Static Analysis

Prof. Leon J. Osterweil
CS 520/620
Spring 2013

Requirements Spec.

Characteristics of System to be built must match required characteristics
Hi level design must show HOW requirements can be met
Test Results must match required behavior

Test Plan

Design

Hi Level consistent views
Low level
Code/must implement design

Code

Test plan exercises this code
DEVELOPMENT PHASES

Requirements Specification → Architecting → Implementation Designing → Coding

System Test Plan → Software Sys. Test Plan → Integration Test Plan → Unit Test Plan

TEST PLANNING

System Testing → Software Sys Testing → Integration Testing → Unit Testing

TESTING PHASES
Summary of Dynamic Testing

- **Strengths:**
  - Microscopic examination of execution details
  - Evaluation in actual runtime environment
  - Oldest approach, most familiar

- **Weaknesses:**
  - Cannot demonstrate absence of faults
  - Hard to generate test data
  - Hard to know when testsets are adequate
  - Testing aids (e.g., assertion checkers) alter execution

Some References for Testing

- Ghezzi, Jazayeri, Mandrioli, Fundamentals of Software Engineering, Chapter 6.3 (Testing)
  - Excellent annotated bibliography at the end of Ch. 6
- Many of those references are now rather old
  - Much recent work in this area
- Proceedings of the International Symposium on Software Testing and Analysis (ISSTA)
- Proceedings of International Conference on Software Engineering (ICSE)
Summary of Problems in Doing Testing Effectively

• Hard to cover program execution space effectively

• Hard to select test data effectively

• Hard to tell if test results are right or wrong
  --if program computes complex function(s)
  --if the number of test cases gets large

• Best to detect errors early--before they become faults

• Testing comes at the end of the lifecycle, when time and budget tend to be short

What do you know when testing is done?
What relations have been checked?
  How thoroughly?
  To whose satisfaction?

Relations and Analysis

• A software product consists of
  – A collection of (types of) artifacts
  – Related to each other by myriad Relations

• The relations are essentially desiderata
  – At least initially

• Before the product can be trusted, the relations need to be verified/confirmed

• That is the role of analysis
  – Does the software do what it is supposed to do?
  – What are its capabilities and its strengths?
  – What is the nature of the artifact(s) that have been built?
  – What can I count on?
  – What should I worry about?
Static Analysis

• Technique for demonstrating the absence of faults without the need for execution
• Specification of Intent: derived from requirements
• Specification of Behavior: derived from model(s)
• Comparison: Done analytically and mathematically
• Results: Theorems about the program (eg. proofs that certain behaviors are impossible—or mandatory)

ANALYSIS AND TESTING PHASES
Testing and Analysis Framework

Specification of Intended Behavior

Development (Synthesis) Process

Evaluation (Analysis) Process

Testing/Analysis Results

Comparison of Behavior to Intent (relation checking)

Dynamic Testing

Specification of Intended Behavior

Required Outputs

Test Execution Results

Result Comparator (Human or Machine)

Failure Reporting

Comparison of Behavior to Intent
Static Analysis

- Specification of Intended Behavior
- (Rqts. (?)) Specification
- Derived From Source Text
- Specification of Actual Behavior
- Mathematical Reasoning
- Theorems Or Counterexamples
- Comparison of Behavior to Intent

Natural Complementarity

- Static Analysis excels at scanning for trouble
- Dynamic testing excels at focusing in sharply
- Both aim to identify violations of well-formedness properties
- Techniques should be mutually supportive, synergistic
- More on this later
Dataflow Analysis

- Specification of Intent: Sequence of events
- Specification of Behavior: Derived from flowgraph model
  - Nodes annotated with events of interest
  - All possible executions modeled as all sequences of events along all flowgraph paths
- Comparison: Analytic process
  - Are all possible event sequences the desired one(s)?
- Result: Theorems demonstrating absence of event sequence errors
- Examples:
  - No variable referenced before definition
  - No file read before it is opened
  - Elevator doesn’t move until doors are shut
  - Rocket won’t try to fire thrusters after fuel is exhausted

Use of the Flow Graph (ImmFol Relation) to Determine Actual Behavior

- Determine local information by looking at local behavior
  - Which artifacts are created, used,
- Infer global information
  - By looking at local information
  - And tracing flow graph edges to find relevant information at other nodes
Documenting Local Behavior

- First, determine local information that is true at each node in the CFG
  - e.g., What variables are defined
    - What variables are referenced
  - Usually stored in sets
    » e.g., ref(n) is the set of variables referenced at node n

- This same type of information available for pre-code artifacts
  - Interface specifications for modules
  - Input and output specifications of requirements elements

Standard Propagation Rules

- Need to propagate information from IMMFOl neighbors
  - Backwards or forwards
- Must take branching into account
- Must add in “local” information
  - What is happening at this node
Inferring Global Behavior Example: Reaching Definitions

- Definition reaches a node if there is a def clear path from the definition to that node
- Do this by tracing paths between nodes
- Definition of x at node 1 reaches nodes 2, 3, 4, 5 but not 6
Another Example: Live Variables

- A variable, x, is live at node p if there exists a def-clear path for x from node p to a use of x.
- x is live at 2, 3, 4, 5 but not at node 6.

This is best done by tracing backwards.

Applicable to models of pre-code artifacts too.
Different Global Behavior Problems Require Different Propagation Rules

• Some use forward tracing
• Some use backward tracing
• Some require ANDing
• Some require ORing
• Some compute ALL results
• Some compute SOME results
• Some compute NONE results
• And various combinations of the above

“Might” or “Must” reaching behavior

Definitions that might reach a node

Definitions that must reach a node
Finite State Verification: Using Data Flow Analysis to Verify Properties

- Data flow analysis used to infer behavior
- Requires use of propagation among nodes
  - Multiple propagations may be needed
- Inferred behavior can then be compared to desired
  - Often comes from Requirements spec.
    » E.g. robustness specs.
- Works on any graph--not just graphs derived from code
  - E.g. DFGs in requirements or architectures
Examples of Properties

• Language specific
  – No undefined references
  – Can’t write to a file until it is opened
• Specific to a system
  – Can’t get money until pwd is OK
  – Can’t move elevator with doors open
  – Etc.

Some properties are much more complicated. Longer sequences of events
Approach

• Define a desired (or undesired) property as a FSA
  – Based on identification of an alphabet of significant events
• Trace all paths through a graph that models the software
  – Where some nodes are annotated as the sites of events of interest
• Use the FSA as an acceptor
  – All paths from start to end through the model should reach an accepting state

Using FSAs to Define: The “Safe Elevator” Property

A Property, P: The elevator does not move while its doors are open.

Events: {open, close, move}

$L(P)$ is the set of all strings accepted by property $P$

All traces through the system should satisfy this property (drive FSA to accepting state)

Error: “trap” state
Using Quantified Regular Expressions

- Alphabet, quantification, regular expression

- For the events \{open, close, move\} show that for all paths

\[((\text{close} \vee \text{move})^*, (\text{open}^+, \text{close})^*)^*, \text{open}^*\]

---

Event Stream Comes from Traces through an annotated CFG

- CFG \( G \) is \((N, n_{\text{initial}}, n_{\text{final}}, E)\)
- Use annotation relation to associate events with nodes
  - \( \Sigma_G \) is the alphabet of \( G \)
  - Events must be indivisible wrt other events in the property
- \( \mathcal{L}(G) \) is the language of \( G \)
  - The set of all strings in \( (\Sigma_G)^* \) that occur on paths from the initial node to the final node
Static Dataflow Analysis

Specification of Intended Behavior

Event Sequences

Possible Execution Sequences

Dataflow Propagation Algorithms

Comparison of Behavior to Intent

Proofs of the Presence or Absence of Faults

Quality Determination Architectural Framework

Specification of Intended Behavior

Development (Synthesis) Process

Evaluation (Analysis) Process

Testing/Analysis Results

Comparison of Behavior to Intent (relation checking)
Characteristics of Dynamic Analysis

- Dynamic analysis approaches are based on sampling the input space
  - Infer behavior or properties of a system from executing a sample of test cases
  - Functional (Black Box) and Structural (White Box) approaches
- Allows very detailed examination of one execution
  - But nothing about any other execution
  - Cannot prove the absence of faults, only the presence of failures

Informal Dynamic Testing

- Specification of Intended Behavior
- Execution Results
- Test Cases
- Evaluation Process
- Failures Observed
- Comparison of Behavior to Intent
Automated Dynamic Testing

- Specification of Intended Behavior
- Rigorous Specs. (Asserts)
- Evaluation Process
- Execution Results
- Automated Comparator
- Comparison of Behavior to Intent
- Specification of Actual Behavior
- Failures Reported

Move from Dynamic Analysis to Static Analysis

- Dynamic analysis approaches are based on sampling the input space
  - Infer behavior or properties of a system from executing a sample of test cases
  - Black Box versus White Box approaches
- Static analysis approaches tend to be based on a “global” assessment of the behavior
  - Based on an understanding of the program (artifact)
  - Again, usually must approximate the semantics to keep the problem tractable
  - Can prove the absence of faults
Static Analysis

Specification of Intended Behavior

Assertions, Theorem Statements

Evaluation Process

Annotated Flow Graph

Comparision of Behavior to Intent

Specfication of Actual Behavior

Rigorous Formal Reasoning, Inference

Proofs of theorems About absence or presence of specific kinds of faults

Static Analysis Approaches

• Data Flow Analysis
• Concurrency Analysis
• Symbolic Evaluation
• Formal Verification
Static Analysis Approaches

- Data Flow Analysis
- Concurrency Analysis
- Symbolic Evaluation
- Formal Verification

Architecture of a Static Finite State Verification System
Simple Example: Actual Behavior

```plaintext
call_for_elevator
1: if (stopped at call_floor) then
2: open;
end if;
...
3: if (stopped at non_call_floor) then
4: close;
end if;
5: move;
...
```

Intended Behavior

```plaintext
1
\[
\text{close} \quad \text{move} \quad \text{open}
\]
2
\[
\text{open} \quad \text{move}
\]
3
\[
\text{close} \quad \text{move} \quad \text{open}
\]```

CS 620 Spring 2013 Univ. of Massachusetts
Copyright L. Osterweil, all rights reserved
**Verification of consistency between system and requirement**

- **System Translator**
- **Annotated CFG**
- **Property Translator**
- **Reasoning Engine**
- **Event alphabet**
- **Property**
- **Consistent**
- **Inconsistent**
- **FSA**

**Event Alphabet**

- Ada, Java, C++, Jovial

**Property**

- Often a robustness requirement

**Determining consistency between functionality and robustness requirement**

**Worklist:** 2, 3, 5

1: if
   - 1: if
     - 1: if
       - 1: if
         - 1: if
           - 1: if
             - 1: if
               - 1: if
                 - 1: if
                   - 1: if
                     - 1: if
                       - 1: if
                         - 1: if
                           - 1: if
                             - 1: if
                               - 1: if
                                 - 1: if
                                   - 1: if
                                     - 1: if
                                       - 1: if
                                         - 1: if
                                           - 1: if
                                             - 1: if
                                               - 1: if
                                                 - 1: if
                                                   - 1: if
                                                     - 1: if
                                                       - 1: if
                                                         - 1: if
                                                           - 1: if
                                                             - 1: if
                                                               - 1: if
                                                                 - 1: if
                                                                   - 1: if
                                                                     - 1: if
                                                                       - 1: if
                                                                         - 1: if
                                                                             - 1: if
                                                                                 - 1: if
                                                                                   - 1: if
                                                                                     - 1: if
                                                                                       - 1: if
                                                                                         - 1: if
                                                                                           - 1: if
                                                                                             - 1: if
                                                                                               - 1: if
                                                                                                 - 1: if
                                                                                                   - 1: if
                                                                                                     - 1: if
                                                                                                       - 1: if
                                                                                                         - 1: if
                                                                                                             - 1: if
                                                                                                               - 1: if
                                                                                                                 - 1: if
                                                                                                                   - 1: if
                                                                                                                     - 1: if
                                                                                                                       - 1: if
                                                                                                                         - 1: if
                                                                                                                             - 1: if
                                                                                                                               - 1: if
                                                                                                                                   - 1: if
                                                                                                                                     - 1: if
                                                                                                                                       - 1: if
                                                                                                                                         - 1: if
                                                                                                                                             - 1: if
                                                                                                                                                - 1: if
                                                                erin a less readable format due to the complexity of the diagram.
Determining consistency between functionality and robustness requirement

Violation Path
Appears to be Unexecutable: A "False Positive"

1: if
2: open
3: if
4: close
5: move

... if (stopped) then
2: open; end if;
... if (stopped) then
4: close; end if;
... move;

One Way to Fix the Example

call_for_elevator
1: if (stopped at call_floor) then
2: open;
else
4: close;
move_to_call_floor
6: open;
end if;
collect_destination;
7: close;
5: move;
...
Now Property Holds

1: if
   {1}
   {1}

   2: open
   {1}
   {2}

   4: close
   {1}
   {1}

   6: open
   {1}
   {2}

   7: close
   {2}
   {1}

   5: move
   {1}
   {1}

Now Property Holds

1: if
   {1}

   2: open
   {1}
   {2}

   4: close
   {1}

   6: open
   {1}
   {2}

   7: close
   {2}
   {1}

   5: move
   {1}
   {1}
But is it really necessary to modify the program?

When maybe the problem is with the precision of the analysis
Produced this Result

With this Spurious Report of a Fault

Spurious because the fault is on a path that is not executable

```plaintext
1: if
2: open
3: if
4: close
5: move

1: if
2: open
3: if
4: close
5: move

1: if (stopped) then
2: open; end if;
3: if (stopped) then
4: close; end if;
5: move;
```
How to address these kinds of problems attributable to lack of precision?

Improving Precision

- System Translator
- Trace Flow Graph
- State Propagation
- Property FSA
- Property Specification
- Constraints
- Property Verified
- Counter Example Trace through TFG
**Constraints**

- Are represented as FSAs
- Describe conditions necessary for feasible execution
- Have a special *violation state* that is entered when an infeasible path is detected
  - Violation is a trap state; once it is entered, never leave that state
Boolean Variable Constraint

== is a predicate
= is assignment

CS 620 Spring 2013 Univ. of Massachusetts
Copyright L. Osterweil, all rights reserved
How do constraints affect the data flow equations

- IN and OUT are now sets of tuples of FSA states
- Merge is still union
- Transfer function now has to look at each FSA state in the in-tuple when computing the out-tuple
  - Property states not propagated when any constraint automaton is in the violation state
- Result looks at paths that are feasible with respect to the constraints
  - The property state is the same as before
  - Every constraint must be in an accepting state

Elevator Revisited

1: if

1, 2, 4: if (stopped) then
3: open;
   end if;

5, 6, 8: if (stopped) then
7: close;
   end if;

9: move;

2: S==t

4: S==f

3: open

5: if

6: S==t

8: S==f

7: close

9: move
State Propagation

Worklist: 2, 4

1: if <1,u> <1,u>

2: S==t

3: open

4: S==f <1,u> <1,f>

5: if <2,t>,<1,f>

6: S==t

7: close

8: S==f <2,t>,<1,f>

9: move

State Propagation

Worklist: 2, 4

1: if <1,u> <1,u>

2: S==t

3: open

4: S==f <1,u> <1,f>

5: if <2,t>,<1,f>

6: S==t

7: close

8: S==f <2,t>,<1,f>

9: move
State Propagation

Worklist: 2, 4, 5, 6, 8

1: if
   <1, u> <1, u>

2: S = t
   <1, t>
   <2, t>

3: open

4: S = f
   <1, f>

5: if
   <2, t>, <1, f>
   <2, t>, <1, f>

6: S = t
   <2, t>, <1, f>

7: close
   <1, t>, <1, f>

8: S = f
   <2, t>, <1, f>

9: move
   <1, t>, <1, f>

State Propagation

Worklist: 2, 4, 5, 6, 8

1: if
   <1, u> <1, u>

2: S = t
   <1, t>
   <2, t>

3: open

4: S = f
   <1, f>

5: if
   <2, t>, <1, f>
   <2, t>, <1, f>

6: S = t
   <2, t>, <1, f>

7: close
   <1, t>, <1, f>

8: S = f
   <2, t>, <1, f>

9: move
   <1, t>, <1, f>
   <1, t>, <1, f>

<2, t>, <1, f>

<2, t>, <1, f>

<2, t>, <1, f>

<2, t>, <1, f>
Concurrent and Distributed Systems

- Extremely difficult to develop and test such systems
- Non-determinism means that
  - the same inputs might produce different outputs on different executions
  - When reasoning about a system there are numerous different alternatives to consider
     » Usually more than a programmer can reasonably consider
- In addition to the problems that can arise with sequential programs, have problems that are unique to concurrent systems
  - Data access problems
  - Synchronization problems
Power and Value of Static Analysis is Best Seen When Applied to Concurrent Systems

• Concurrent software is much harder, more complicated
• Requires very powerful analysis
• Finite state verification shines in this domain

Concurrent systems are complex

• Non-determinism means that
  – the same inputs might produce different outputs on different executions
  – When reasoning about a system there are numerous alternatives to consider
    » Usually more than a human can reasonably consider
• In addition to the problems that can arise with sequential programs, have problems that are unique to concurrent systems
  – Data access problems
  – Synchronization problems
Data Access Anomalies

- Typically you want mutual exclusion
  - shared resource (e.g., data) that should only have a single access at a time
  - e.g., don’t want two travel agents assigning the last seat on a plane
- Typically you don’t want race conditions
  - order of execution affects results
  - undesirable nondeterminism

\[
\begin{array}{c}
\text{task } A \\
x := x + 1; \\
\text{write } x; \\
\text{task } B \\
x := x - 1; \\
\text{write } x;
\end{array}
\]

if initially \( x = 5 \), then could output (6, 5), (4, 5), or (5, 5)

Interleaved Model of Execution; Examples

\[
\begin{array}{c}
\text{task } A \\
x := x + 1; \\
\text{write } x; \\
\text{task } B \\
x := x - 1; \\
\text{write } x;
\end{array}
\]

\[
\begin{array}{c}
\text{task } B \\
x := x - 1; \\
\text{write } x; \\
\text{task } A \\
x := x + 1; \\
\text{write } x;
\end{array}
\]

\[
\begin{array}{c}
\text{task } B \\
x := x - 1; \\
\text{task } A \\
x := x + 1; \\
\text{write } x; \\
\text{write } x;
\end{array}
\]

\[
\begin{array}{c}
\text{task } A \\
x := x + 1; \\
\text{task } B \\
x := x - 1; \\
x := x - 1; \\
\text{write } x; \\
\text{write } x;
\end{array}
\]
Infinite wait anomalies (continued)

- **Deadlock**
  - set of tasks mutually waiting on each other; none can advance
  - Often tasks hold resources that other tasks need
  - Also called, deadly embrace

- **Livelock**
  - execution does not come to a standstill but none of the tasks can advance

Reachability-based Model Checking: some history

- Originally proposed for hardware
- Early 80’s: E. Clarke and Emerson; Quielle and Sifakis
- Late 80’s: Improved algorithms and property notations (E. Clarke, Emerson, Sistla)
- 90’s: Symbolic Model Checking (SMV) and other optimizations (Burch, E. Clarke, Dill, Long, and McMillan)
- Current: Hybrid approaches that combine model checking with
  - Theorem proving techniques
  - Symbolic execution
  - Optimization techniques (e.g., points to analysis)
Reachability Graph

• Models state space
  – Each node represents a possible state in a distributed system
    » States represent the value of all the variables
    » For concurrent systems, this includes the program counter for each task
  – Considering only the value of the program counter for each task then each state is a vector where the ith element is the current program counter of the ith task
    » \( \langle \text{pc}_{1,i}; \text{pc}_{2,j}; \ldots; \text{pc}_{r,l} \rangle \)
    » Coarse-grained representation of a RG; doesn’t consider values of variables
  – More powerful analysis requires more complete and detailed state vector

Reachability Graph

• Typically, each edge represents progress in a single task
  – Multiple concurrent events may be possible, but allowing only single events captures all states and simplifies the graph structure (interleaved execution model)
• Only have multiple tasks progress when required by the semantics of the programming construct
  – E.g., rendezvous
• Only contains states that are potentially reachable from the start state
Reachability Graph Example

task control flow graphs
T1
\[ \text{begin} \rightarrow \text{T2.Q} \rightarrow \text{end} \]

T2
\[ \text{begin} \rightarrow \text{Accept Q} \rightarrow \text{end} \]

Reachability graph
\[ b_1, b_2 \rightarrow q, b_2 \rightarrow b_1, q' \rightarrow q, q' \rightarrow e_1, q' \rightarrow q, e_2 \rightarrow e_1, e_2 \]

Reachability Graph Example (clarified)

task control flow graphs
T1
\[ \text{begin} \rightarrow \text{T2.Q} \rightarrow \text{end} \]

T2
\[ \text{begin} \rightarrow \text{Accept Q} \rightarrow \text{end} \]

Reachability graph
\[ b_{q, q'} \rightarrow b_{q, b_2} \rightarrow b_1, b_{q'} \rightarrow r(q, q') \rightarrow e_1, q' \rightarrow q, e_2 \rightarrow e_1, e_2 \]

b_{q, q'} means that a task is blocked at q
r(q, q') means that the rendezvous between q and q' occurs
Use a worklist to build the reachability graph

Task control flow graphs

T1

begin

T2.Q

end

T2

begin

Accept Q

end

Reachability graph

Worklist:

\(<b_1, b_2><b_q, b_2><b_1, b_q><r(q, q')><e_1, q'><q, e_2><e_1, e_2>\)

Useful in determining possible/impossible synchronizations

Infeasible synchronizations

Infeasible synchronization??
Two possible synchronizations

begin
  T2.Q
  Accept Q
  T2.Q
end

begin
  Accept Q
  T2.Q
end

But this is “precise up to symbolic execution”

This is a bit harder

synchronizations
Also identifies deadlocks

Conclusions

- Finite state verification approaches are improving
- Being used in industry for hardware systems
- With the increasing interest in software security and quality, becoming more widely used for software systems
Evaluation of Static Analysis

• Strengths:
  – Can demonstrate the absence of faults
  – Proofs can be automatically generated and proven
  – Algorithms are fast (low-order polynomial)
  – No need to generate test data
  – You know when you are done

• Weaknesses
  – Behavior specification is a model with inaccuracies
    » Not all paths are executable
  – Only certain classes of faults analyzable
    » Mostly sequence specific
    » Weak on functionality

Symbolic Execution

• Specification of Intent: Formulae, functions

• Specification of Behavior: Functions derived from annotated flowgraph, symbol table
  – Annotate nodes with function(s) computed there
  – Specify path to be studied
  – Compute function(s) computed as composition(s) of functions at path nodes, constraints of path edges
  – Comparison: Solving simultaneous constraints; symbolic algebra

• Results: Demonstrations that given paths computed the right function(s)
Symbolic Execution

Specification of Intended Behavior

Function to be Computed

Specification of Actual Behavior

Formula Inferred from Actual Code

Functional Equivalence Theorem Prover

Comparison of Behavior to Intent

Proofs of Functional Correctness