189B: Testing

Instructor: Tevfik Bultan
Verification, Validation, Testing

- **Verification**: Demonstration of consistency, completeness, and correctness of the software artifacts at each stage of and between each stage of the software life-cycle.
  - Different types of verification: manual inspection, testing, formal methods
  - Verification answers the question: Am I building the product right?
- **Validation**: The process of evaluating software at the end of the software development to ensure compliance with respect to the customer needs and requirements.
  - Validation can be accomplished by verifying the artifacts produced at each stage of the software development life cycle
  - Validation answers the question: Am I building the right product?
- **Testing**: Examination of the behavior of a program by executing the program on sample data sets.
  - Testing is a verification technique used at the implementation stage.
Software Testing

• Goal of testing
  – finding faults in the software
  – demonstrating that there are no faults in the software (for the test cases that has been used during testing)

• It is not possible to prove that there are no faults in the software using testing

• Testing should help locate errors, not just detect their presence
  – a “yes/no” answer to the question “is the program correct?” is not very helpful

• Testing should be repeatable
  – could be difficult for distributed or concurrent software
  – effect of the environment, uninitialized variables
Testing Software is Hard

- If you are testing a bridge’s ability to sustain weight, and you test it with 1000 tons you can infer that it will sustain weight \( \leq 1000 \) tons.

- This kind of reasoning does not work for software systems:
  - software systems are not linear nor continuous.

- Exhaustively testing all possible input/output combinations is too expensive:
  - the number of test cases increase exponentially with the number of input/output variables.
Some Definitions

• Let $P$ be a program and let $D$ denote its input domain

• A **test case** $t$ is an element of input domain $t \in D$
  – a test case gives a valuation for all the input variables of the program

• A **test set** $T$ is a finite set of test cases, i.e., a subset of $D$, $T \subseteq D$

• The basic difficulty in testing is finding a test set that will uncover the faults in the program

• Exhaustive testing corresponds to setting $T = D$
Exhaustive Testing is Hard

```c
int max(int x, int y)
{
    if (x > y)
        return x;
    else
        return x;
}
```

- Number of possible test cases (assuming 32 bit integers)
  - \(2^{32} \times 2^{32} = 2^{64}\)
- Do bigger test sets help?
  - Test set \(\{(x=3, y=2), (x=2, y=3)\}\) will detect the error
  - Test set \(\{(x=3, y=2), (x=4, y=3), (x=5, y=1)\}\) will not detect the error although it has more test cases
- The power of the test set is not determined by the number of test cases
- But, if \(T_1 \supseteq T_2\), then \(T_2\) will detect every fault detected by \(T_1\)
Exhaustive Testing

• Assume that the input for the $\text{max}$ procedure was an integer array of size $n$
  – Number of test cases: $2^{32 \times n}$

• Assume that the size of the input array is not bounded
  – Number of test cases: $\infty$

• The point is, naive exhaustive testing is pretty hopeless
Random Testing

- Use a random number generator to generate test cases

- Derive estimates for the reliability of the software using some probabilistic analysis

- Coverage is a problem
Generating Test Cases Randomly

- If we pick test cases randomly it is unlikely that we will pick a case where \( x \) and \( y \) have the same value.
- If \( x \) and \( y \) can take \( 2^{32} \) different values, there are \( 2^{64} \) possible test cases. In \( 2^{32} \) of them \( x \) and \( y \) are equal.
  - Probability of picking a case where \( x \) is equal to \( y \) is \( 2^{-32} \).
- It is not a good idea to pick the test cases randomly (with uniform distribution) in this case.
- So, naive random testing is pretty hopeless too.

```cpp
bool isEqual(int x, int y) {
    if (x == y)
        z := false;
    else
        z := false;
    return z;
}
```
Types of Testing

• Functional (Black box) vs. Structural (White box) testing
  – Functional testing: Generating test cases based on the functionality of the software
  – Structural testing: Generating test cases based on the structure of the program
  – Black box testing and white box testing are synonyms for functional and structural testing, respectively.
    • In black box testing the internal structure of the program is hidden from the testing process
    • In white box testing internal structure of the program is taken into account
• Module vs. Integration testing
  – Module testing: Testing the modules of a program in isolation
  – Integration testing: Testing an integrated set of modules
Functional Testing, Black-Box Testing

• Functional testing:
  – identify the functions which software is expected to perform
  – create test data which will check whether these functions are performed by the software
  – no consideration is given how the program performs these functions, program is treated as a black-box: **black-box testing**
  – need an **oracle**: oracle states precisely what the outcome of a program execution will be for a particular test case. This may not always be possible, oracle may give a range of plausible values

• A systematic approach to functional testing: requirements based testing
  – driving test cases automatically from a formal specification of the functional requirements
Domain Testing

- Partition the input domain to equivalence classes
- For some requirements specifications it is possible to define equivalence classes in the input domain
- Here is an example: A factorial function specification:
  - If the input value $n$ is less than 0 then an appropriate error message must be printed. If $0 \leq n < 20$, then the exact value $n!$ must be printed. If $20 \leq n \leq 200$, then an approximate value of $n!$ must be printed in floating point format using some approximate numerical method. The admissible error is 0.1% of the exact value. Finally, if $n > 200$, the input can be rejected by printing an appropriate error message.
- Possible equivalence classes: $D_1 = \{n < 0\}$, $D_2 = \{0 \leq n < 20\}$, $D_3 = \{20 \leq n \leq 200\}$, $D_4 = \{n > 200\}$
- Choose one test case per equivalence class to test
Equivalence Classes

• If the equivalence classes are disjoint, then they define a partition of the input domain
• If the equivalence classes are not disjoint, then we can try to minimize the number of test cases while choosing representatives from different equivalence classes
• Example: $D_1 = \{x \text{ is even}\}$, $D_2 = \{x \text{ is odd}\}$, $D_3 = \{x \leq 0\}$, $D_4 = \{x > 0\}$
  – Test set $\{x=48, x=-23\}$ covers all the equivalence classes
• On one extreme we can make each equivalence class have only one element which turns into exhaustive testing
• The other extreme is choosing the whole input domain $D$ as an equivalence class which would mean that we will use only one test case
Testing Boundary Conditions

• For each range \([R_1, R_2]\) listed in either the input or output specifications, choose five cases:
  – Values less than \(R_1\)
  – Values equal to \(R_1\)
  – Values greater than \(R_1\) but less than \(R_2\)
  – Values equal to \(R_2\)
  – Values greater than \(R_2\)
• For unordered sets select two values
  – 1) in, 2) not in
• For equality select 2 values
  – 1) equal, 2) not equal
• For sets, lists select two cases
  – 1) empty, 2) not empty
Testing Boundary Conditions

- For the factorial example, ranges for variable $n$ are:
  - $[-\infty, 0], [0,20], [20,200], [200, \infty]$
  - A possible test set:
    - $\{n = -5, n=0, n=11, n=20, n= 25, n=200, n= 3000\}$
  - If we know the maximum and minimum values that $n$ can take we can also add those $n=$MIN, $n=$MAX to the test set.
Structural Testing, White-Box Testing

• Structural Testing
  – the test data is derived from the structure of the software

  – **white-box testing**: the internal structure of the software is taken into account to derive the test cases

• One of the basic questions in testing:
  – when should we stop adding new test cases to our test set?
  – Coverage metrics are used to address this question
Coverage Metrics

- Coverage metrics
  - **Statement coverage**: all statements in the programs should be executed at least once
  - **Branch coverage**: all branches in the program should be executed at least once
  - **Path coverage**: all execution paths in the program should be executed at least once

- The best case would be to execute all paths through the code, but there are some problems with this:
  - the number of paths increases fast with the number of branches in the program
  - the number of executions of a loop may depend on the input variables and hence may not be possible to determine
  - most of the paths can be infeasible

- Coverage tool: gcov (gcc based coverage tool)
Statement Coverage

• Choose a test set $T$ such that by executing program $P$ for each test case in $T$, each basic statement of $P$ is executed at least once

• Executing a statement once and observing that it behaves correctly is not a guarantee for correctness, but it is an heuristic
  - this goes for all testing efforts since in general checking correctness is undecidable

```c
bool isEqual(int x, int y)
{
    if (x = y)
        z := false;
    else
        z := false;
    return z;
}

int max(int x, int y)
{
    if (x > y)
        return x;
    else
        return x;
}
```
areTheyPositive(int x, int y)
{
    if (x >= 0)
        print("x is positive");
    else
        print("x is negative");
    if (y >= 0)
        print("y is positive");
    else
        print("y is negative");
}

Following test set will give us statement coverage:
T_1 = {(x=12,y=5), (x=−1,y=35), (x=115,y=−13),(x=−91,y=−2)}

There are smaller test cases which will give us statement coverage too:
T_2 = {(x=12,y=−5), (x=−1,y=35)}

There is a difference between these two test sets though
Statement vs. Branch Coverage

assignAbsolute(int x) {
    if (x < 0)
        x := -x;
    z := x;
}

Consider this program segment, the test set 
T = {x=−1} will give statement coverage, 
however not branch coverage

Control Flow Graph:

Test set {x=−1} does not 
execute this edge, hence, it 
does not give branch coverage
Control Flow Graphs (CFGs)

- Nodes in the control flow graph are basic blocks
  - A **basic block** is a sequence of statements always entered at the beginning of the block and exited at the end
- Edges in the control flow graph represent the control flow

```java
if (x < y) {
    x = 5 * y;
    x = x + 3;
} else
    y = 5;
    x = x + y;
```

- Each block has a sequence of statements
- No jump from or to the middle of the block
- Once a block starts executing, it will execute till the end
Branch Coverage

- Construct the control flow graph

- Select a test set $T$ such that by executing program $P$ for each test case $d$ in $T$, each edge of $P'$'s control flow graph is traversed at least once

```
x := -x

B0
(x < 0)       true
B1
x := -x
false
B2
z := x
```

Test set $\{x=-1\}$ does not execute this edge, hence, it does not give branch coverage.

Test set $\{x=-1, x=2\}$ gives both statement and branch coverage.
Path Coverage

• Select a test set $T$ such that by executing program $P$ for each test case $d$ in $T$, all paths leading from the initial to the final node of $P$’s control flow graph are traversed
areTheyPositive(int x, int y) {
    if (x >= 0)
        print("x is positive");
    else
        print("x is negative");
    if (y >= 0)
        print("y is positive");
    else
        print("y is negative");
}

Test set:
T_2 = {(x=12,y=-5), (x=-1,y=35)}
gives both branch and statement coverage but it does not give path coverage

Set of all execution paths: {(B0,B1,B3,B4,B6), (B0,B1,B3,B5,B6), (B0,B2,B3,B4,B6), (B0,B2,B3,B5,B6)}
Test set T_2 executes only paths: (B0,B1,B3,B5,B6) and (B0,B2,B3,B4,B6)
areTheyPositive(int x, int y) {
    if (x >= 0)
        print("x is positive");
    else
        print("x is negative");
    if (y >= 0)
        print("y is positive");
    else
        print("y is negative");
}

Test set:
T₁ = {(x=12,y=5), (x=−1,y=35),
(x=115,y=−13),(x=−91,y=−2)}
gives both branch, statement and path coverage
Path Coverage

- Number of paths is exponential in the number of conditional branches
  - Testing cost may be expensive

- Note that every path in the control flow graphs may not be executable
  - It is possible that there are paths which will never be executed due to dependencies between branch conditions

- In the presence of cycles in the control flow graph (for example loops) we need to clarify what we mean by path coverage
  - Given a cycle in the control flow graph we can go over the cycle arbitrary number of times, which will create an infinite set of paths
  - Redefine path coverage as: each cycle must be executed 0, 1, ..., k times where k is a constant (k could be 1 or 2)
Condition Coverage

- In the branch coverage we make sure that we execute every branch at least once
  - For conditional branches, this means that, we execute the TRUE branch at least once and the FALSE branch at least once
- Conditions for conditional branches can be compound boolean expressions
  - A compound boolean expression consists of a combination of boolean terms combined with logical connectives AND, OR, and NOT
- Condition coverage:
  - Select a test set $T$ such that by executing program $P$ for each test case $d$ in $T$, (1) each edge of $P$’s control flow graph is traversed at least once and (2) each boolean term that appears in a branch condition takes the value TRUE at least once and the value FALSE at least once
- Condition coverage is a refinement of branch coverage (part (1) is same as the branch coverage)
Condition Coverage

```java
something(int x)
{
    if (x < 0 || y < x)
    {
        y := -y;
        x := -x;
    }
    z := x;
}
```

T = \{(x=-1, y=1), (x=1, y=1)\} will achieve statement, branch and path coverage, however T will not achieve condition coverage because the boolean term (y < x) never evaluates to true. This test set satisfies part (1) but does not satisfy part (2).

T = \{(x=-1, y=1), (x=1, y=0)\} will not achieve condition coverage either. This test set satisfies part (2) but does not satisfy part (1). It does not achieve branch coverage since both test cases take the true branch, and, hence, it does not achieve condition coverage by definition.

T = \{(x=-1, y=-2), (x=1, y=1)\} achieves condition coverage.
Multiple Condition Coverage

• Multiple Condition Coverage requires that all possible combination of truth assignments for the boolean terms in each branch condition should happen at least once.

• For example for the previous example we had:

\[ x < 0 \land y < x \]

\begin{align*}
\text{term1} &\equiv x < 0 \\
\text{term2} &\equiv y < x
\end{align*}

• Test set \{(x=\text{-}1, y=\text{-}2), (x=1, y=1)\}, achieves condition coverage:
  – test case \((x=\text{-}1, y=\text{-}2)\) makes \(\text{term1}=\text{true}, \text{term2}=\text{true}\), and the whole expression evaluates to true (i.e., we take the true branch).
  – test case \((x=1, y=1)\) makes \(\text{term1}=\text{false}, \text{term2}=\text{false}\), and the whole expression evaluates to false (i.e., we take the false branch).

• However, test set \{(x=\text{-}1, y=\text{-}2), (x=1, y=1)\} does not achieve multiple condition coverage since we did not observe the following truth assignments:
  – \(\text{term1}=\text{true}, \text{term2}=\text{false}\)
  – \(\text{term1}=\text{false}, \text{term2}=\text{true}\)
Types of Testing

• Unit (Module) testing
  – testing of a single module in an isolated environment

• Integration testing
  – testing parts of the system by combining the modules

• System testing
  – testing of the system as a whole after the integration phase

• Acceptance testing
  – testing the system as a whole to find out if it satisfies the requirements specifications
Types of Testing

• Unit (Module) testing
  – testing of a single module in an isolated environment

• Integration testing
  – testing parts of the system by combining the modules

• System testing
  – testing of the system as a whole after the integration phase

• Acceptance testing
  – testing the system as a whole to find out if it satisfies the requirements specifications
Unit Testing

- Involves testing a single isolated module

- Note that unit testing allows us to isolate the errors to a single module
  - we know that if we find an error during unit testing it is in the module we are testing

- Modules in a program are not isolated, they interact with each other.
  Possible interactions:
  - calling procedures in other modules
  - receiving procedure calls from other modules
  - sharing variables

- For unit testing we need to isolate the module we want to test, we do this using two things
  - drivers and stubs
Drivers and Stubs

• **Driver:** A program that calls the interface procedures of the module being tested and reports the results
  
  – A driver simulates a module that calls the module currently being tested

• **Stub:** A program that has the same interface as a module that is being used by the module being tested, but is simpler.
  
  – A stub simulates a module called by the module currently being tested
  
  – Mock objects: Create an object that mimics only the behavior needed for testing

•
Drivers and Stubs

- Driver and Stub should have the same interface as the modules they replace.
- Driver and Stub should be simpler than the modules they replace.
Integration Testing

• Integration testing: Integrated collection of modules tested as a group or partial system

• Integration plan specifies the order in which to combine modules into partial systems

• Different approaches to integration testing
  – Bottom-up
  – Top-down
  – Big-bang
  – Sandwich
Module Structure

- A uses C and D; B uses D; C uses E and F; D uses F, G, H and I; H uses I
- Modules A and B are at level 3; Module D is at level 2
- Modules C and H are at level 1; Modules E, F, G, I are at level 0
- Level 0 components do not use any other components
- Level i components use at least one component on level i-1 and no component at a level higher than i-1

We assume that the uses hierarchy is a directed acyclic graph.
- If there are cycles merge them to a single module
Bottom-Up Integration

• Only terminal modules (i.e., the modules that do not call other modules) are tested in isolation

• Modules at lower levels are tested using the previously tested higher level modules

• Non-terminal modules are not tested in isolation

• Requires a module driver for each module to feed the test case input to the interface of the module being tested
  – However, stubs are not needed since we are starting with the terminal modules and use already tested modules when testing modules in the lower levels
Bottom-up Integration
Top-down Integration

• Only modules tested in isolation are the modules which are at the highest level

• After a module is tested, the modules directly called by that module are merged with the already tested module and the combination is tested

• Requires stub modules to simulate the functions of the missing modules that may be called
  – However, drivers are not needed since we are starting with the modules which is not used by any other module and use already tested modules when testing modules in the higher levels
Top-down Integration
Other Approaches to Integration

• Sandwich Integration
  – Compromise between bottom-up and top-down testing
  – Simultaneously begin bottom-up and top-down testing and meet at a predetermined point in the middle

• Big Bang Integration
  – Every module is unit tested in isolation
  – After all of the modules are tested they are all integrated together at once and tested
  – No driver or stub is needed
  – However, in this approach, it may be hard to isolate the bugs!
System Testing, Acceptance Testing

- System and Acceptance testing follows the integration phase
  - testing the system as a whole

- Test cases can be constructed based on the requirements specifications
  - main purpose is to assure that the system meets its requirements

- Manual testing
  - Somebody uses the software on a bunch of scenarios and records the results
  - Use cases and use case scenarios in the requirements specification would be very helpful here
  - manual testing is sometimes unavoidable: usability testing
System Testing, Acceptance Testing

- Alpha testing is performed within the development organization

- Beta testing is performed by a select group of friendly customers

- Stress testing
  - push system to extreme situations and see if it fails
  - large number of data, high input rate, low input rate, etc.
Regression testing

• You should preserve all the test cases for a program

• During the maintenance phase, when a change is made to the program, the test cases that have been saved are used to do **regression testing**
  – figuring out if a change made to the program introduced any faults

• Regression testing is crucial during maintenance
  – It is a good idea to automate regression testing so that all test cases are run after each modification to the software

• When you find a bug in your program you should write a test case that exhibits the bug
  – Then using regression testing you can make sure that the old bugs do not reappear
Test Plan

• Testing is a complicated task
  – it is a good idea to have a test plan

• A test plan should specify
  – Unit tests
  – Integration plan
  – System tests
  – Regression tests
Test Driven Development

• A style of programming that has become popular with agile software development approaches such as extreme programming

• Basic idea: Write the test cases before writing the code
  – Test first, code second

• Divide the implementation to small chunks
  – First write the test that tests the next functionality
  – Check if the test fails (it should, since the functionality is not implemented yet)
  – Then, write the code to implement the functionality
  – Run all the tests and make sure that the code passes all the tests
Automated Testing

• Automated testing refers to the techniques which generate the test sets automatically

• We will talk about several automated testing techniques

• Exhaustive bounded testing

• Random testing

• Fuzzing

• Symbolic Execution
Korat

• An automated testing tool
  – Application domain is unit testing of complex data structures

• It uses Java predicates to generate the test cases
  – These are Java methods which return a boolean value
  – For example, pre and post-conditions of methods

• Korat generates the test cases from pre and postconditions of methods

• There is no need to write an extra specification if the class contract is written as Java predicates
Korat

• Korat uses the method precondition to automatically generate all nonisomorphic test cases up to a given small size
  
  – Given a predicate and a bound on the size of its inputs Korat generates all nonisomorphic inputs for which the predicate returns true

• Korat then executes the method on each test case and uses the method postcondition as a test oracle to check the correctness of output

  – Korat exhaustively explores the bounded input space of the predicate but does so efficiently by monitoring the predicate’s executions and pruning large portions of the search space
Small Scope Hypothesis

• Success of Korat depends on the small scope hypothesis

• Small scope hypothesis
  – If there is a bug, there is typically a counter-example demonstrating the bug within a small scope.

• This is not a bad assumption if you are analyzing data structures (the target for Korat)
Random Testing

• We discussed that random testing is hopeless is one uses a uniform distribution for inputs
  – The chances of covering a particular condition is very low

• However, if we use the program being tested to guide how we choose the test cases, then random test generation can be more effective
  – Construct the inputs using the methods that are part of the program that is being tested

• This is the approach used in feedback-directed random test generation
Feedback-Directed Random Unit Testing

• This is a unit testing approach where it is assumed that the unit under test consists of a set of methods
  – A class, or a set of classes in an object oriented program for example

• The basic idea is to build inputs incrementally by randomly selecting a method call to apply and finding arguments from among previously constructed inputs
  – The result (object) returned by the newly generated call is first checked against
    • Contracts (to look for contract violations)
    • Filters (to eliminate duplicate or uninteresting cases)
  – Then it is added to the available set of inputs to be used as an input in future method calls
Randoop

- Randoop is a fully automated testing tool that implements the feedback-directed random test generation for .NET and Java.

- An object-oriented unit test consists of a sequence of method calls that set up the state (by creating and mutating objects) and an assertion about the result of the final call.
  - Randoop generates such unit tests.

- Randoop found serious errors in widely-deployed commercial open-source software.
Fuzzing

- A type of random testing
- Generate many anomalous/abnormal test cases, run them, and observe the application behavior for errors

Types of fuzzing:
- Mutation based fuzzing: mutate existing test cases to generate new test cases
- Generation based fuzzing: generate test cases based on input models
  - Tool: Peach Fuzzer
- Evolutionary fuzzing: generate test cases based on the feedback obtained from the program
  - Tools: American fuzzy lop (AFL) fuzzer, libFuzzer
Symbolic Execution

• Executes the program on *symbolic* values
• Symbolic values are unspecified input values that can take any concrete value
• Symbolic execution captures program behavior for any concrete input value
• Symbolic execution generates *path conditions (PC)* where each path condition captures the constraints on the input for a given execution path
• Symbolic execution generates path conditions for all execution paths up to a certain execution depth
• Symbolic execution uses a constraint solver to determine if a path condition is satisfiable
  – If a path condition is not satisfiable, this means that corresponding path is not feasible and should not be explored anymore
A 4-digit PIN Checker

```c
bool checkPIN(guess[]) {
    for(i = 0; i < 4; i++)
        if(guess[i] != PIN[i])
            return false
    return true
}
```

*P: PIN, G: guess*
Symbolic Execution of PIN Checker

bool checkPIN(guess[])
for(i = 0; i < 4; i++)
    if(guess[i] != PIN[i])
        return false
return true

\( P: \text{PIN}, \ G: \text{guess} \)
What about loops?

- How does symbolic execution deal with loops (or recursion) in our code?

- Loops and recursion can create arbitrarily long paths.

- Need to set a bound on the number of iterations, depth of recursion, and/or size of PCs.
Limitations of Symbolic Execution

• Path explosion!

• Cumulative cost of solving path conditions.

• Solver limitations (complex/undecidable constraints).

• Heap modeling. Pointers, aliasing, pointer arithmetic.

• Interactions with the environment. Library calls, system calls, native calls.
Pros and cons

• Serious limitations, but also serious advantages.
• Within the class of programs that are currently amenable to symbolic execution, amazing things can be achieved.
• Great tool if we are smart about when to use it, what to use it for, and what to combine it with.
Symbolic Execution Tools

- Symbolic PathFinder (Java bytecode)
- KLEE (LLVM)
- Otter (C)
- RubyX (Ruby)
- SymDroid (Dalvik bytecode)
- Mayhem (binaries)
- angr (binaries)
- SymJS (Java Script)