An Extended Static Checker for Modula-3

K. Rustan M. Leino
Greg Nelson
DIGITAL, SRC

Joint work with Dave Detlefs & Jim Saxe

3 April 1998
Compiler Construction, ETAPS’98
Lisbon, Portugal
Testing vs. Verification

- Testing has proven more cost-effective than formal verification
- Many errors are not found by testing
- Those that are, are found late
- Test cases vs. specifications
Extended Static Checking

- Statically detect certain common run-time errors
- Use formal methods — for limited checking
What ESC/Modula-3 does

Annotated Modula-3 program → ESC/Modula-3 → "NIL dereference error on line 218"

Checks for:
- NIL-dereference errors
- array bounds errors
- NARROW faults
- race conditions
- deadlocks
- ...
How ESC/Modula-3 works

Annotated Modula-3

Modula-3-to-V.C. compiler

Verification condition (logical formula)

Theorem prover

Error message
Main Research Contributions

• Fast automatic theorem prover
• Theory of dependencies
  - generalized data abstraction
INTERFACE TextWr;

TYPE T <: ROOT;

<*> SPEC VAR valid: MAP T TO BOOLEAN *>  
<*> SPEC VAR state: MAP T TO ANY *>  

PROCEDURE Init(t: T);  
<*> SPEC Init(t)  
   MODIFIES valid[t], state[t]  
   ENSURES valid'[t] *>  
(* Initialize the text writer "t". *)
PROCEDURE PutInt(t: T; i: INTEGER);
<* SPEC PutInt(t, i)
   MODIFIES state[t]
   REQUIRES valid[t] *>  
(* Write the ASCII version of "i" to "t". *)

PROCEDURE GetText(t: T): TEXT;
<* SPEC GetText(t)
   MODIFIES state[t]
   REQUIRES valid[t] *>  
(* Return the text that has been written to "t". *)

PROCEDURE Close(t: T);
<* SPEC Close(t)
   MODIFIES valid[t], state[t] *>  
(* Destroy "t", reclaiming its internal buffers. *)

END TextWr.
IMPORT TextWr;

PROCEDURE ArrayToText(a: ARRAY OF INTEGER): TEXT =
    VAR twr := NEW(TextWr.T);
    BEGIN
        FOR i := 1 TO NUMBER(a) DO
            TextWr.PutInt(twr, a[i])
        END;
        RETURN TextWr.GetText(twr)
    END;
END ArrayToText;
Conclusions

- finds error that testing would find late, or not at all
- simple, idiomatic annotations
- fully automated
- acceptable performance

AltaVista query: extended static checking