Property Qualification

Graziano Pravadelli
Dipartimento di Informatica Università di Verona

Agenda

- Property qualification
  - Incompleteness analysis
  - Vacuity analysis
  - Over specification analysis

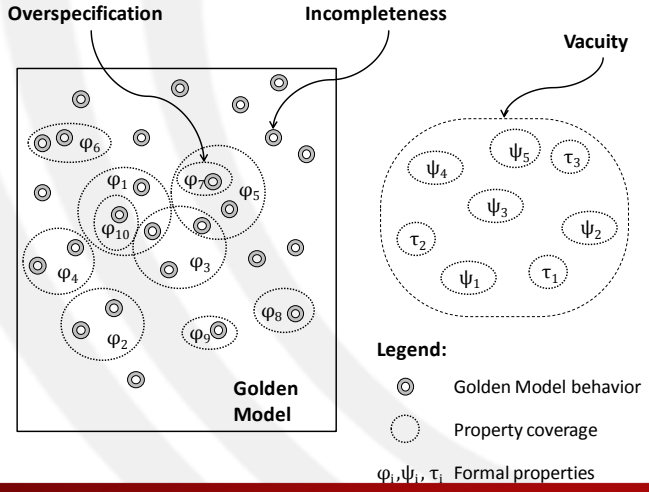
Property qualification

- Same idea as for *testbench qualification*
- *Property qualification* aims at evaluating the quality of properties
  - If a design satisfy a set of properties can we say that the design is correct?
- Testbench qualification + Property qualification = *Functional qualification*

Property qualification

- Are properties enough?
  - Incompleteness analysis
    - To measure how good is the set of properties in discovering bugs
      - The implementation could be wrong even if it satisfies all the properties
- Are properties vacuously satisfied?
  - Vacuity analysis
    - To identify useless properties and tautologies
      - Properties trivially satisfied lead to a false sense of safety
- Are properties over specified?
  - Over specification analysis
    - To compact the set of properties
      - Properties can be derived as logical consequence of other properties

Property qualification



Property qualification

- Current approaches present limitations
  - Property incompleteness
    - Unable to identify missing properties
  - Vacuity analysis
    - Unable to identify all possible cases of vacuity
  - Over specification analysis
    - Based on theorem proving
- The majority of approaches are based on formal methods

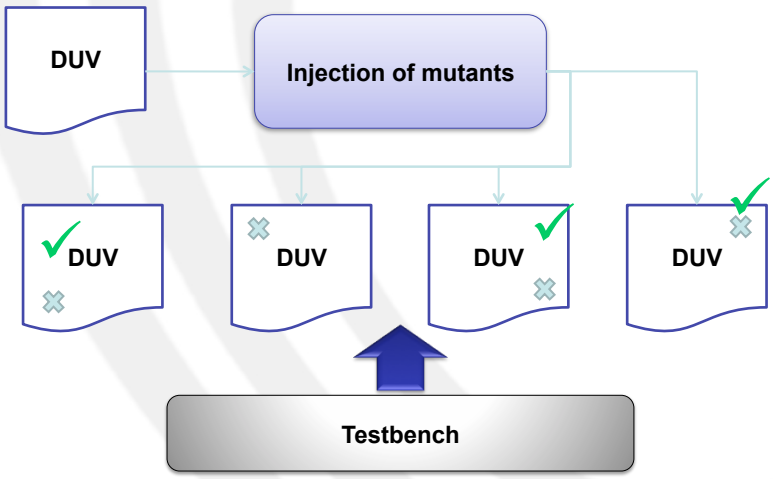
Property qualification

- Our approach is based on
  - mutation analysis and
  - mutation testing

Mutation analysis

- Mutation analysis is
  - a field of computer science involving the mutation of source code by introducing statements or modifying existing statements in small ways
  - the process of measuring how good a test set is
- The mutations are based on well-defined *mutation operators (mutants)* that simulate the presence of design errors (bugs)

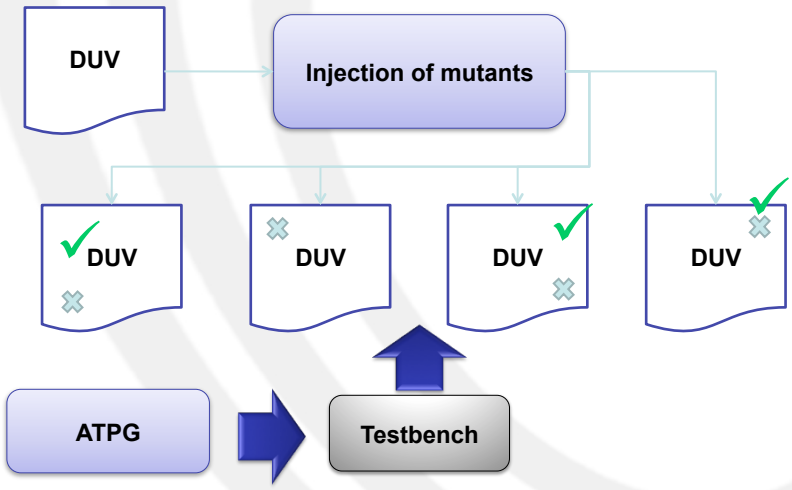
Mutation analysis



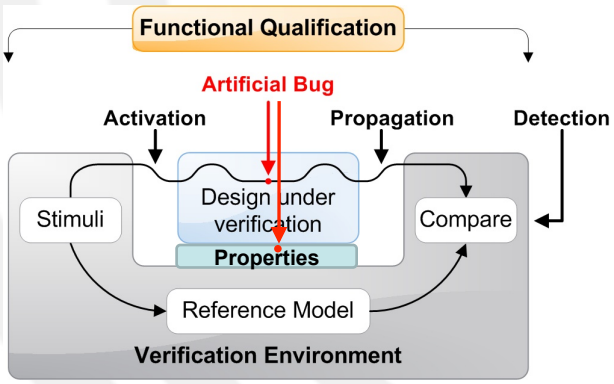
Mutation testing

- Mutation testing is
  - the process of generating tests to improve the mutation analysis score
  - is a broader topic than mutation analysis

Mutation testing



MA-based functional qualification environment



Goal

- New methodology for property qualification
  - Homogeneous
  - Comprehensive
  - Not based on formal techniques
  - Effective as current formal approaches
  - More efficient
- Based on
  - Mutation analysis (dynamic verification)

Property qualification by MA overview