#### ProB: A Model Checker for B

Michael Leuschel and Michael Butler

Department of Electronics and Computer Science University of Southampton Highfield, Southampton, SO17 1BJ, UK

#### Abstract -- Summary

• Animator and model checker for B Methode

- Model & constrained based checker
- ProB findes correct values for operation arguments
- ProB enables user to uncover errors in specifications

#### B Methode

- Theory and methodology for formal development
- Based on abstract machine with refinement
  - Generalized machine
  - Machine refines max. one machine
- Set theoretic constructs
  - Sets, relations functions
  - Basic types (integer, ...)
- Invariants
  - Hold on every variable value chance
  - Predicate logic

# Pro B - Proofing

- Proofing
  - Consistency checking
    - Operation preserves Invariants
    - Model checking (this tool @ this paper)
  - Refinement checking
    - valid refinement of machine
  - Exhaustive model checking
    - Only small finite sets
    - Integer limited to small numeric ranges
    - Traverse all reachable states

# Pro B - Checking

- Interactive Proof
   Automatic and manual
- State reach ability
- Invariant violation
  - From the initial state
    - $\rightarrow$  model Checker
  - State before violation
    - $\rightarrow$  constraint based checker

MACHINE Lift VARIABLES floor INVARIANT floor: 0..99 INITIALISATION floor := 4 OPERATIONS inc = PRE floor<99 THEN floor := floor + 1 END ; dec = BEGIN floor := floor - 1 END END Fig. 1. Lift example in B



Fig. 2. Counter-examples for the Lift Machine

#### B (AMN) -> Jbtool -> XML -> Pillow -> Prolog



#### Pro B Kernel

- Statements
  - Modify variables
- Expressions
  - Return value

B Type	B value	Prolog encoding
number	5	int(5)
boolean	true	term(true)
element of a finite set $S$	C	fd(3,'S')
pair	(2,5)	(int(2),int(5))
sequence	[2, 5]	<pre>cons(int(2),cons(int(5),nil))</pre>
$\operatorname{set}$	$\{2, 5\}$	[int(2), int(5)]

- No variable modification
- Boolen expressions
  - Return TRUE or FALSE
  - predicates

#### **Pro B Animator**

- Back trace able step by step animation
- Support non deterministic operations
- Symbolic & ordinary animation
- Value initialization
- Visualization

ACHINE car_alarm_machine ETS /* onumorated */ car_alarm_statemachine_STATES=(OpenAndUnlo sm_alarmhandling_nested_STATES=(DeckFin_nes sm_inhandling_nested_STATES=(DeckFin_nes	scked, ClosedAndUnlocked, OpenAndLocked, ClosedAndLoc ound, Flash, sm_alarmhandling_nested_NULL); who, checkfoldPin, sm_inhandling_nested_NULL);	ked, Armed, SiltendAndOpen, AlarmHandling, Pir	Handling, DoorHandling);	
ONCRETE CONSTANTS				
time_for_action				
BSTRACT_VARIABLES	B <sup>*</sup> Analysing Coverage			
actual_time,		Coverage for transitions:		
car_alarm_statemachine,	Tenters	14		
car_scate_ataim,	Invariant violatedia	-		
car state closed.	openi72			
car state locked.	invariant_not_checked:72			
car state open,	liver58 deadlocked:1			
car state unlocked,	total:131			
sm_alarmhandling_nested,	TOTAL_EVENTS			
sm_pinhandling_nested,	193 CONFRED FUENTS			
wrong_pin_count	Satup constants:1			
· PROMOTED OPERATIONS	finitialize_methine(1			
close_open,	willock_srmed:1			
open_unlocked, Enter navinum re p	if operations: close_silent(1			
unlock open	unlock_silents1			
open locked,	Center armed: 4			
close locked,	and a state and a	Peter .		
unlock closed,		and a second sec		
lock_closed,	Save	Done		
wait_20,				
uploak smaa				
				Un 17, OB 22
State Properties	Enabled Operators	•	j. Hittiry	10 17, 09 22
El State Properties artant JA e for action = 1	Enabled Operators	◆ →	ے۔ Hetary coefied_cheduidon	UN 17, ON 22
<ul> <li>State Properties statut_plic</li> <li>for justom + 1 sub_tom - 200</li> </ul>	Enabled Operators	All recognition		54 27, OR 22
El State Propertes aran (, 4 fe, yctor = 1 dar, pres = 200 dar, press den a Alamandring	finabled Operations	▲ → Service service restrict	Konstandor Hellery 	IN 17, OR 22
Sate Proverties     July	Ended Operators	Eleveragen sentege handrege		IN 17, OR 22
State Properties           State Properties           State Anno 1           State States 1           State States - Assessed by State States - FAIS           State States - FAIS           State States - FAIS	Endine Operators	Le 🖢	Hintery Kostelat_chestaktion foesuriected peestanduriected mpeerindedid en	UN 17, GH 22
Status Provedse           Status Provedse           V, M, Korn 1           Land Prove 200           Jahr J, Honsek M, Kallenderg           Jahr J, Honsek M, Kallenderg <td< td=""><td>Ended Convolution</td><td>the second second</td><td>History - Martiney - Martine</td><td>UN 17, ON 22</td></td<>	Ended Convolution	the second	History - Martiney - Martine	UN 17, ON 22
Stark Treaming           C Stark Treaming           C Stark Treaming           Stark Treaming           Stark Stark Treaming	Index Occurres	televen sorozan sorozo soro sor	Jeden States Andrew States Andrew States Jeser States Jeser States	UN 17, CM 22
Sea Anguesta morta di Jacobierto	Edd Gardon	<ul> <li>Improve International</li></ul>	Hear - He	UN 17, OR 22
Statu Investments     Social and a status     Soc	Entre Greation	tet Branne Branne Briten Briten C_ann Bra	Jeden States Anternet	UN 17, ON 22
State Angestes     more de     more d	Ended Garantee	Entropy Entropy British Britis		(A 17, 08 22
The State Answerse The State Answerse State of the State of the State of the State State of the State State State of the State	Ended Question	te ∎ terrete terre	Henry Henry 	UN 17, ON 22
E dash hearins E dash hearins (2000) (	E baiel Gacatere	Enormal Enormal Hereitan Herei	Hotey Hotey Market	Un 17, ON 22
Statutheartis mode Statutheartis mode Statute	Totald Gausties	Encorange Encorange Interfect Interf	Hotory 	Un 17, ON 22
Beach Aspects     To Jack Processing State     Jack Processing     Jack Processin	Ender Operation	Comparing a second	Anter	Un 17, ON 22
Seath Angel Index     Seath Teaching Control of Seath Teaching Co	indiad Greaters		January Haray	UN 17, ON 22
Stein Ansertes     mortuna     Security	Todad Garanters	E Constant International Internati	in a second seco	Un 17, ON 22
IS Subschweise Softwart (Sterring Sterring) Softwart (Sterring Sterring S	E baix Guenne	Engrand     E	I Harry Harr	Un 17, UN 22

Screenshot from ProB Classic

## Pro B Consistency Checking

- Temporal Model Checking
  - Normalization Strategy for states (reduce multiple state checking)
  - Adapted A\* (depth or bread first)
  - Store already checked states in datebase

```
MACHINE counter
VARIABLES n
INVARIANT n : 0..10 & n /= 2
INITIALISATION n := 3
OPERATIONS
inc = PRE n<10 THEN n := n + 1 END
END
```

Fig. 5. A simple counter machine with an error

# Pro B Consistency Checking

- Constraint Based Checking
  - Assert invariant is valid
  - Assert invariant is not valid
    - Execute until only suspended Goals
    - Expand goals
    - Invert
    - Constraint check

constraint\_check(OpName,State,Operation,NewState) :-

- b\_extract\_types\_and\_invariant(Variables,VarTypes,Invariant),
- b\_set\_up\_variable\_types(Variables,VarTypes,State),
- b\_set\_up\_variable\_types(Variables,VarTypes,NewState),

b\_test\_boolean\_expression(Invariant,[],State),

- b\_not\_test\_boolean\_expression(Invariant,[],NewState),
- b\_execute\_operation(OpName,Operation,State,NewState,\_Abort).

Slide #10

#### **Case Studies**

- Volvo vehicle function
  - 15 Variables
  - 550 LOC (AMN)
  - 26 Operations
  - $\rightarrow$  few minutes calculation (1 Ghz G4 Powerbook)
  - $\rightarrow$  1360 states
  - $\rightarrow$  25696 transitions
  - $\rightarrow$ Invariant checking
  - $\rightarrow$  Deadlock checking

#### <u>Modelling and Proof of a</u> <u>Tree-structured File</u>

#### System in Event-B and Rodin

Kriangsak Damchoom 1, Michael Butler 1 and Jean-Raymond Abrial 2

> 1 University of Southampton United Kingdom 2 ETH Zurich Switzerland

#### Literature

- M. Leuschel and M. Butler, "ProB: A model checker for B," in *FME 2003: Formal Methods*, Springer, 2003, pp. 855–874.
- [2] K. Damchoom, M. Butler, and J.-R. Abrial, "Modelling and proof of a tree-structured file system in Event-B and Rodin," in *Formal Methods and Software Engineering*, Springer, 2008, pp. 25–44.
- [3] K. Robinson, "A Concise Summary of the Event B mathematical toolkit." 2010.