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
    → model Checker
  - State before violation
    → 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

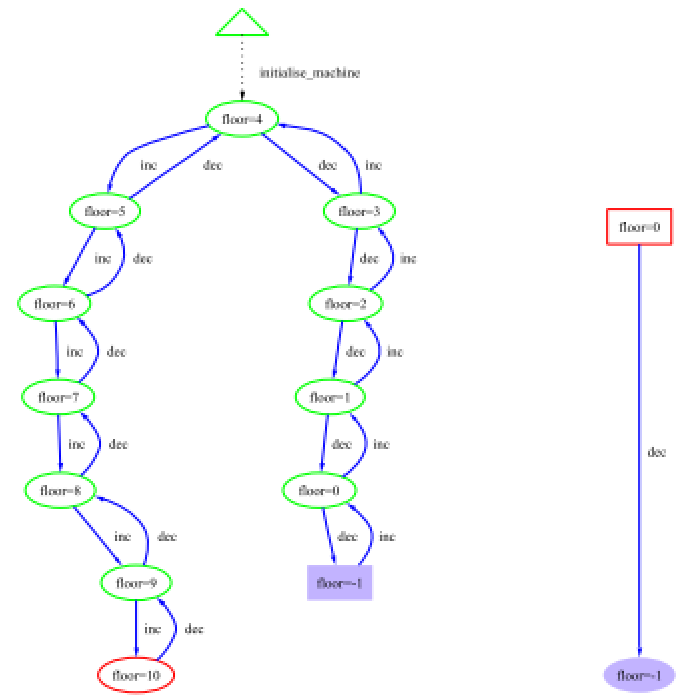


Fig. 2. Counter-examples for the Lift Machine

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

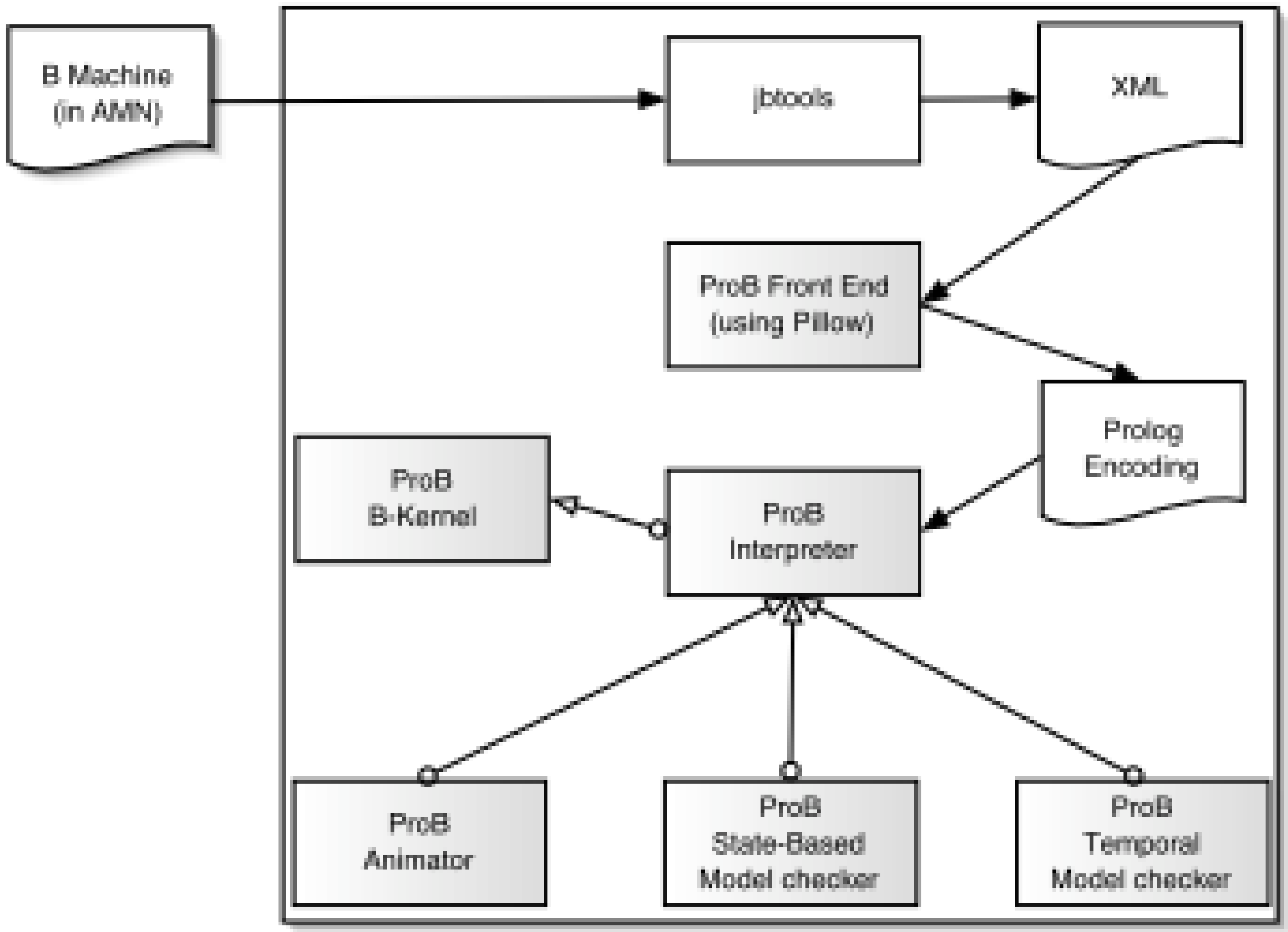


Fig. 3. Overview of the ProB System

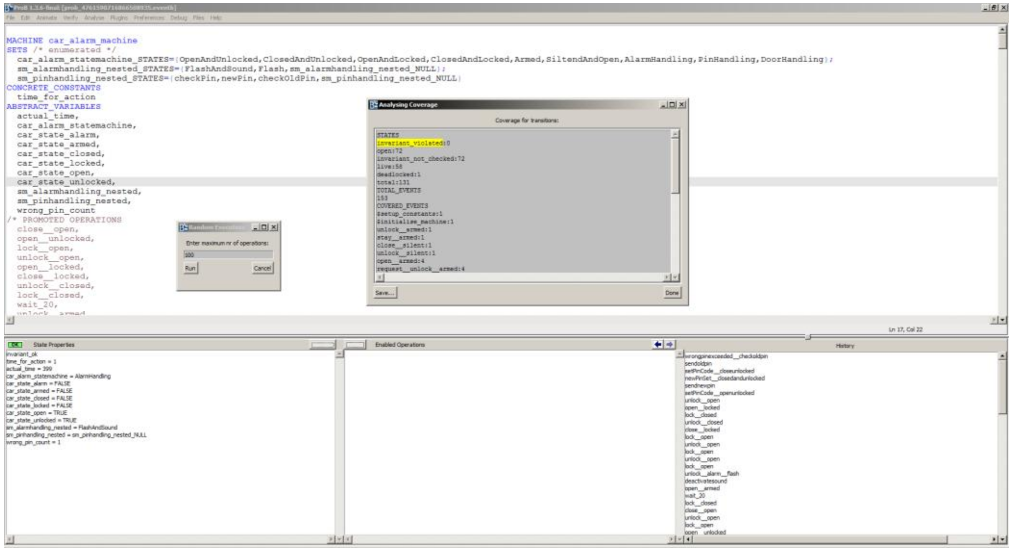
Pro B Kernel

- Statements
  - Modify variables
- Expressions
  - Return value
  - No variable modification
- Boolen expressions
  - Return TRUE or FALSE
  - predicates

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	$[2, 5]$	`cons(int(2),cons(int(5),nil))`
set	$\{2, 5\}$	`[int(2), int(5)]`

Pro B Animator

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



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).
```

Case Studies

- Volvo vehicle function
  - 15 Variables
  - 550 LOC (AMN)
  - 26 Operations

→few minutes calculation (1 Ghz G4 Powerbook)

→1360 states

→25696 transitions

→Invariant checking

→Deadlock checking

Modelling and Proof of a Tree-structured File 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

[1] 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.