TVVS - Test, Verification and Validation of Software

Security Testing

Ana Paiva

apaiva@fe.up.pt **www.fe.up.pt/~apaiva**

Security Testing

- Security testing is a process to determine that an information system protects data and maintains functionality
- To check whether there is any information leakage
- To test the application whether it has unauthorized access and having the encoded security code
- To finding out the potential loopholes and weaknesses of the system

Security Testing

Security Testing is (according to ISTQB): Testing to determine the security of the software product

Types:

- Vulnerability Scanning
- Security Scanning
- Penetration Testing
- Risk Assessment
- Security Auditing
- Ethical Hacking
- Password cracking
- (…)

Security Testing

- **Vulnerability Scanning**: This is done through automated software to scan a system against known vulnerability signatures.

- **Security Scanning:** It involves identifying network and system weaknesses, and later provides solutions for reducing these risks. This scanning can be performed for both Manual and Automated scanning.

- **Penetration testing**: This kind of testing simulates an attack from a malicious hacker. This testing involves analysis of a particular system to check for potential vulnerabilities to an external hacking attempt.

Security Testing

- **Risk Assessment:** This testing involves analysis of security risks observed in the organization. Risks are classified as Low, Medium and High. This testing recommends controls and measures to reduce the risk.
- **Security Auditing:** This is an internal inspection of Applications and Operating systems for security flaws. An audit can also be done via line by line inspection of code
- **Ethical hacking:** It's hacking an Organization Software systems. Unlike malicious hackers, who steal for their own gains, the intent is to expose security flaws in the system.
- **Password Cracking**: Programs can be used to identify weak passwords

Security Concepts

- Confidentiality
- Integrity
- Authentication
- Authorization
- Availability
- Non-repudiation

Security Concepts

- Confidentiality
  - Ensuring information is accessible only for those with authorized access and to prevent information theft
- Integrity
  - A measure intended to allow the receiver to determine that the information which it is providing is correct
- Authentication
  - The process of establishing the identity of the user

Security Concepts

- Authorization
  - The process of determining that a requester is allowed to receive a service or perform an operation
- Availability
  - Assuring information and communications services will be ready for use when expected
- Non-repudiation
  - A measure intended to prevent the later denial that an action happened, or communication that took place

Some Tools...

- OWASP
- WireShark
- W3af
- Nessus
- Nikto
- Gendarme
- Flawfinder
- …

TVVS - Test, Verification and Validation of Software

Test case design

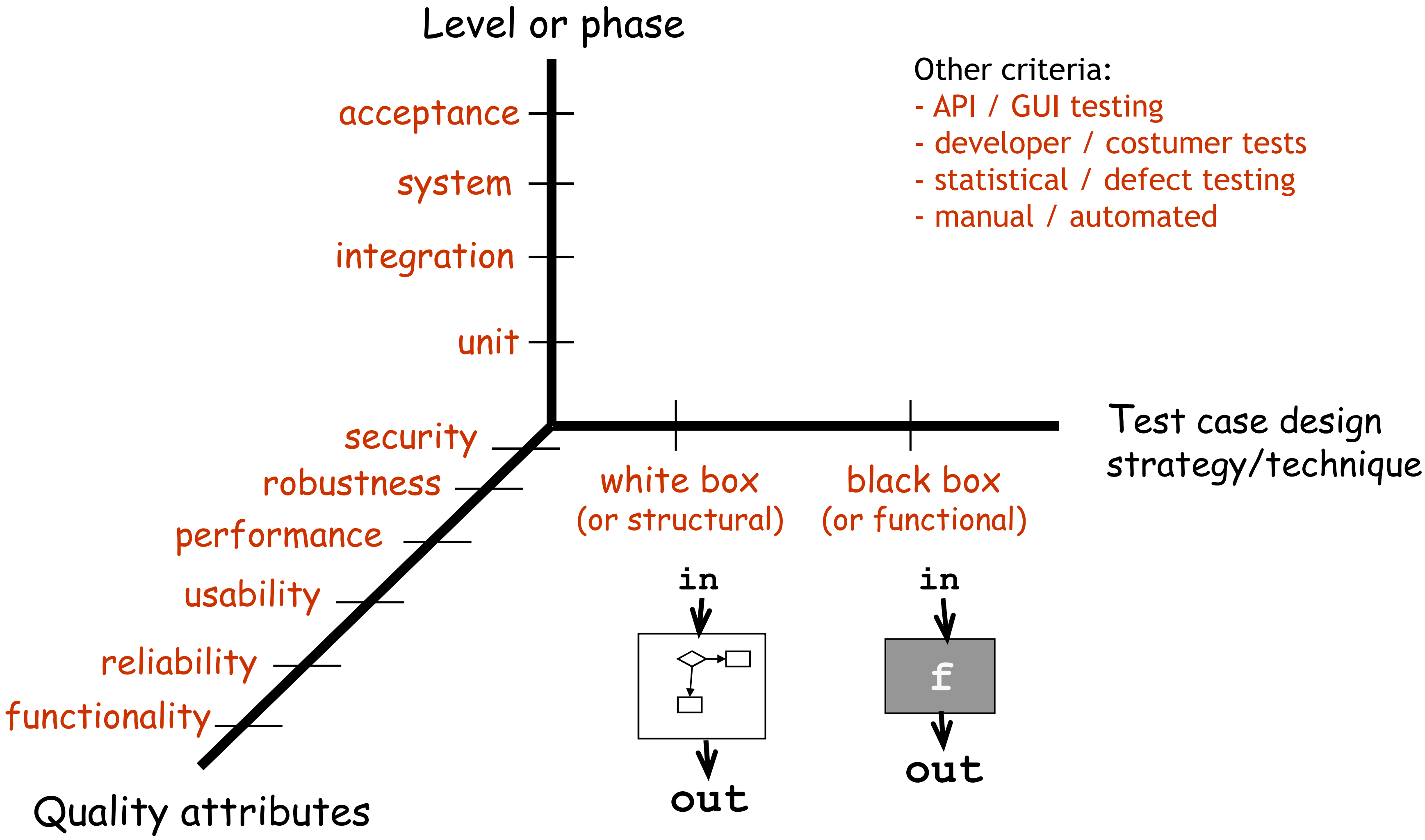
Ana Paiva

apaiva@fe.up.pt **www.fe.up.pt/~apaiva**

Agenda

- Introduction
- Black-box testing techniques
- Exercise

Test types (remember)



Other criteria:
- API / GUI testing
- developer / costumer tests
- statistical / defect testing
- manual / automated

Test cases (remember)

- **test case**
  - (1) A set of input values, execution preconditions, expected results and execution post-conditions, developed for a particular objective or test condition, such as to exercise a particular program path or to verify compliance with a specific requirement.

    [according to ISTQB]

  - **(2)** (IEEE Std 829-1983) Documentation specifying inputs, predicted results, and a set of execution conditions for a test item

    [IEEE Standard Glossary of Software Engineering Terminology 610.12-1990]

- **test condition**: An item or event of a component or system that could be verified by one or more test cases, e.g., a function, transaction, feature, quality attribute, or structural element.[according to ISTQB]

Test adequacy (remember)

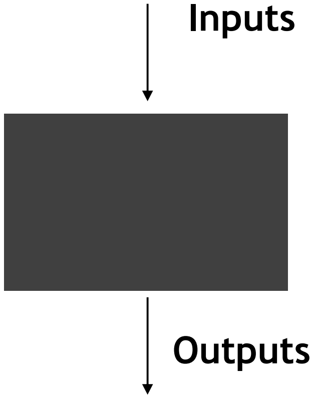
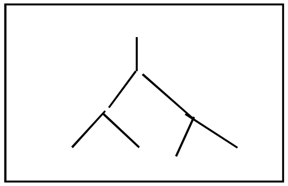
- Adequacy criteria - Criteria to decide if a given test suite is adequate, i.e., to give us “enough” confidence that “most” of the defects are revealed
  - Used in the evaluation and in the design/selection of test cases
  - In practice, reduced to coverage criteria

Coverage criteria (remember)

- Coverage criteria
  - Requirements/specification coverage (black-box)
    - At least one test case for each requirement/specification statement
  - Code coverage (white-box)
    - Control flow coverage (statement, decision, MC/DC coverage …)
    - Data flow coverage
  - Model coverage
    - State-transition coverage
    - Use case and scenario coverage
  - Fault coverage

See also: “Software Unit Test Coverage and Adequacy”, Hong Zhu et al, ACM Computing Surveys, December 1997

Test case design strategies and techniques

Strategy	Tester's View	Knowledge sources	Techniques / Methods
Black-box testing (not code-based) (sometimes called functional testing)		Requirements document Specifications User manual Models Domain knowledge Defect analysis data Intuition Experience	Equivalence class partitioning Boundary value analysis Cause effect graphing Pairwise testing Error guessing Random testing State-transition testing Scenario-based testing
White-box testing (also called code-based or structural testing)		Program code Control flow graphs Data flow graphs Cyclomatic complexity High-level design Detailed design	Control flow testing/coverage: •Statement coverage •Branch (or decision) coverage •Condition coverage •Branch and condition coverage •Modified condition/decision coverage •Multiple condition coverage •Independent path coverage •Path coverage •LCSAJ coverage Data flow testing/coverage Class testing/coverage Mutation testing

(adapted from: I. Burnstein, pg.65)

Test automation

- Automatic test case generation
  - Automatic generation of test inputs is easier than the automatic generation of test outputs (usually requires a formal specification)
  - May reduce test development costs
  - Usually, lower capability to find failures per test case, but overall capability may be higher because more test cases can be generated (than manually)
- Automatic test case execution
  - Requires that test cases are written/converted in/into some executable language
  - Increases test development costs (coding) but practically eliminates test (re)execution costs, which is particularly important in regression testing
  - Unit testing frameworks and tools for API testing; Capture/replay tools for GUI testing
  - Performance testing tools

Agenda

- Introduction
- Black box testing techniques
- Exercise

Black-box testing

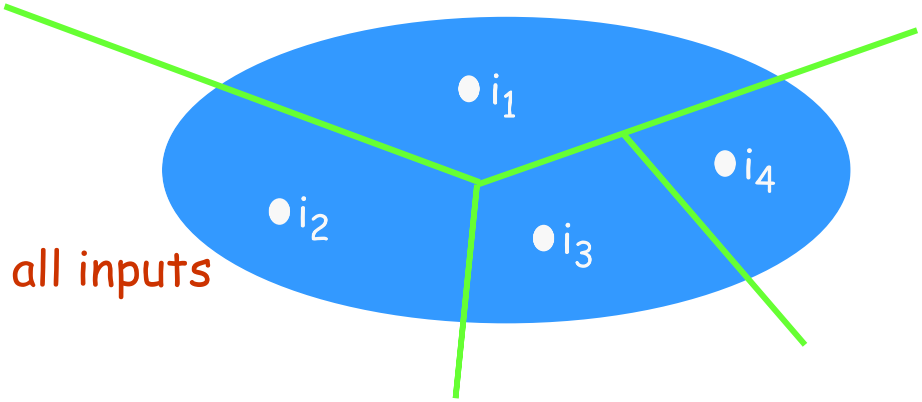
- Equivalence class (or domain) partitioning
- Boundary-value analysis
- Cause-effect graphing (or decision table)
- Pairwise testing
- Error guessing
- Risk based testing
- Testing for race conditions
- Random testing
- Requirements based testing
- Model-based testing (MBT)
- …

Equivalence class partitioning

Divide all possible inputs into classes (partitions) such that :

- There is a finite number of input equivalence classes
- You may reasonably assume that
  - the program behaves analogously for inputs in the same class
  - one test with a representative value from a class is sufficient
  - if the representative detects a defect
    then other class members would detect the same defect

(Can also be applied to outputs)

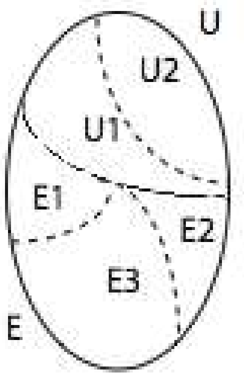


Equivalence class partitioning

Faults targeted

- The entire set of inputs to any application can be divided into at least two subsets: one containing all the expected, or legal, inputs (E) and the other containing all unexpected, or illegal, inputs (U).

- Each of the two subsets, can be further subdivided into subsets on which the application is required to behave differently (e.g., E1, E2, E3, and U1, U2).



© Aditya P. Mathur 2006

Sistematic procedure for equivalence partitioning (1)

- **1. Identify the input domain:** Read the requirements carefully and identify all input and output variables, their types, and any conditions associated with their use.
  - Environment variables, such as class variables used in the method under test and environment variables in Unix, Windows, and other operating systems, also serve as input variables. Given the set of values each variable can assume, an approximation to the input domain is the product of these sets.
- **2. Equivalence classing:** Partition the set of values of each variable into disjoint subsets. Each subset is an equivalence class. Together, the equivalence classes based on an input variable partition the input domain. Partitioning the input domain using values of one variable, is done based on the expected behavior of the program.
  - Values for which the program is expected to behave in the "same way" are grouped together. Note that "same way" needs to be defined by the tester.

Sistematic procedure for equivalence partitioning (2)

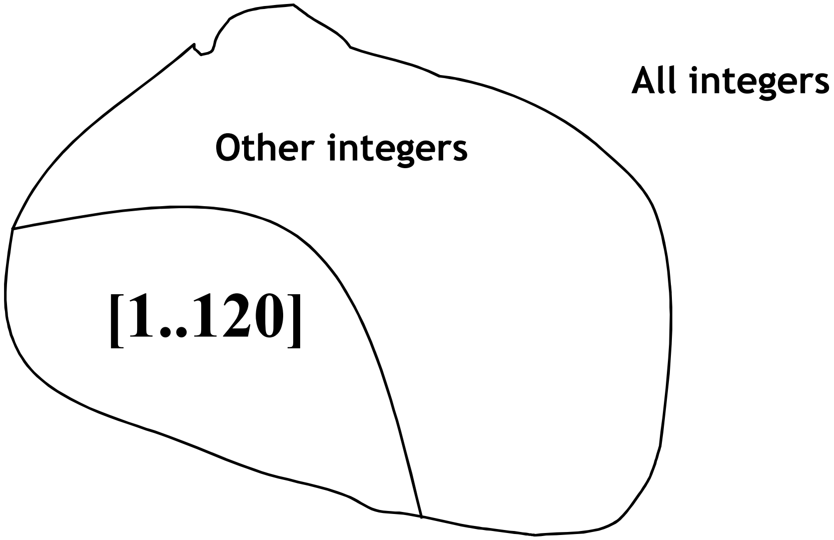
- **3. Combine equivalence classes:** This step is usually omitted and the equivalence classes defined for each variable are directly used to select test cases. However, by not combining the equivalence classes, one misses the opportunity to generate useful tests.
    - The equivalence classes are combined using the multidimensional partitioning approach described earlier.
- **4. Identify infeasible equivalence classes:** An infeasible equivalence class is one that contains a combination of input data that cannot be generated during test. Such an equivalence class might arise due to several reasons.
    - For example, suppose that an application is tested via its GUI, i.e., data is input using commands available in the GUI. The GUI might disallow invalid inputs by offering a palette of valid inputs only. There might also be constraints in the requirements that render certain equivalence infeasible.

Equivalence class partitioning

- Identify input equivalence classes
  - Based on conditions on inputs/outputs in specification/description
  - Both valid and invalid input equivalence classes
  - Based on heuristics and experience, E.g.,:
    - “input x in [1..10]” → classes: $x < 1$, $1 \leq x \leq 10$, $x > 10$
    - “enumeration A, B, C” → classes: A, B, C, not$\{A,B,C\}$
    - “input integer n” → classes: n not an integer, n<min, min≤n<0, 0≤n≤max, n>max
- Define one (or a couple of) test cases for each class
  - Test cases that cover valid classes (1 test case for 1 or more valid classes)
  - Test cases that cover at most one invalid class (1 test case for 1 invalid class)
  - Usually useful to test for 0/null/empty and other special cases
- Combine equivalent classes
  - Combine valid with invalid values to increase the capability of detecting missing code
- Identify infeasible classes

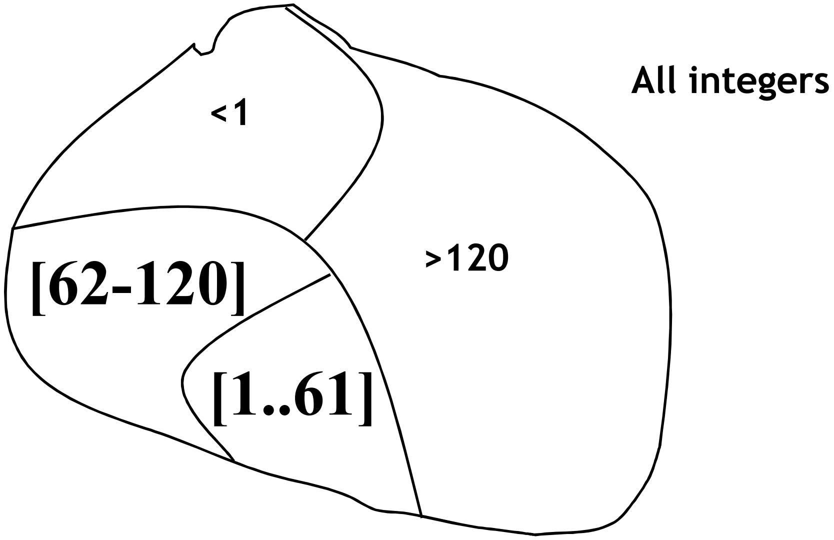
Equivalence class partitioning - Example 1

- Consider an application A that takes an integer denoted by age as input. Let us suppose that the only legal values of age are in the range [1..120]. The set of input values is now divided into a set E containing all integers in the range [1..120] and a set U containing the remaining integers.



Equivalence class partitioning - Example 1

- Further, assume that the application is required to process all values in the range [1..61] in accordance with requirement R1 and those in the range [62..120] according to requirement R2. Thus E is further subdivided into two regions depending on the expected behavior.
- Similarly, it is expected that all invalid inputs less than or equal to 1 are to be treated in one way while all greater than 120 are to be treated differently. This leads to a subdivision of U into two categories.



© Aditya P. Mathur 2006

Equivalence class partitioning - Example 1

- Tests selected using the equivalence partitioning technique aim at targeting faults in the application under test with respect to inputs in any of the four regions, i.e., two regions containing expected inputs and two regions containing the unexpected inputs.

- It is expected that any single test selected from the range [1..61] will reveal any fault with respect to R1. Similarly, any test selected from the region [62..120] will reveal any fault with respect to R2. A similar expectation applies to the two regions containing the unexpected inputs.

Equivalence class partitioning - Example 2

Test a function that calculates the absolute value of an integer *x*

- Equivalence classes :

Criteria	Valid eq. classes	Invalid eq. classes
nr of inputs	1 (1)	0 (2), > 1 (3)
input type	integer (4)	non-integer (5)
particular x	< 0 (6), >= 0 (7)	

- Test cases :

x = -10 (1,4,6)

x = 100 (1,4,7)

x = (2)

x = 10 20 (3)

x = “XYZ” (5)

Equivalence class partitioning - Example 3

- Test a program that computes the *sum* of the first *N* integers as long as this *sum* is less than *maxint*. Otherwise an error should be reported. If *N* is negative, then it takes the absolute value *N*.

- Formally:
  Given integer inputs *N* and *maxint* compute result :

$$\text{result} = \sum_{K=0}^{|N|} k \quad \text{if this} <= \text{maxint, error otherwise}$$

Equivalence class partitioning - Example 3

- Equivalence classes:

Condition	Valid eq. classes	Invalid eq. classes
nr of inputs	2	< 2, > 2
type of input	int int	int no-int, no-int int, no-int no-int
abs(N)	$N < 0$, $N \geq 0$	
maxint	$\sum k \leq$ maxint, $\sum k >$ maxint	

- Test Cases :

	maxint	N	result
Valid	100	10	55
	100	-10	55
	10	10	error
Invalid	10	-	error
	10 20	30	error
	"XYZ"	10	error
	100	9.1E4	error

Equivalence classes based on program output

- In some cases the equivalence classes are based on the output generated by the program. For example, suppose that a program outputs an integer.

- It is worth asking: “Does the program ever generate a 0? What are the maximum and minimum possible values of the output?”

- These two questions lead to the two following equivalence classes based on outputs:
  - E1: Output value v is 0.
  - E2: Output value v is the maximum possible.
  - E3: Output value v is the minimum possible.
  - E4: All other output values.

- Based on the output equivalence classes one may now derive equivalence classes for the inputs. Thus each of the four classes given above might lead to one equivalence class consisting of inputs.

Equivalence classes for variables: range

Eq. Classes	Example	
	Constraints	Classes
One class with values inside the range and two with values outside the range.	**speed $\in$[60..90]**	**{50}, {75}, {92}**
	area: float area$\geq$0.0	**{{-1.0}, {15.52}}**
	age: int	**{{-1}, {56}, {132}}**
	letter: char	**{{J}, {3}}**

Equivalence classes for variables: strings

Eq. Classes	Example	
	Constraints	Classes
At least one containing all legal strings and one all illegal strings based on any constraints.	firstname: string	{{ε}, {Sue}, {Loooong Name}}

Equivalence classes for variables: enumeration

Eq. Classes	Example	
	Constraints	**Classes**
Each value in a separate class	autocolor:{red, blue, green}	{{red,} {blue}, {green}}
	up:boolean	{{true}, {false}}

Equivalence classes for variables: arrays

Eq. Classes	Example	
	Constraints	**Classes**
One class containing all legal arrays, one containing the empty array, and one containing a larger than expected array.	int [ ] aName: new int[3];	{[ ]}, {[-10, 20]}, {[-9, 0, 12, 15]}

Equivalence classes for variables: compound data types

- Arrays in Java and records, or structures, in C++, are compound types. Such input types may arise while testing components of an application such as a function or an object.
- While generating equivalence classes for such inputs, one must consider legal and illegal values for each component of the structure.

```
struct transcript{
            string fName; // First name.
            string lName; //  Last name.
            string cTitle [200]; // Course titles.
            char grades [200]; // Letter grades corresponding
                                   to course titles.
}
```

Partitioning

- Unidimensional partitioning
  - One way to partition the input domain is to consider one input variable at a time. Thus each input variable leads to a partition of the input domain. We refer to this style of partitioning as unidimensional equivalence partitioning or simply unidimensional partitioning.

  This type of partitioning is commonly used.

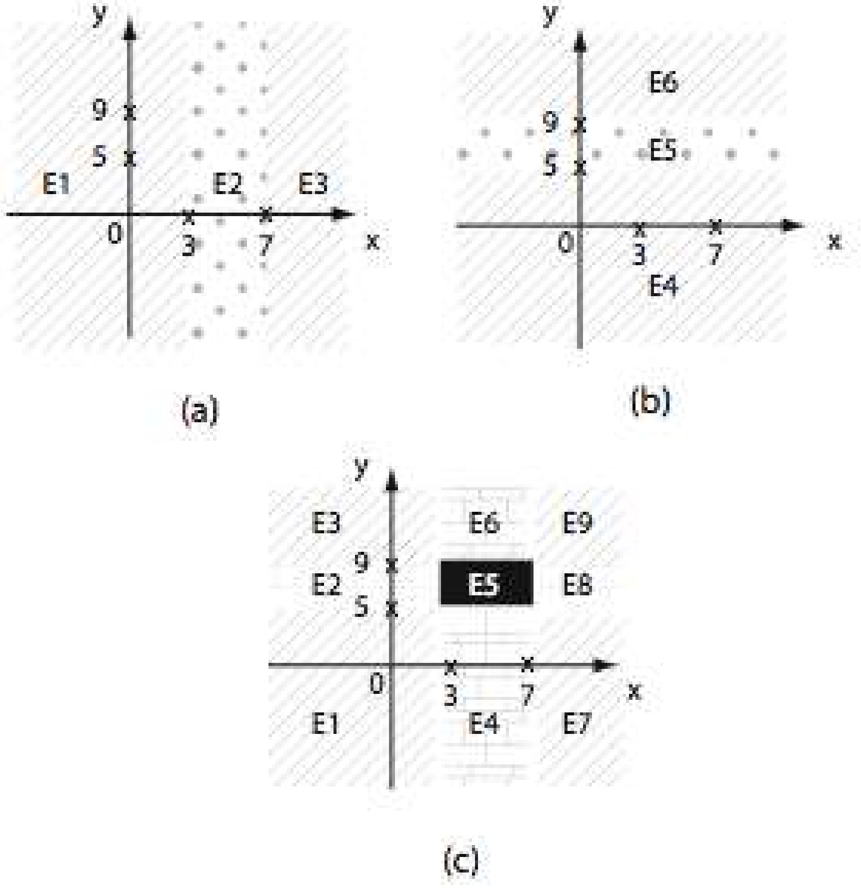
- Multidimensional partitioning
  - Another way is to consider the input domain *I* as the set product of the input variables and define a relation on *I*. This procedure creates one partition consisting of several equivalence classes. We refer to this method as multidimensional equivalence partitioning or simply multidimensional partitioning.
  - Multidimensional partitioning leads to a large number of equivalence classes that are difficult to manage manually. Many classes so created might be infeasible. Nevertheless, equivalence classes so created offer an increased variety of tests as is illustrated in the next section.

Partitioning Example (1)

- Consider an application that requires two integer inputs *x* and *y*. Each of these inputs is expected to lie in the following ranges: $3 \le x \le 7$ and $5 \le y \le 9$.
- For unidimensional partitioning we apply the partitioning guidelines to *x* and *y* individually. This leads to the following six equivalence classes.
- E1: $x<3$ E2: $3 \le x \le 7$ E3: $x>7$ (y ignored)
- E4: $y<5$ E5: $5 \le y \le 9$ E6: $y>9$ (x ignored)
- For multidimensional partitioning we consider the input domain to be the set product X x Y. This leads to 9 equivalence classes.

Partitioning Example (2)

- 9 equivalent classes
  - E1: x<3, y<5
  - E3: x<3, y>9
  - E2: x<3, 5≤y≤9
  - E4: 3≤x≤7, y<5
  - E5: 3≤x≤7, 5≤y≤9
  - E6: 3≤x≤7, y>9
  - E7: x>7, y<5
  - E8: x>7, 5≤y≤9
  - E9: x>7, y>9



(a)

(b)

(c)

Boundary value analysis

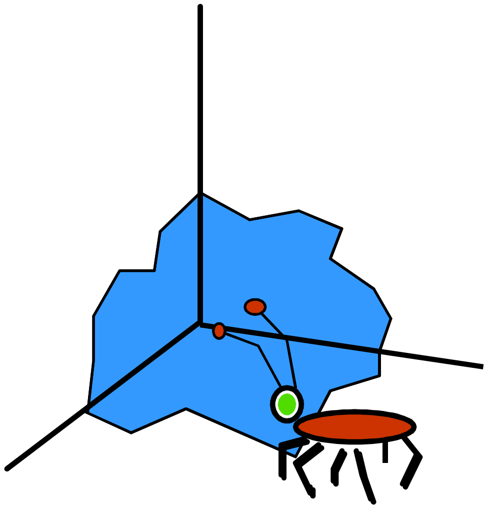
Based on experience / heuristics :

- Testing boundary conditions of equivalence classes is more effective, i.e., values directly on, above, and beneath edges of classes
  - If a system behaves correctly at boundary values, than it probably will work correctly at "middle" values
- Choose input boundary values as tests in input classes instead of, or additional to arbitrary values
- Choose also inputs that invoke output boundary values (values on the boundary of output classes)
- Example strategy as extension of equivalence class partitioning:
  - choose one (or more) arbitrary value(s) in each equivalent class
  - choose values exactly on lower and upper boundaries of equivalent classes
  - choose values immediately below and above each boundary (if applicable)

Boundary value analysis

“Bugs lurk in corners and congregate at boundaries.”

[Boris Beizer, "Software testing techniques"]



Boundary value analysis
Example 1

Test a function for calculation of absolute value of an integer

- Valid equivalence classes :

Condition	Valid eq. classes	Invalid eq. Classes
particular abs	< 0, >= 0	

- Test cases :

class x < 0, arbitrary value:	x = -10
class x >= 0, arbitrary value	x = 100
classes x < 0, x >= 0, on boundary :	x = 0
classes x < 0, x >= 0, below and above:	x = -1, x = 1

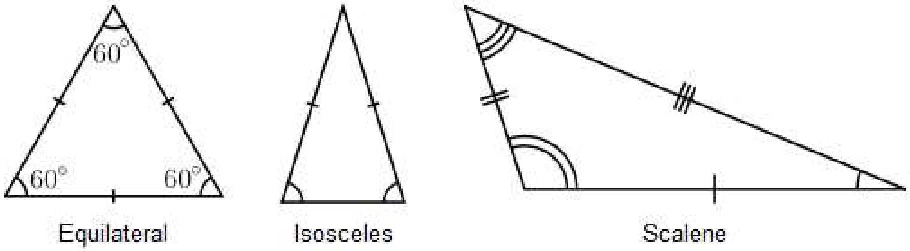
Boundary value analysis
A self-assessment test 1 [Myers]

- "A program reads three integer values. The three values are interpreted as representing the lengths of the sides of a triangle. The program prints a message that states whether the triangle is scalene (all lengths are different), isosceles (two lengths are equal), or equilateral (all lengths are equal)."

Write a set of test cases to test this program.

Inputs: l_1, l_2, l_3 , integer, $l_i > 0$, $l_i < l_j + l_k$

Output: error, scalene, isosceles or equilateral

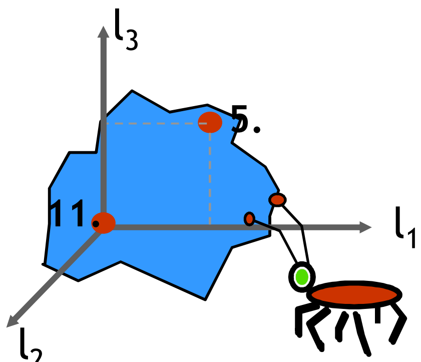


Boundary value analysis
A self-assessment test 1 [Myers]

Test cases for:

valid inputs:

1. valid scalene triangle ?
2. valid equilateral triangle ?
3. valid isosceles triangle ?
4. 3 permutations of previous ?



“Bugs lurk in corners and congregate at boundaries.”

invalid inputs:

5. side = 0 ? (boundary "plane")
6. negative side ?
7. one side is sum of others ? (boundary)
8. 3 permutations of previous ?
9. one side larger than sum of others ?
10. 3 permutations of previous ?
11. all sides = 0 ? (boundary "corner")
12. non-integer input ?
13. wrong number of values ?

Boundary value analysis
Example 2

- Given inputs maxint and N compute result :

$$\text{result} = \sum_{K=0}^{|N|} k \quad \text{if this} <= \text{maxint}, \quad \text{error otherwise}$$

- Valid equivalence classes :

condition	valid eq. classes	boundary values.
abs(N)	$N < 0$, $N \geq 0$	N = (-2), -1, 0, 1
maxint	$\sum k \leq$ maxint,	$\sum k$ = maxint-1,
	$\sum k >$ maxint	maxint,
		maxint+1,
		(maxint+2)

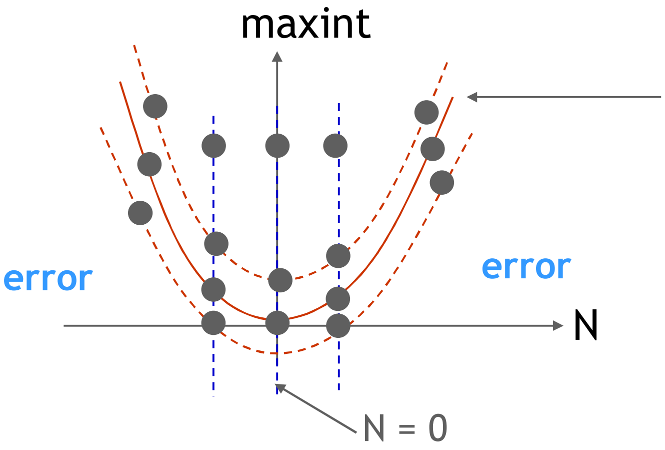
Boundary value analysis
Example 2

- Test Cases :

maxint	*N*	result
55	10	55
54	10	error
56	10	55
0	0	0

maxint	*N*	result
100	0	0
100	-1	1
100	1	1
…	…	…

- How to combine the boundary conditions of different inputs ? Take all possible boundary combinations ? This may blow up ……



maxint = 0+1+2+...+|N|

Boundary value analysis
Example 3: search routine specification

```
procedure Search (Key : ELEM ; T: ELEM_ARRAY;
      Found : out BOOLEAN; L: out ELEM_INDEX) ;

Pre-condition
            -- the array has at least one element
            T'FIRST <= T'LAST
Post-condition
            -- the element is found and is referenced by L
            ( Found and T (L) = Key)
or
            -- the element is not in the array
            ( not Found and
            not (exists i, T'FIRST >= i <= T'LAST, T (i) = Key ))
```

(source: Ian Sommerville)

Boundary value analysis
Example 3 - input partitions

- P1 - Inputs which conform to the pre-conditions (valid)
  - array with 1 value (boundary)
  - array with more than one value (different size from test case to test case)
- P2 - Inputs where a pre-condition does not hold (invalid)
  - array with zero length
- P3 - Inputs where the key element is a member of the array
  - first, last and middle positions in different test cases
- P4 - Inputs where the key element is not a member of the array

Boundary value analysis

Example 3 - test cases (valid cases only)

Array	**Element**
Single value	In sequence
Single value	Not in sequence
More than 1 value	First element in sequence
More than 1 value	Last element in sequence
More than 1 value	Middle element in sequence
More than 1 value	Not in sequence

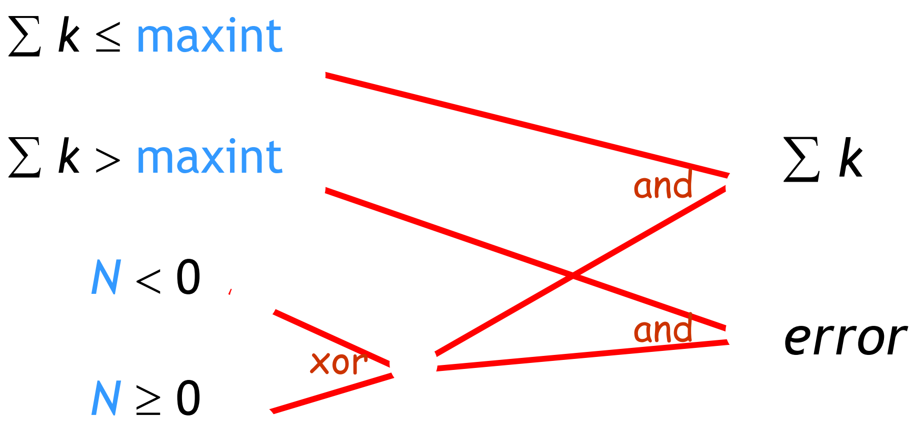
Input sequence (T)	**Key** (Key)	**Output** (Found, L)
17	17	true, 1
17	0	false, ??
17, 29, 21, 23	17	true, 1
41, 18, 9, 31, 30, 16, 45	45	true, 7
17, 18, 21, 23, 29, 41, 38	23	true, 4
21, 23, 29, 33, 38	25	false, ??

Cause-effect graphing

- Black-box technique to analyze combinations of input conditions
- Identify causes and effects in specification
  - causes ↓ inputs / initial state conditions
  - effects ↓ outputs / final state conditions
- Make Boolean Graph linking causes and effects
- Annotate impossible combinations of causes and effects
- Develop decision table from graph with in each column a particular combination of inputs and outputs
- Transform each column into test case

Cause-effect graphing

Example 2



$\sum k \le \text{maxint}$

$\sum k > \text{maxint}$

$N < 0$

$N \ge 0$

$\sum k$

error

Decision table

("truth table")

Each entry in de decision table is a 0 or a 1 depending on whether or not the corresponding condition is false or true

causes	$\sum k \le \text{maxint}$	1	1	0	0
(inputs)	$\sum k > \text{maxint}$	0	0	1	1
	$N < 0$	1	0	1	0
	$N \ge 0$	0	1	0	1
effects	$\sum k$	1	1	0	0
(outputs)	*error*	0	0	1	1

Cause-effect graphing

- Systematic method for generating test cases representing combinations of conditions
- Differently from eq. class partitioning, we define a test case for each possible combination of conditions
- Combinatorial explosion of number of possible combinations
  - In the worst case, if *n* causes are related to an effect *e*, then the maximum number of combinations that bring *e* to a *1-state* is 2^n.

Pairwise testing

- **pairwise testing:** A black box test design technique in which test cases are designed to execute all possible discrete combinations of each pair of input parameters.

- The number of pairwise test cases will be O(*mn*), where *m* and *n* are the number of possibilities for each of the two parameters with the most choices.

$$O(mn) = Max(X) \text{ x } Max(X \backslash Max(X))$$

and X is the set with the numbers of possibilities for every parameters

Pairwise testing

Parameter Name	Value 1	Value 2	Value 3	Value 4
Enabled	True	False	*	*
Choice Type	1	2	3	*
Category	a	b	c	d

X = {2,3,4}

O(*mn*) = 4 x 3 = 12

Enabled	Choice Type	Category
True	3	a
True	1	d
False	1	c
False	2	d
True	2	c
False	2	a
False	1	a
False	3	b
True	2	b
True	3	d
False	3	c
True	1	b

Error guessing

- Just ‘guess’ where the errors are ……
- Intuition and experience of tester
- Ad hoc, not really a technique
- But can be quite effective
- Strategy:
  - Make a list of possible errors or error-prone situations (often related to boundary conditions)
  - Write test cases based on this list

Risk based testing

- **Risk-based testing** (RBT) is a type of software testing that prioritizes the features and functions to be tested based on priority/importance and likelihood or impact of failure. More sophisticated ‘error guessing’
- Try to identify critical parts of program (high risk code sections):
  - parts with unclear specifications
  - developed by junior programmer while his wife was pregnant ……
  - complex code :
    measure code complexity - tools available (McGabe, Logiscope,…)
- High-risk code will be more thoroughly tested
  (or be rewritten immediately ……)

Testing for race conditions

- Also called bad timing and concurrency problems
- Problems that occur in multitasking systems (with multiple threads or processes)
- A kind of boundary analysis related to the dynamic views of a system (state-transition view and process-communication view)
- Examples of situations that may expose race conditions:
  - problems with shared resources:
    - saving and loading the same document at the same time with different programs
    - sharing the same printer, communications port or other peripheral
    - using different programs (or instances of a program) to simultaneously access a common database
  - problems with interruptions:
    - pressing keys or sending mouse clicks while the software is loading or changing states
  - other problems:
    - shutting down or starting two or more instances of the software at the same time
- Knowledge used: dynamic models (state-transition models, process models)

[source: Ron Patton]

Random testing

- Input values are randomly generated
- Do you know that a monkey using a piano keyboard could play a Vivaldi opera? Could the same monkey, using your application, discovery defects?
- Two kinds of tools
  - **Dumb monkeys** – low IQ; they can't recognize an error when they see one
  - **Smart monkeys** – generate inputs with some knowledge to reflect expected usage; get knowledge from state table or model of the AUT.
- Microsoft says that 10 to 20% of the bugs in Microsoft projects are found by these tools

Random testing

- Advantages
  - Good for finding system crashes
  - Particularly adequate for performance testing (it's not necessary to check the correctness of outputs)
  - No effort in generating test cases
  - Independent of updates
  - Increase confidence on the software when running several hours without finding errors
  - “Easy” to implement
- Disadvantages
  - Not good for finding other kinds of errors
  - Difficult to reproduce the errors (repeat test cases / sequence of inputs)
  - Unpredictable
  - May not cover special cases that are discovered by "manual" techniques

Deriving test cases from requirements and use cases

- Particularly adequate for system and acceptance testing
- From requirements:
  - You have a list of requirements
  - Define at least one test case for each requirement
  - Build and maintain a (tests to requirements) traceability matrix
- From use cases:
  - You have use cases that capture functional requirements
  - Each use case is described by one or more *normal* flow of events and zero or more *exceptional* flow of events
  - Define at least one test case for each flow of events (also called *scenario*)
  - Build and maintain a (tests to use cases) traceability matrix

State-transition testing

- Construct a state-transition model (state machine view) of the item to be tested (from the perspective of a user/client). E.g., with a state diagram in UML
- Define test cases to exercise all states and all transitions between states
  - Usually, not all possible paths (sequences of states and transitions), because of combinatorial explosion
  - Each test case describes a sequence of inputs and outputs (including input and output states), and may cover several states and transitions
  - Also test to fail – with unexpected inputs for a particular state
- We will talk about this techniques in more detail in the following lectures

Black box testing: Which One ?

- Black box testing techniques :
  - Equivalence partitioning
  - Boundary value analysis
  - Cause-effect graphing
  - Error guessing
  - …………
- Which one to use ?
  - None of them is complete
  - All are based on some kind of heuristics
  - They are complementary

Black box testing: which one ?

- Always use a combination of techniques
  - When a formal specification is available try to use it
  - Identify valid and invalid input equivalence classes
  - Identify output equivalence classes
  - Apply boundary value analysis on valid equivalence classes
  - Guess about possible errors
  - Cause-effect graphing for linking inputs and outputs

Index

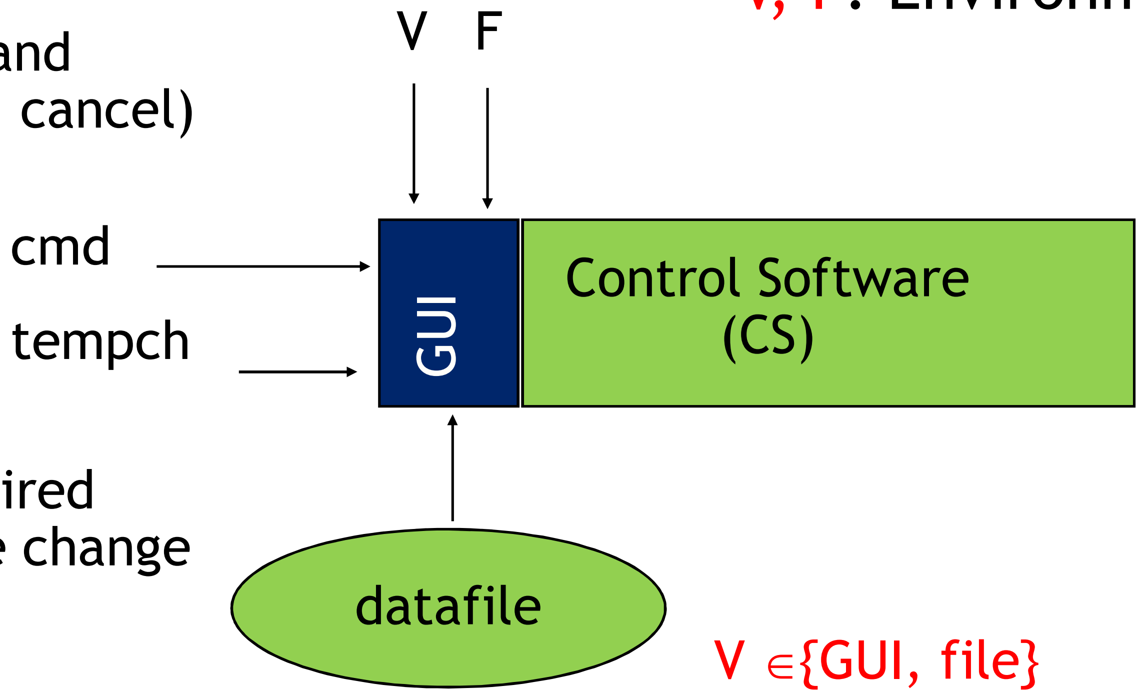
- Introduction
- Black box testing techniques
- Exercise

Exercise

- The control software of BCS, abbreviated as CS, allows a human operator to give one of three commands (*cmd*): change the boiler temperature (*temp*), shut down the boiler (*shut*), and cancel the request (*cancel*).
- Command temp causes CS to ask the operator to enter the amount by which the temperature is to be changed (*tempch*). Values of *tempch* are in the range [-10..10] in increments of 5 degrees Fahrenheit. An temperature change of 0 is not an option.
- BCS examines variable *V*. If *V* is set to *GUI*, the operator is asked to enter one of the three commands via a *GUI*. However, if *V* is set to *file*, BCS obtains the command from a command file.
- The command file may contain any one of the three commands, together with the value of the temperature to be changed if the command is *temp*. The file name is obtained from variable *F*.

Exercise

cmd: command
(temp, shut, cancel)



V, F: Environment variables

tempch: desired
temperature change
(-10..10)

V ∈{GUI, file}

F: file name if V is set to “file.”

Exercise

- Identify input domain
- Identify equivalence classes
- Combine equivalence classes
- Discard infeasible equivalence classes
- Generate sample tests for BCS from the remaining feasible equivalence classes

Identify input domain

Variable	Kind	Type	Value(s)
V	Environment	Enumerated	{GUI, file}
F	Environment	String	A file name
cmd	Input via GUI or file	Enumerated	{temp,cancel,shut}
tempch	Input via GUI or file	Enumerated	{-10,-5,5,10}

S = V x F x cmd x tempch

Equivalence class partition

Variable	Partition
V	{{GUI},{file},{undefined}}
F	f_valid, f_invalid
cmd	{{temp},{cancel},{shut},{c_invalid}}
tempch	{{-10},{-5},{5},{10},{t_invalid}}

Combine equivalence classes

- Variables V, F, cmd and tempch have been partitioned into 3, 2, 4 and 2 susets, respectively
- Set products of these four variables leads to a total of 3x2x4x5=120

Discard infeasable classes

- The amount by which the boiler temperature is to be changed is needed only when the operator selects **temp** for **cmd**, Thus all equivalent classes that match the following template are infeasible
  - {(V, F, {cancel,shut,c_invalid}, t_valid U t_invalid)} =
- GUI does not allow invalid values of temperature change to be input. Two more equivalent classes infeasible
  - {(GUI, F, temp, t_invalid)} =

Discard infeasable classes

- Carefully designed application might not ask for the values of tempch when **V=file** and **F** contains a file name that does not exist
  - {(file, f_invalid, temp, t_valid U t_invalid)} =
- Application will not allow values of **tempch** to be input when **V** is undefined
  - {(undefined, -, temp, t_valid U t_invalid)} =
- Discard 90+2+5+5=102 equivalence classes
- 18 equivalent classes remain

Result

{(GUI, f_valid, temp, t_valid)}	= 4
{(GUI, f_invalid, temp, t_valid)}	= 4
{(GUI, –, cancel, NA)}	= 2
{(file, f_valid, temp, t_valid U t_invalid)}	= 5
{(file, f_valid, shut, NA)}	= 1
{(file, f_invalid, NA, NA)}	= 1
{(undefined, NA, NA, NA)}	= 1
	total = 18

‘–’ means that data can be input but is not used by the software

‘NA’ means that data cannot be input to the control software

References

- Practical Software Testing, Ilene Burnstein, Springer-Verlag, 2003
- Software Testing, Ron Patton, SAMS, 2001
- The Art of Software Testing, Glenford J. Myers, Wiley & Sons, 1979 (Chapter 4 - Test Case Design)
  - Classical
- Software testing techniques, Boris Beizer, Van Nostrand Reinhold, 2nd Ed, 1990
  - Bible
- Foundations of Software Testing, 1st edition, by Aditya P. Mathur, Pearson Education, 2008
- Testing Computer Software, 2nd Edition, Cem Kaner, Jack Falk, Hung Nguyen, John Wiley & Sons, 1999
  - Practical, black box only
- Software Engineering, Ian Sommerville, 6th Edition, Addison-Wesley, 2000
- Test Driven Development, Kent Beck, Addison Wesley, 2002
- http://www.swebok.org/
  - Guide to the Software Engineering Body of Knowledge (SWEBOK), IEEE Computer Society
- http://www.mccabe.com/iq_research_metrics.htm
- What Is a Good Test Case?, Cem Kaner, Florida Institute of Tecnology, 2003
- Software Unit Test Coverage and Adequacy, Hong Zhu et al, ACM Computing Surveys, December 1997