PROJECT
"COUVERTURE"

Innovative MC/DC measurement method

PLDI 2009
SRC
Dublin, June 15

PROJECT KEYWORDS

- **Open Source** Free Software
- **Multiple languages**
- Academic & Industry
- **Non-intrusive** code coverage
- **MC/DC** measure
- Critical software development
- Civil avionics norms (DO-178B) [4]

MC/DC [3]

Modified **C**ondition/**D**ecision **C**overage

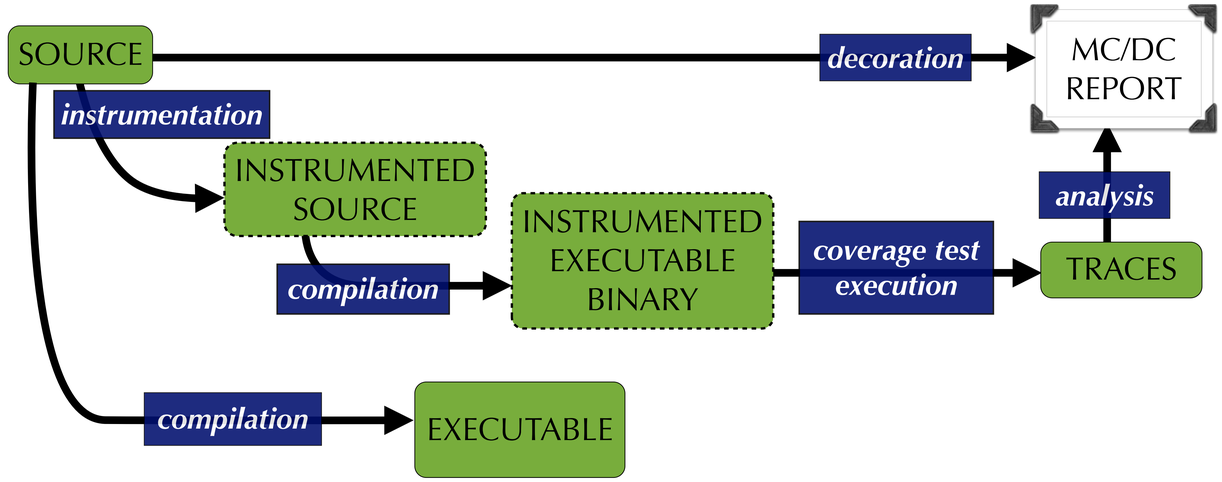
- **Condition:** *expr* ⇝T or F
- **Decision:** chosen path after condition evaluation
- Decision should depend on every condition (condition independency)
- **Detect useless code**
- **Minimize** number of tests
- Needed by certification authorities such as civil avionics, railway, etc
- Language independent

MC/DC MEASURE EXAMPLE

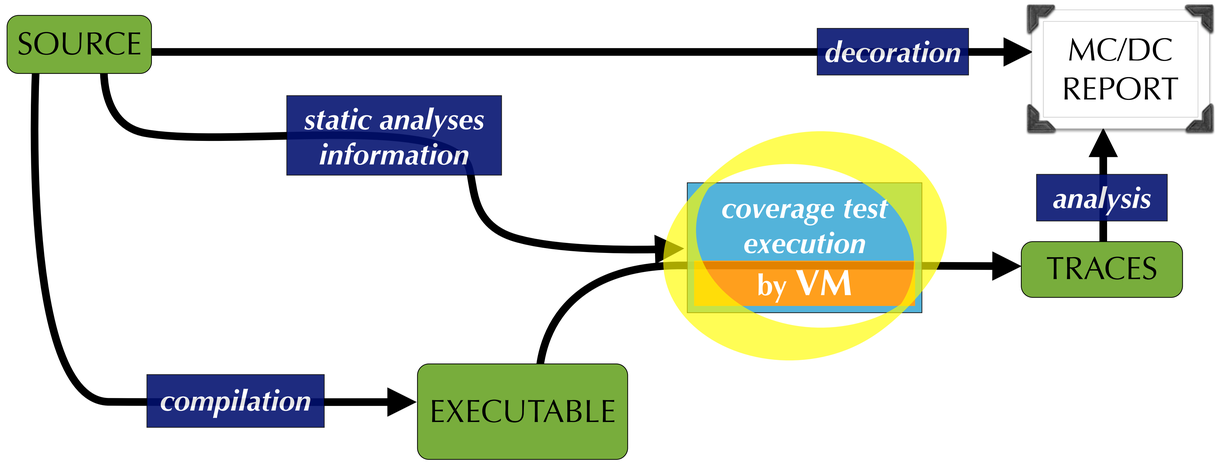
```
let all_positive1 a b c =
  (a > 0) && (b > 0) && (c > 0) ;;

  (* all_positive1 1 1 1 ;; *)
  (* all_positive1 1 1 0 ;; *)

let all_positive2 a b c =
  (a > 0) && (b > 0) && (c > 0) ;;

  (* all_positive2 1 1 1 ;; *)
  (* all_positive2 1 0 1 ;; *)
  (* all_positive2 1 1 0 ;; *)
let all_positive3 a b c =
  (a > 0) && (b > 0) && (c > 0) ;;

  (* all_positive3 1 1 1 ;; *)
  (* all_positive3 0 1 1 ;; *)
  (* all_positive3 1 0 1 ;; *)
  (* all_positive3 1 1 0 ;; *)
```


Philippe Wang
PhD Student, advisor: Emmanuel Chailloux
Université Pierre et Marie Curie
Laboratoire d'Informatique de Paris 6
CNRS UMR 7606
http://www-apr.lip6.fr/~pwang/

Usual method: Source Instrumentation



Innovative method: Instrumenting Virtual Machine



Particularities

- **Same** binary for testing & production (easier DO qualification process)
- As complete as source instrumentation (e.g. MLcov [2] for Caml)

Use of a Virtual Machine

- **No need for hardware for testing** (earlier testing)
- No need for specialized hardware for traces extraction

upmc.fr cnrs.fr lip6.fr

COUVERTURE
La certification libre
projet-couverture.com

CLASSIC APPROACH

- Instrumentation: compile source code with additional instructions
- Execute instrumented (fatter) binary
- Traces produced by binary itself
- Analyze traces
- Generate report

MY APPROACH PARTICULARITIES

- **High level & Higher order language**
- Caml language, **Caml bytecode** [5]
- **Modified Caml VM** (in Caml)
- Control Flow Analysis
- Use of types information
- Traces produced by Virtual Machine (change of execution environment)
- Need more pre-execution information

REFERENCES

1. B. Pagano *et al.*, *Certified development tools implementation in Objective Caml*. PADL, LNCS(4902) (Jan 2008)
2. MLcov tool (by Esterel Technologies) www.esterel-technologies.com/technology/free-software/
3. K.J. Hayhurst *et al.*, *A Practical Tutorial on Modified Condition/Decision Coverage*. Tech report, NASA/TM-2001-210876 (May 2001)
4. RTCA/DO-178B. *Software Considerations in Airborne Systems and Equipment Certification*. Radio Technical Commission for Aeronautics (Dec 1992)
5. X. Leroy *et al.*, *The Objective Caml system release 3.11: Documentation and user's manual, 2008*.

PARTNERS: ADA for PPC (QEMU)

AdaCore The GNAT Pro Company — adacore.com
TELECOM ParisTech — telecom-paristech.fr
Open Wide Architecte Open Source — openwide.fr