunct<>}$

epa $\vee$ abortepa	
s00	-
s01	-
:	:
s20	t5
s21	t5
s22	t5
s33	t9
s34	t9
s35	t9
s36	t9
s47	t10
s48	t10
s49	t10
s50	t10
s51	t10
s52	t3
s52	t10
:	

Compose production rule

epv(A,B)	
s00	-
s01	-
:	:
s20	t5
s20	t9
s21	t5
s21	t9
s22	t5
s22	t9
s33	t4
s33	t7
s33	t9
s34	t4
s34	t7
s35	t3
s35	t4
s35	t7
s36	t3
s36	t4
s47	t10
s48	t10
s49	t10
s50	t10
s51	t8
s51	t10
s52	t8
s52	t10
:	:

epa $\vee$ abortepa	
s00	-
s01	-
:	:
s20	t5
s21	t5
s22	t5
s33	t9
s34	t9
s35	t9
s36	t9
s47	t10
s48	t10
s49	t10
s50	t10
s51	t10
s52	t3
s52	t10
:	:

$\xrightarrow{\mathit{compose}<1,2>}$

epv $\wedge$ (epa $\vee$ abortepa)	
:	:
s20	t5
s21	t5
s22	t5
s33	t9
s47	t10
s48	t10
s49	t10
s50	t10
s51	t10
s52	t10
:	:

Implication conjecture

epv $\wedge$ (epa $\vee$ abortepa)	
:	:
s20	t5
s21	t5
s22	t5
s33	t9
s47	t10
s48	t10
s49	t10
s50	t10
s51	t10
s52	t10
:	:

$\Rightarrow$

pending(A,B)	
s00	-
s01	-
:	:
s20	t5
s21	t5
s22	t5
s33	t9
s34	t9
s35	t9
s36	t9
s47	t10
s48	t10
s49	t10
s50	t10
s51	t10
s52	t3
s52	t10
:	

$\forall$ A,B . state(A) $\wedge$ trans(A,B) $\wedge$ epv(A,B) $\wedge$ (epa(A,B) $\vee$ abortepa(A,B)) $\Rightarrow$ pending(A,B)

or,

Invariant: epv $\cap$ (epa $\cup$ abortepa) $\subseteq$ pending

Challenge

13697 conjectures were generated in 25 seconds by HR after 1000 theory formation steps for this refinement of the mondex case study.

How do we select the right invariants?

Guidance through proof failure analysis

- We use proof failure analysis to focus the search in HR.
- Proof failure analysis guides us to:
  - Select the appropriate production rules to be used by HR during the search.
  - Reduce the number of conjectures we are interested in.

This is achieved by using two classes of heuristics:

- *Pre-Heuristics (PH):* those used in configuring HR.
- *Selection Heuristics (SH):* those used in selecting conjectures from HR's output.

HR configuration heuristics

PH1. *Prioritise core and non-core concepts that occur within the failed POs.*

PH2. *Select production rules which will give rise to conjectures relating to the concepts occurring within the failed POs*

e.g. *arithmetic pr is selected if the arithmetic operators, i.e.* $+$,-,*,$/$, *occur*.

PH3. *Generate conjectures that fit the shape of the expected invariants.*

Application of the pre-heuristics to the Mondex case study:

$\mathbf{PO_1}$:	$\mathbf{PO_2}$:
t $\in$ epv	t $\in$ epa
t $\in$ abortepa	t $\in$ abortepv
$\vdash$	$\vdash$
t $\in$ pending	t $\in$ pending

PH1: pending, epv, abortepa, epa, abortepv, *others...*
PH2. compose, disjunct and negate production rules.
PH3. implication conjectures.

Conjecture selection heuristics

SH1. *Select conjectures that focus purely on prioritised core and non-core concepts.*

SH2. *Select conjectures where the sets of variables occurring on the left- and right-hand sides are disjoint.*

SH3. *Select only the more general conjectures.*

SH4. *Select conjectures that discharge the failed POs.*

SH5. *Select conjectures that minimise the number of additional proof failures that are introduced.*

Conjecture selection heuristics applied

Results of the application of the selection-heuristics to the concept of *pending*:

Heuristic	**Implication conjectures**
SH1	30
SH2	30
SH3	9
SH4	5
SH5	**2**

Obtained conjectures:

$$\forall\ A,B\ .\ state(A) \land trans(A,B) \land epv(A,B) \land (epa(A,B) \lor abortepa(A,B)) \Rightarrow pending(A,B)$$
$$\forall\ A,B\ .\ state(A) \land trans(A,B) \land epa(A,B) \land (epv(A,B) \lor abortepv(A,B)) \Rightarrow pending(A,B)$$

in other words,

Invariant 1: epv $\cap$ (epa $\cup$ abortepa) $\subseteq$ pending
Invariant 2: epa $\cap$ (epv $\cup$ abortepv) $\subseteq$ pending

Results so far

Event-B model	Step	Failed POs	Invariants			
			Automatically discovered			
			Glue	System	Total	Iteration
Traffic light	Level 1-2	2	2	0	**2**	1
Vending machine (arith)	Level 1-2	6	3	0	**3**	1
Vending machine (sets)	Level 1-2	6	3	0	**3**	1
Cars on a bridge	Level 1-2	2	1	0	**1**	1
	Level 2-3	6	0	5	**5**	1
	Level 3-4	7	0	5	**5**	1
Mondex	Level 3-4	5	4	0	**4**	1
		6	1	4	**5**	2
		1	0	1	**1**	3
	Level 4-5	3	0	3	**3**	1
		5	0	4	**4**	2
		4	0	2	**2**	3
	Level 8-9	14	10	0	**10**	1

Automatically discovered invariants

$$\begin{aligned}
&\mathrm{available} = \mathrm{productStatus}^{-1}[\{\mathrm{AVAILABLE}\}]\\
&\mathrm{limited} = \mathrm{productStatus}^{-1}[\{\mathrm{LIMITED}\}]\\
&\mathrm{soldOut} = \mathrm{productStatus}^{-1}[\{\mathrm{SOLDOUT}\}]
\end{aligned}$$

Vending machine (sets)

$$\begin{aligned}
&\mathrm{stock} = \mathrm{stockMilk} + \mathrm{stockPlain}\\
&\mathrm{sold} = \mathrm{soldMilk} + \mathrm{soldPlain}\\
&\mathrm{givenCoin} = \mathrm{EMPTY_COIN} \Leftrightarrow \mathrm{coin} = \mathrm{NO_COIN}
\end{aligned}$$

Vending machine (arith)

$$\begin{aligned}
&\mathrm{n} = \mathrm{a} + \mathrm{b} + \mathrm{c}\\
&\mathrm{ml_tl} = \mathrm{green} \Rightarrow \mathrm{c} = 0\\
&\mathrm{il_tl} = \mathrm{green} \Rightarrow \mathrm{a} = 0\\
&\mathrm{ml_tl} = \mathrm{red} \Rightarrow \mathrm{ml_pass} = 1\\
&\mathrm{il_tl} = \mathrm{red} \Rightarrow \mathrm{il_pass} = 1\\
&\mathrm{il_tl} = \mathrm{green} \Rightarrow \mathrm{ml_tl} = \mathrm{red}\\
&\mathrm{ml_out_10} = \mathrm{TRUE} \Rightarrow \mathrm{ml_tl} = \mathrm{green}\\
&\mathrm{il_out_10} = \mathrm{TRUE} \Rightarrow \mathrm{il_tl} = \mathrm{green}\\
&\mathrm{IL_IN_SR} = \mathrm{on} \Rightarrow \mathrm{A} > 0\\
&\mathrm{IL_OUT_SR} = \mathrm{on} \Rightarrow \mathrm{B} > 0\\
&\mathrm{ML_IN_SR} = \mathrm{on} \Rightarrow \mathrm{C} > 0
\end{aligned}$$

Cars on a bridge

$$\begin{aligned}
&\mathrm{epr} \cap \mathrm{reqM} \subseteq \mathrm{epv} \cup \mathrm{abortepv}\\
&\mathrm{epv} \cap \mathrm{valM} \subseteq \mathrm{epa} \cup \mathrm{abortepa}\\
&\mathrm{endT} = \mathrm{endF} \cup \mathrm{ackM}\\
&\mathrm{reqM} \cap \mathrm{idleF} \subseteq \mathrm{epv} \cup \mathrm{abortepv}\\
&\mathrm{valM} \cap \mathrm{idleT} = \varnothing\\
&\mathrm{epr} \cap \mathrm{valM} = \varnothing\\
&\mathrm{epr} \cap \mathrm{abortepa} = \varnothing\\
&\mathrm{valM} \cap \mathrm{idleF} = \varnothing\\
&\mathrm{abortepa} \cap \mathrm{idleF} = \varnothing
\end{aligned}$$

Mondex (ref 4)

$$\begin{aligned}
&\mathrm{idleFP} = \mathrm{statusF}^{-1}[\{\mathrm{IDLEF}\}]\\
&\mathrm{eprP} = \mathrm{statusF}^{-1}[\{\mathrm{EPR}\}]\\
&\mathrm{epaP} = \mathrm{statusF}^{-1}[\{\mathrm{EPA}\}]\\
&\mathrm{aborteprP} = \mathrm{statusF}^{-1}[\{\mathrm{ABORTEPR}\}]\\
&\mathrm{abortepaP} = \mathrm{statusF}^{-1}[\{\mathrm{ABORTEPA}\}]\\
&\mathrm{endFP} = \mathrm{statusF}^{-1}[\{\mathrm{ENDF}\}]\\
&\mathrm{idleTP} = \mathrm{statusF}^{-1}[\{\mathrm{IDLET}\}]\\
&\mathrm{epvP} = \mathrm{statusF}^{-1}[\{\mathrm{EPV}\}]\\
&\mathrm{abortepvP} = \mathrm{statusF}^{-1}[\{\mathrm{ABORTEPV}\}]\\
&\mathrm{endTP} = \mathrm{statusF}^{-1}[\{\mathrm{ENDT}\}]
\end{aligned}$$

Mondex (ref 8)

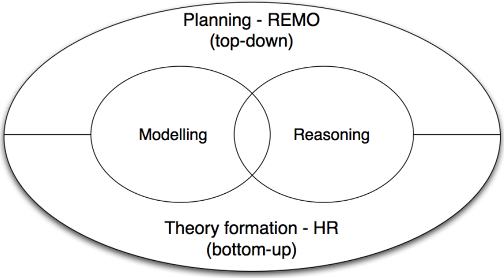
$$\begin{aligned}
&\mathrm{r_light} = \mathrm{TRUE} \vee \mathrm{amber_light} = \mathrm{TRUE} \Leftrightarrow \mathrm{red_light} = \mathrm{TRUE}\\
&\mathrm{g_light} = \mathrm{TRUE} \Leftrightarrow \mathrm{green_light} = \mathrm{TRUE}
\end{aligned}$$

Traffic light

Summary

- We have applied ATF to reason about Event-B models.
- We have performed a series of experiments to automatically discover invariants of various Event-B models through the HR system.
- The key contribution of our approach is the development of the set of heuristics that use proof failure analysis.

Current work



- Bottom-up ATF assumes correct models, we want to use top-down planning to support ATF when incorrect models appear.
- Top-down planning is limited by the patterns observed, bottom-up ATF supports planning when an invariant template is not available in a pattern.
- Currently we are developing refinement plans within our existing REMO system.

		Horizontal refinement				Vertical refinement					
Model	**Refinement**	**Cases**	**Sequence**		**Control Ellab.**	**Part2Fun**	**Set2Part**	**Data Extension**	**Data Rename**	**Data Removal**	**HR**
			Acum	**Plain**							
Cars on a bridge	Ref 1						✔				✔
	Ref 2	✔✔	✔✔								✔
	Ref 3			✔							✔
Mondex	Ref 1			✔					✔		
	Ref 2									✔	
	Ref 3	✔		✔✔							✔
	Ref 4			✔							✔
	Ref 5				✔						
	Ref 6							✔	✔		
	Ref 7									✔	
	Ref 8					✔					✔
Flash file system	Ref 1						✔				
	Ref 2				✔						
	Ref 3				✔						
	Ref 4				✔						
	Ref 5		✔								
	Ref 6		✔								
Location access controller	Ref 1				✔						
	Ref 2			✔							
	Ref 3						✔				
	Ref 4						✔✔				
plc	Ref 1										
	Ref 2			✔							
	Ref 3						✔				
	Ref 4						✔				
	Ref 5					✔					
Network topology discovery	Ref 1										
	Ref 2			✔							
	Ref 3							✔			
	Ref 4										
	Ref 5									✔	
	Ref 6				✔						
	Ref 7							✔		✔	