Environment Models
Decomposition

Ilia Zakharov
Ilja.zakharov@ispras.ru
Ivannikov Institute For System Programming of RAS
Motivation
Thorough Verification of a Kernel Module

- Manually designed environment model
  - High verification code coverage
  - Carefully initialized data structures to avoid undefined values
- Functional requirements checking
  - pre- and post- conditions
  - Separated specific sequences of callback calls
  - Different setups of an environment model
    - Enabled or forbidden function models failing
    - Different sets of values for input data structures
Environment Model Generator

Configuration -> Specifications -> Build Base

EMG

Intermediate Environment Model

Translator

Environment Model
Intermediate Environment Model
Problems

- Too many options: it obscures the analysis
- Too long time needed to reach “deep code”
- Any revealed error prevents analysis of other paths
- Some environment model setups are incompatible
- Error traces are overloaded
Method
Environment Model Generator with Decomposer
Decomposition

**Process Decomposition:**
Separate *processes* into *scenarios*

**Scenario Selection:**
Combine new models by replacing original processes with newly generated scenarios
Example of Process Decomposition
Process Decomposition

Process A

- !(a)
  - <b>
    - [d]
    - <c>
  - (d)
    - <x>
      - <y>
      - <z>

Process B

Scenario A.1

- !(a)
  - <b>
    - <c>
  - [d]

Scenario A.2

- !(a)
  - <b>
    - [d]
  - (d)

Scenario B.1

- !(d)
  - <x>
    - <y>

Scenario B.2

- !(d)
  - <x>
    - <y>
Impact

- Less timeout results
- Easy development of environment models
- No more stucking after the first found error
Example with Savepoint
Model with Savepoint
Impact

- Less timeout results
- Reduce the number of environment models
- Different setups of an environment model
- Straightforward error traces
Scenarios

Process A

(\text{!a})
\text{<b>}
\text{<c>}
\text{[d]}
\text{<x>}
\text{<y>}
\text{<z>}

Process B

Scenario A.1

(\text{!a})
\text{<b>}
\text{<c>}
\text{[d]}

Scenario A.2

(\text{!a})
\text{<b>}
\text{<c>}
\text{[d]}

Scenario B.1

(\text{!d})
\text{<x>}
\text{<y>}

Scenario B.2

(\text{!d})
\text{<x>}
\text{<y>}
\text{<z>}

16
Scenario Selection

Model 1

Model 2

Model 3

Model

Scenarios

Process A

A.1, A.2

Process B

B.1, B.2

A.1

- 

A.2

B.1

B.2
Demo
Thank You