UNIT – 1

UNIT – 1. INTRODUCTION

1. PURPOSE OF TESTING:

- Testing consumes atleast half of the time and work required to produce a functional program.
- MYTH: Good programmers write code without bugs. (Its wrong!!!)
- History says that even well written programs still have 1-3 bugs per hundred statements.
- **Productivity and Quality in software:**
  - In production of comsumer goods and other products, every manufacturing stage is subjected to quality control and testing from component to final stage.
  - If flaws are discovered at any stage, the product is either discarded or cycled back for rework and correction.
  - Productivity is measured by the sum of the costs of the material, the rework, and the discarded componenets, and the cost of quality assurance and testing.
  - There is a trade off between quality assurance costs and manufacturing costs: If sufficient time is not spent in quality assurance, the reject rate will be high and so will be the net cost. If inspection is good and all errors are caught as they occur, inspection costs will dominate, and again the net cost will suffer.
  - Testing and Quality assurance costs for 'manufactured' items can be as low as 2% in consumer products or as high as 80% in products such as space-ships, nuclear reactors, and aircrafts, where failures threaten life. Where as the manufacturing cost of a software is trivial.
  - The biggest part of software cost is the cost of bugs: the cost of detecting them, the cost of correcting them, the cost of designing tests that discover them, and the cost of running those tests.
  - For software, quality and productivity are indistinguishable because the cost of a software copy is trivial.
- Testing and Test Design are parts of quality assurance should also focus on bug prevention. *A prevented bug is better than a detected and corrected bug.*
- Phases in a tester's mental life can be categorised into the following 5 phases:
  1. **Phase 0: (Until 1956: Debugging Oriented)** There is no difference between testing and debugging. Phase 0 thinking was the norm in early days of software development till testing emerged as a discipline.
  2. **Phase 1: (1957-1978: Demonstration Oriented)** The purpose of testing here is to show that software works. Highlighted during the late 1970s. This failed because the probability of showing that software works 'decreases' as testing increases. *i.e.* The more you test, the more likely you'll find a bug.
  3. **Phase 2: (1979-1982: Destruction Oriented)** The purpose of testing is to show that software doesnt work. This also failed because the software will never get

released as you will find one bug or the other. Also, a bug corrected may also lead to another bug.

4. **Phase 3: (1983-1987: Evaluation Oriented)** The purpose of testing is not to prove anything but to reduce the perceived risk of not working to an acceptable value (Statistical Quality Control). Notion is that testing does improve the product to the extent that testing catches bugs and to the extent that those bugs are fixed. The product is released when the confidence on that product is high enough. (Note: This is applied to large software products with millions of code and years of use.)
5. **Phase 4: (1988-2000: Prevention Oriented)** Testability is the factor considered here. One reason is to reduce the labour of testing. Other reason is to check the testable and non-testable code. Testable code has fewer bugs than the code that's hard to test. Identifying the testing techniques to test the code is the main key here.

Test Design: We know that the software code must be designed and tested, but many appear to be unaware that tests themselves must be designed and tested. Tests should be properly designed and tested before applying it to the acutal code.

Testing is'nt everything: There are approaches other than testing to create better software. Methods other than testing include:

6. **Inspection Methods:** Methods like walkthroughs, deskchecking, formal inspections and code reading appear to be as effective as testing but the bugs caught donot completely overlap.
7. **Design Style:** While designing the software itself, adopting stylistic objectives such as testability, openness and clarity can do much to prevent bugs.
8. **Static Analysis Methods:** Includes formal analysis of source code during compilation. In earlier days, it is a routine job of the programmer to do that. Now, the compilers have taken over that job.
9. **Languages:** The source language can help reduce certain kinds of bugs. Programmers find new bugs while using new languages.
10. **Development Methodologies and Development Environment:** The development process and the environment in which that methodology is embedded can prevent many kinds of bugs.

2. DICHOTOMIES:

- **Testing Versus Debugging:** Many people consider both as same. Purpose of testing is to show that a program has bugs. The purpose of testing is to find the error or misconception that led to the program's failure and to design and implement the program changes that correct the error.
- Debugging usually follows testing, but they differ as to goals, methods and most important psychology. The below tab le shows few important differences between testing and debugging.

Testing	Debugging
Testing starts with known conditions, uses predefined procedures and has predictable outcomes.	Debugging starts from possibly unknown intial conditions and the end can not be predicted except statistically.
Testing can and should be planned, designed and scheduled.	Procedure and duration of debugging cannot be so constrained.
Testing is a demonstration of error or apparent correctness.	Debugging is a deductive process.
Testing proves a programmer's failure.	Debugging is the programmer's vindication (Justification).
Testing, as executes, should strive to be predictable, dull, constrained, rigid and inhuman.	Debugging demands intutive leaps, experimentation and freedom.
Much testing can be done without design knowledge.	Debugging is impossible without detailed design knowledge.
Testing can often be done by an outsider.	Debugging must be done by an insider.
Much of test execution and design can be automated.	Automated debugging is still a dream.

- **Function Versus Structure:** Tests can be designed from a functional or a structural point of view. In **functional testing**, the program or system is treated as a blackbox. It is subjected to inputs, and its outputs are verified for conformance to specified behaviour. Functional testing takes the user point of view- bother about functionality and features and not the program's implementation. **Structural testing** does look at the implementation details. Things such as programming style, control method, source language, database design, and coding details dominate structural testing.
- Both Structural and functional tests are useful, both have limitations, and both target different kinds of bugs. Functional tets can detect all bugs but would take infinite time to do so. Structural tests are inherently finite but cannot detect all errors even if completely executed.
- **Designer Versus Tester:** Test designer is the person who designs the tests where as the tester is the one actually tests the code. During functional testing, the designer and tester are probably different persons. During unit testing, the tester and the programmer merge into one person.
- Tests designed and executed by the software designers are by nature biased towards structural consideration and therefore suffer the limitations of structural testing.
- **Modularity Versus Efficiency:** A module is a discrete, well-defined, small component of a system. Smaller the modules, difficult to integrate; larger the modules, difficult to

understand. Both tests and systems can be modular. Testing can and should likewise be organised into modular components. Small, independent test cases can be designed to test independent modules.

- **Small Versus Large:** Programming in large means constructing programs that consists of many components written by many different programmers. Programming in the small is what we do for ourselves in the privacy of our own offices. Qualitative and Quantitative changes occur with size and so must testing methods and quality criteria.
- **Builder Versus Buyer:** Most software is written and used by the same organization. Unfortunately, this situation is dishonest because it clouds accountability. If there is no separation between builder and buyer, there can be no accountability.
- The different roles / users in a system include:
    1. **Builder:** Who designs the system and is accountable to the buyer.
    2. **Buyer:** Who pays for the system in the hope of profits from providing services.
    3. **User:** Ultimate beneficiary or victim of the system. The user's interests are also guarded by.
    4. **Tester:** Who is dedicated to the builder's destruction.
    5. **Operator:** Who has to live with the builders' mistakes, the buyers' murky (unclear) specifications, testers' oversights and the users' complaints.

3. MODEL FOR TESTING:

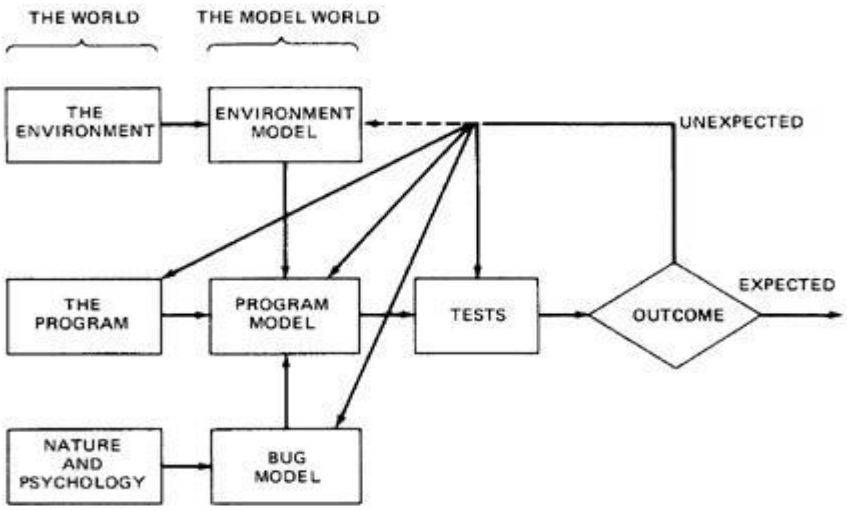


Figure 1.1: A Model for Testing

Above figure is a model of testing process. It includes three models: A model of the environment, a model of the program and a model of the expected bugs.

- **ENVIRONMENT:**
  - A Program's environment is the hardware and software required to make it run. For online systems, the environment may include communication lines, other systems, terminals and operators.
  - The environment also includes all programs that interact with and are used to create the program under test - such as OS, linkage editor, loader, compiler, utility routines.
  - Because the hardware and firmware are stable, it is not smart to blame the environment for bugs.
- **PROGRAM:**
  - Most programs are too complicated to understand in detail.
  - The concept of the program is to be simplified inorder to test it.
  - If simple model of the program doesnot explain the unexpected behaviour, we may have to modify that model to include more facts and details. And if that fails, we may have to modify the program.
- **BUGS:**
  - Bugs are more insidious (deceiving but harmful) than ever we expect them to be.
  - An unexpected test result may lead us to change our notion of what a bug is and our model of bugs.
  - Some optimistic notions that many programmers or testers have about bugs are usually unable to test effectively and unable to justify the dirty tests most programs need.
  - **OPTIMISTIC NOTIONS ABOUT BUGS:**
    1. **Benign Bug Hypothesis:** The belief that bugs are nice, tame and logical. (Benign: Not Dangerous)
    2. **Bug Locality Hypothesis:** The belief that a bug discovered with in a component effects only that component's behaviour.
    3. **Control Bug Dominance:** The belief that errors in the control structures (if, switch etc) of programs dominate the bugs.
    4. **Code / Data Separation:** The belief that bugs respect the separation of code and data.
    5. **Lingua Salvator Est:** The belief that the language syntax and semantics (e.g. Structured Coding, Strong typing, etc) eliminates most bugs.
    6. **Corrections Abide:** The mistaken belief that a corrected bug remains corrected.
    7. **Silver Bullets:** The mistaken belief that X (Language, Design method, representation, environment) grants immunity from bugs.
    8. **Sadism Suffices:** The common belief (especially by independent tester) that a sadistic streak, low cunning, and intuition are sufficient to eliminate most bugs. Tough bugs need methodology and techniques.

9. **Angelic Testers:** The belief that testers are better at test design than programmers are at code design.

- **TESTS:**
  - Tests are formal procedures, Inputs must be prepared, Outcomes should predicted, tests should be documented, commands need to be executed, and results are to be observed. *All these errors are subjected to error*
  - **We do three distinct kinds of testing on a typical software system. They are:**
    1. **Unit / Component Testing:** A **Unit** is the smallest testable piece of software that can be compiled, assembled, linked, loaded etc. A unit is usually the work of one programmer and consists of several hundred or fewer lines of code. **Unit Testing** is the testing we do to show that the unit does not satisfy its functional specification or that its implementation structure does not match the intended design structure. A **Component** is an integrated aggregate of one or more units. **Component Testing** is the testing we do to show that the component does not satisfy its functional specification or that its implementation structure does not match the intended design structure.
    2. **Integration Testing: Integration** is the process by which components are aggregated to create larger components. **Integration Testing** is testing done to show that even though the componenets were individually satisfactory (after passing component testing), checks the combination of components are incorrect or inconsistent.
    3. **System Testing:** A **System** is a big component. **System Testing** is aimed at revealing bugs that cannot be attributed to components. It includes testing for performance, security, accountability, configuration sensitivity, startup and recovery.
- **Role of Models:** The art of testing consists of creating , selecting, exploring, and revising models. Our ability to go through this process depends on the number of different models we have at hand and their ability to express a program's behaviour.
- **PLAYING POOL AND CONSULTING ORACLES**
  - Testing is like playing a pool game. Either you hit the ball to any pocket (kiddie pool) or you specify the pocket in advance (real pool). So is the testing. There is kiddie testing and real testing. In kiddie testing, the observed outcome will be considered as the expected outcome. In Real testing, the outcome is predicted and documented before the test is run.
  - The tester who cannot make that kind of predictions does not understand the program's functional objectives.
  - **Oracles:** An oracle is any program, process, or body of data that specifies the expected outcome of a set of tests as applied to a tested object. Example of oracle : Input/Outcome Oracle - an oracle that specifies the expected outcome for a specified input.

- **Sources of Oracles:** If every test designer had to analyze and predict the expected behaviour for every test case for every component, then test design would be very expensive. The hardest part of test design is predicting the expected outcome, but we often have oracles that reduce the work. They are:
  1. **Kiddie Testing:** run the test and see what comes out. If you have the outcome in front of you, and especially if you have the values of the internal variables, then it is much easier to validate that outcome by analysis and show it to be correct than it is to predict what the outcome should be and validate your prediction.
  2. **Regression Test Suites:** Today's software development and testing are dominated not by the design of new software but by rework and maintenance of existing software. In such instances, most of the tests you need will have been run on a previous versions. Most of those tests should have the same outcome for the new version. Outcome prediction is therefore needed only for changed parts of components.
  3. **Purchased Suits and Oracles:** Highly standardized software that differ only as to implementation often has commercially available test suites and oracles. The most common examples are compilers for standard languages.
  4. **Existing Program:** A working, trusted program is an excellent oracle. The typical use is when the program is being rehosted to a new language, operating system, environment, configuration with the intention that the behavior should not change as a result of the rehosting.

- **IS COMPLETE TESTING POSSIBLE?**
  - If the objective of the testing were to prove that a program is free of bugs, then testing not only would be practically impossible, but also would be theoretically impossible.
  - **Three different approaches can be used to demonstrate that a program is correct.They are:**
    1. **Functional Testing:**
       - Every program operates on a finite number of inputs. A complete functional test would consists of subjecting the program to all possible input streams.
       - For each input the routine either accepts the stream and produces a correct outcome, accepts the stream and produces an incorrect outcome, or rejects the stream and tells us that it did so.
       - For example, a 10 character input string has 280 possible input streams and corresponding outcomes, so complete functional testing in this sense is IMPRACTICAL.

- But even theoritically, we can't execute a purely functional test this way because we don't know the length of the string to which the system is responding.

2. **Structural Testing:**
   - The design should have enough tests to ensure that every path through the routine is exercised at least once. Right off that's is impossible because some loops might never terminate.
   - The number of paths through a small routine can be awesome because each loop multiplies the path count by the number of times through the loop.
   - A small routine can have millions or billions of paths, so total **Path Testing** is usually IMPRACTICAL.
3. **Formal Proofs of Correctness:**
   - Formal proofs of correctness rely on a combination of functional and structural concepts.
   - Requirements are stated in a formal language (e.g. Mathematics) and each program statement is examined and used in a step of an inductive proof that the routine will produce the correct outcome for all possible input sequences.
   - The IMPRACTICAL thing here is that such proofs are very expensive and have been applied only to numerical routines or to formal proofs for crucial software such as system's security kernel or portions of compilers.

- Each approach leads to the conclusion that complete testing, in the sense of a proof is neither theoretically nor practically possible.

- **THEORITICAL BARRIERS OF COMPLETE TESTING:**
  - "We can never be sure that the specifications are correct"
  - "No verification system can verify every correct program"
  - "We can never be certain that a verification system is correct"
- Not only all known approaches to absoulte demonstrations of correctness impractical, but they are impossible. Therefore, our objective must shift from a absolute proof to a 'suitably convincing' demonstration.

4. CONSEQUENCES OF BUGS:

- **IMPORTANCE OF BUGS:** The importance of bugs depends on frequency, correction cost, installation cost, and consequences.
  1. **Frequency:** How often does that kind of bug occur? Pay more attention to the more frequent bug types.

2. **Correction Cost:** What does it cost to correct the bug after it is found? The cost is the sum of 2 factors: (1) the cost of discovery (2) the cost of correction. These costs go up dramatically later in the development cycle when the bug is discovered. Correction cost also depends on system size.
3. **Installation Cost:** Installation cost depends on the number of installations: small for a single user program but more for distributed systems. Fixing one bug and distributing the fix could exceed the entire system's development cost.
4. **Consequences:** What are the consequences of the bug? Bug consequences can range from mild to catastrophic.

A reasonable metric for bug importance is

Importance= ($) = Frequence * (Correction cost + Installation cost + Consequential cost)

- **CONSEQUENCES OF BUGS:** The consequences of a bug can be measure in terms of human rather than machine. Some consequences of a bug on a scale of one to ten are:
  1. **Mild:** The symptoms of the bug offend us aesthetically (gently); a misspelled output or a misaligned printout.
  2. **Moderate:** Outputs are misleading or redundant. The bug impacts the system's performance.
  3. **Annoying:** The system's behaviour because of the bug is dehumanizing. *E.g.* Names are truncated orarbitarily modified.
  4. **Disturbing:** It refuses to handle legitimate (authorized / legal) transactions. The ATM wont give you money. My credit card is declared invalid.
  5. **Serious:** It loses track of its transactions. Not just the transaction itself but the fact that the transaction occurred. Accountability is lost.
  6. **Very Serious:** The bug causes the system to do the wrong transactions. Instead of losing your paycheck, the system credits it to another account or converts deposits to withdrawals.
  7. **Extreme:** The problems aren't limited to a few users or to few transaction types. They are frequent and arbitrary instead of sporadic infrequent) or for unusual cases.
  8. **Intolerable:** Long term unrecoverable corruption of the database occurs and the corruption is not easily discovered. Serious consideration is given to shutting the system down.
  9. **Catastrophic:** The decision to shut down is taken out of our hands because the system fails.
  10. **Infectious:** What can be worse than a failed system? One that corrupt other systems even though it doesnot fall in itself ; that erodes the social physical environment; that melts nuclear reactors and starts war.

- **FLEXIBLE SEVERITY RATHER THAN ABSOLUTES:**
  - Quality can be measured as a combination of factors, of which number of bugs and their severity is only one component.
  - Many organizations have designed and used satisfactory, quantitative, quality metrics.
  - Because bugs and their symptoms play a significant role in such metrics, as testing progresses, you see the quality rise to a reasonable value which is deemed to be safe to ship the product.
  - The factors involved in bug severity are:

1. **Correction Cost:** Not so important because catastrophic bugs may be corrected easier and small bugs may take major time to debug.
2. **Context and Application Dependency:** Severity depends on the context and the application in which it is used.
3. **Creating Culture Dependency:** Whats important depends on the creators of software and their cultural aspirations. Test tool vendors are more sensitive about bugs in their software then games software vendors.
4. **User Culture Dependency:** Severity also depends on user culture. Naive users of PC software go crazy over bugs where as pros (experts) may just ignore.
5. **The software development phase:** Severity depends on development phase. Any bugs gets more severe as it gets closer to field use and more severe the longer it has been around.

5. TAXONOMY OF BUGS:

- There is no universally correct way categorize bugs. The taxonomy is not rigid.
- A given bug can be put into one or another category depending on its history and the programmer's state of mind.
- The major categories are: (1) Requirements, Features and Functionality Bugs (2) Structural Bugs (3) Data Bugs (4) Coding Bugs (5) Interface, Integration and System Bugs (6) Test and Test Design Bugs.

- **REQUIREMENTS, FEATURES AND FUNCTIONALITY BUGS:** Various categories in Requirements, Features and Functionlity bugs include:

1. **Requirements and Specifications Bugs:**
   - Requirements and specifications developed from them can be incomplete ambiguous, or self-contradictory. They can be misunderstood or impossible to understand.
   - The specifications that don't have flaws in them may change while the design is in progress. The features are added, modified and deleted.
   - Requirements, especially, as expressed in specifications are a major source of expensive bugs.

- The range is from a few percentage to more than 50%, depending on the application and environment.
- What hurts most about the bugs is that they are the earliest to invade the system and the last to leave.

2. **Feature Bugs:**
   - Specification problems usually create corresponding feature problems.
   - A feature can be wrong, missing, or superfluous (serving no useful purpose). A missing feature or case is easier to detect and correct. A wrong feature could have deep design implications.
   - Removing the features might complicate the software, consume more resources, and foster more bugs.
3. **Feature Interaction Bugs:**
   - Providing correct, clear, implementable and testable feature specifications is not enough.
   - Features usually come in groups or related features. The features of each group and the interaction of features with in the group are usually well tested.
   - The problem is unpredictable interactions between feature groups or even between individual features. For example, your telephone is provided with call holding and call forwarding. The interactions between these two features may have bugs.
   - Every application has its peculiar set of features and a much bigger set of unspecified feature interaction potentials and therefore result in feature interaction bugs.

Specification and Feature Bug Remedies:

- Most feature bugs are rooted in human to human communication problems. One solution is to use high-level, formal specification languages or systems.
- Such languages and systems provide short term support but in the long run, does not solve the problem.
- ***Short term Support:*** Specification languages facilitate formalization of requirements and inconsistency and ambiguity analysis.
- ***Long term Support:*** Assume that we have a great specification language and that can be used to create unambiguous, complete specifications with unambiguous complete testsand consistent test criteria.
- The specification problem has been shifted to a higher level but not eliminated.

Testing Techniques for functional bugs: Most functional test techniques- that is those techniques which are based on a behavioral description of software, such as transaction flow testing, syntax testing, domain testing, logic testing and state testing are useful in testing functional bugs.

STRUCTURAL BUGS: Various categories in Structural bugs include:

9. **Control and Sequence Bugs:**
   - Control and sequence bugs include paths left out, unreachable code, improper nesting of loops, loop-back or loop termination criteria incorrect, missing process steps, duplicated processing, unnecessary processing, rampaging, GOTO's, ill-conceived (not properly planned) switches, sphagetti code, and worst of all, pachinko code.
   - One reason for control flow bugs is that this area is amenable (supportive) to theoritical treatment.
   - Most of the control flow bugs are easily tested and caught in unit testing.
   - Another reason for control flow bugs is that use of old code especially ALP & COBOL code are dominated by control flow bugs.
   - Control and sequence bugs at all levels are caught by testing, especially structural testing, more specifically path testing combined with a bottom line functional test based on a specification.
10. **Logic Bugs:**
   - Bugs in logic, especially those related to misundertanding how case statements and logic operators behave singly and combinations
   - Also includes evaluation of boolean expressions in deeply nested IF-THEN-ELSE constructs.
   - If the bugs are parts of logical (i.e. boolean) processing not related to control flow, they are characterized as processing bugs.
   - If the bugs are parts of a logical expression (i.e control-flow statement) which is used to direct the control flow, then they are categorized as control-flow bugs.
11. **Processing Bugs:**
   - Processing bugs include arithmetic bugs, algebraic, mathematical function evaluation, algorithm selection and general processing.
   - Examples of Processing bugs include: Incorrect conversion from one data representation to other, ignoring overflow, improper use of grater-than-or-eual etc
   - Although these bugs are frequent (12%), they tend to be caught in good unit testing.
12. **Initialization Bugs:**
   - Initialization bugs are common. Initialization bugs can be improper and superfluous.
   - Superfluous bugs are generally less harmful but can affect performance.
   - Typical initialization bugs include: Forgetting to initialize the variables before first use, assuming that they are initialized elsewhere, initializing to the wrong format, representation or type etc
   - Explicit declaration of all variables, as in Pascal, can reduce some initialization problems.

13. **Data-Flow Bugs and Anomalies:**
    - Most initialization bugs are special case of data flow anamolies.
    - A data flow anomaly occurs where there is a path along which we expect to do something unreasonable with data, such as using an uninitialized variable, attempting to use a variable before it exists, modifying and then not storing or using the result, or initializing twice without an intermediate use.

DATA BUGS:

- Data bugs include all bugs that arise from the specification of data objects, their formats, the number of such objects, and their initial values.
- Data Bugs are atleast as common as bugs in code, but they are foten treated as if they didnot exist at all.
- *Code migrates data:* Software is evolving towards programs in which more and more of the control and processing functions are stored in tables.
- Because of this, there is an increasing awareness that bugs in code are only half the battle and the data problems should be given equal attention.

Dynamic Data Vs Static data:

- Dynamic data are transitory. Whatever their purpose their lifetime is relatively short, typically the processing time of one transaction. A storage object may be used to hold dynamic data of different types, with different formats, attributes and residues.
- Dynamic data bugs are due to leftover garbage in a shared resource. This can be handled in one of the three ways: (1) Clean up after the use by the user (2) Common Cleanup by the resource manager (3) No Clean up
- Static Data are fixed in form and content. They appear in the source code or database directly or indirectly, for example a number, a string of characters, or a bit pattern.
- Compile time processing will solve the bugs caused by static data.

- **Information, parameter, and control:** Static or dynamic data can serve in one of three roles, or in combination of roles: as a parameter, for control, or for information.
- **Content, Structure and Attributes: Content** can be an actual bit pattern, character string, or number put into a data structure. Content is a pure bit pattern and has no meaning unless it is interpreted by a hardware or software processor. All data bugs result in the corruption or misinterpretation of content. **Structure** relates to the size, shape and numbers that describe the data object, that is memory location used to store the content. (e.g A two dimensional array). **Attributes** relates to the specification meaning that is the semantics associated with the contents of a data object. (e.g. an integer, an alphanumeric string, a subroutine). *The severity and subtlelty of bugs increases as we go from content to attributes because the things get less formal in that direction.*

CODING BUGS:

- Coding errors of all kinds can create any of the other kind of bugs.
- Syntax errors are generally not important in the scheme of things if the source language translator has adequate syntax checking.
- If a program has many syntax errors, then we should expect many logic and coding bugs.
- The documentation bugs are also considered as coding bugs which may mislead the maintenance programmers.

INTERFACE, INTEGRATION, AND SYSTEM BUGS:

- Various categories of bugs in Interface, Integration, and System Bugs are:

1.**External Interfaces:**

- The external interfaces are the means used to communicate with the world.
- These include devices, actuators, sensors, input terminals, printers, and communication lines.
- The primary design criterion for an interface with outside world should be robustness.
- All external interfaces, human or machine should employ a protocol. The protocol may be wrong or incorrectly implemented.
- Other external interface bugs are: invalid timing or sequence assumptions related to external signals
- Misunderstanding external input or output formats.
- Insufficient tolerance to bad input data.

2. **Internal Interfaces:**

- Internal interfaces are in principle not different from external interfaces but they are more controlled.
- A best example for internal interfaces are communicating routines.
- The external environment is fixed and the system must adapt to it but the internal environment, which consists of interfaces with other components, can be negotiated.
- Internal interfaces have the same problem as external interfaces.

3. **Hardware Architecture:**

- Bugs related to hardware architecture originate mostly from misunderstanding how the hardware works.
- Examples of hardware architecture bugs: address generation error, i/o device operation / instruction error, waiting too long for a response, incorrect interrupt handling etc.
- The remedy for hardware architecture and interface problems is two fold: (1) Good Programming and Testing (2) Centralization of hardware interface software in programs written by hardware interface specialists.

4. **Operating System Bugs:**
   - Program bugs related to the operating system are a combination of hardware architecture and interface bugs mostly caused by a misunderstanding of what it is the operating system does.
   - Use operating system interface specialists, and use explicit interface modules or macros for all operating system calls.
   - This approach may not eliminate the bugs but at least will localize them and make testing easier.
5. **Software Architecture:**
   - Software architecture bugs are the kind that called - interactive.
   - Routines can pass unit and integration testing without revealing such bugs.
   - Many of them depend on load, and their symptoms emerge only when the system is stressed.
   - Sample for such bugs: Assumption that there will be no interrupts, Failure to block or un block interrupts, Assumption that memory and registers were initialized or not initialized etc
   - Careful integration of modules and subjecting the final system to a stress test are effective methods for these bugs.
6. **Control and Sequence Bugs (Systems Level):**
   - These bugs include: Ignored timing, Assuming that events occur in a specified sequence, Working on data before all the data have arrived from disc, Waiting for an impossible combination of prerequisites, Missing, wrong, redundant or superfluous process steps.
   - The remedy for these bugs is highly structured sequence control.
   - Specialize, internal, sequence control mechanisms are helpful.
7. **Resource Management Problems:**
   - Memory is subdivided into dynamically allocated resources such as buffer blocks, queue blocks, task control blocks, and overlay buffers.
   - External mass storage units such as discs, are subdivided into memory resource pools.
   - Some resource management and usage bugs: Required resource not obtained, Wrong resource used, Resource is already in use, Resource dead lock etc
   - **Resource Management Remedies:** A design remedy that prevents bugs is always preferable to a test method that discovers them.
   - The design remedy in resource management is to keep the resource structure simple: the fewest different kinds of resources, the fewest pools, and no private resource management.

8. **Integration Bugs:**
   - Integration bugs are bugs having to do with the integration of, and with the interfaces between, working and tested components.
   - These bugs results from inconsistencies or incompatibilities between components.
   - The communication methods include data structures, call sequences, registers, semaphores, communication links and protocols results in integration bugs.
   - The integration bugs do not constitute a big bug category(9%) they are expensive category because they are usually caught late in the game and because they force changes in several components and/or data structures.

9. **System Bugs:**
   - System bugs covering all kinds of bugs that cannot be ascribed to a component or to their simple interactions, but result from the totality of interactions between many components such as programs, data, hardware, and the operating systems.
   - There can be no meaningful system testing until there has been thorough component and integration testing.
   - System bugs are infrequent(1.7%) but very important because they are often found only after the system has been fielded.

TEST AND TEST DESIGN BUGS:

- Testing: testers have no immunity to bugs. Tests require complicated scenarios and databases.
- They require code or the equivalent to execute and consequently they can have bugs.
- Test criteria: if the specification is correct, it is correctly interpreted and implemented, and a proper test has been designed; but the criterion by which the software's behavior is judged may be incorrect or impossible. So, a proper test criteria has to be designed. The more complicated the criteria, the likelier they are to have bugs.

Remedies: The remedies of test bugs are:

1. **Test Debugging:** The first remedy for test bugs is testing and debugging the tests. Test debugging, when compared to program debugging, is easier because tests, when properly designed are simpler than programs and donot have to make concessions to efficiency.
2. **Test Quality Assurance:** Programmers have the right to ask how quality in independent testing is monitored.
3. **Test Execution Automation:** The history of software bug removal and prevention is indistinguishable from the history of programming automation aids.

Assemblers, loaders, compilers are developed to reduce the incidence of programming and operation errors. Test execution bugs are virtually eliminated by various test execution automation tools.

4. **Test Design Automation:** Just as much of software development has been automated, much test design can be and has been automated. For a given productivity rate, automation reduces the bug count - be it for software or be it for tests.

FLOWGRAPHS AND PATH TESTING

1. BASICS OF PATH TESTING:

- **PATH TESTING:**
  - Path Testing is the name given to a family of test techniques based on judiciously selecting a set of test paths through the program.
  - If the set of paths are properly chosen then we have achieved some measure of test thoroughness. For example, pick enough paths to assure that every source statement has been executed at least once.
  - Path testing techniques are the oldest of all structural test techniques.
  - Path testing is most applicable to new software for unit testing. It is a structural technique.
  - It requires complete knowledge of the program's structure.
  - It is most often used by programmers to unit test their own code.
  - The effectiveness of path testing rapidly deteriorates as the size of the software aggregate under test increases.
- **THE BUG ASSUMPTION:**
  - The bug assumption for the path testing strategies is that something has gone wrong with the software that makes it take a different path than intended.
  - As an example "GOTO X" where "GOTO Y" had been intended.
  - Structured programming languages prevent many of the bugs targeted by path testing: as a consequence the effectiveness for path testing for these languages is reduced and for old code in COBOL, ALP, FORTRAN and Basic, the path testing is indespensable.
- **CONTROL FLOW GRAPHS:**
  - The control flow graph is a graphical representation of a program's control structure. It uses the elements named process blocks, decisions, and junctions.
  - The flow graph is similar to the earlier flowchart, with which it is not to be confused.
  - **Flow Graph Elements:** A flow graph contains four different types of elements. (1) Process Block (2) Decisions (3) Junctions (4) Case Statements
    1. **Process Block:**
       - A process block is a sequence of program statements uninterrupted by either decisions or junctions.
       - It is a sequence of statements such that if any one of statement of the block is executed, then all statement thereof are executed.
       - Formally, a process block is a piece of straight line code of one statement or hundreds of statements.

- A process has one entry and one exit. It can consists of a single statement or instruction, a sequence of statements or instructions, a single entry/exit subroutine, a macro or function call, or a sequence of these.

2. **Decisions:**
   - A decision is a program point at which the control flow can diverge.
   - Machine language conditional branch and conditional skip instructions are examples of decisions.
   - Most of the decisions are two-way but some are three way branches in control flow.
3. **Case Statements:**
   - A case statement is a multi-way branch or decisions.
   - Examples of case statement are a jump table in assembly language, and the PASCAL case statement.
   - From the point of view of test design, there are no differences between Decisions and Case Statements
4. **Junctions:**
   - A junction is a point in the program where the control flow can merge.
   - Examples of junctions are: the target of a jump or skip instruction in ALP, a label that is a target of GOTO.

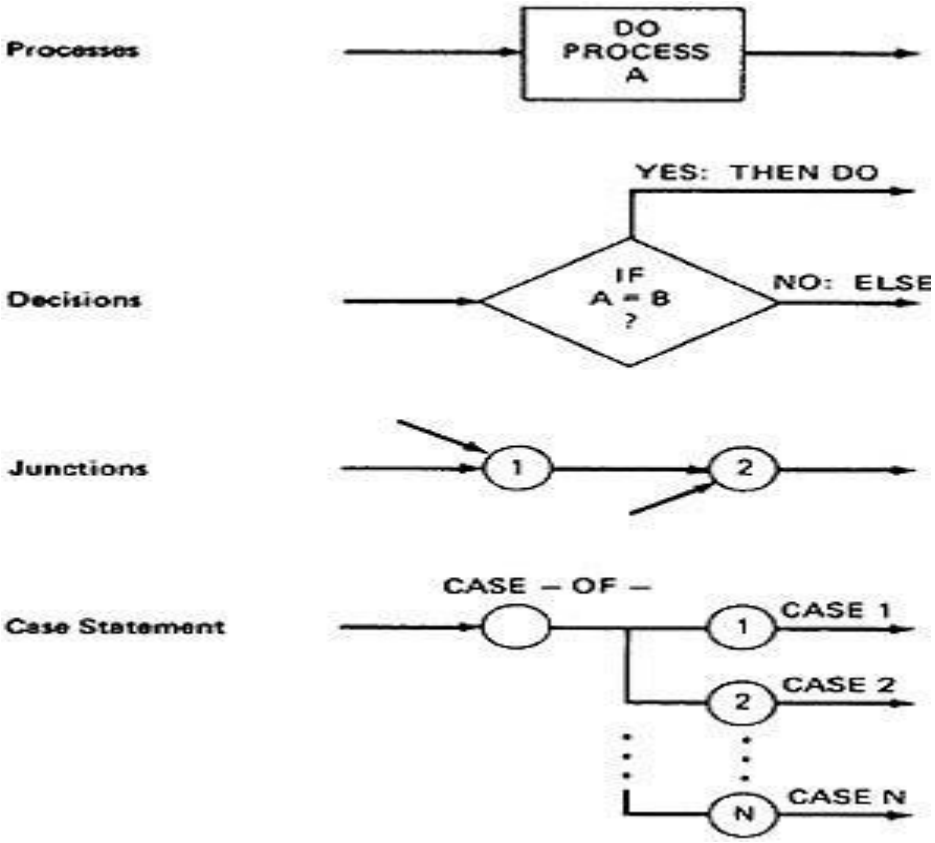


Figure 1.1: Flowgraph Elements

CONTROL FLOW GRAPHS Vs FLOWCHARTS:

- A program's flow chart resembles a control flow graph.
- In flow graphs, we don't show the details of what is in a process block.
- In flow charts every part of the process block is drawn.
- The flowchart focuses on process steps, where as the flow graph focuses on control flow of the program.
- The act of drawing a control flow graph is a useful tool that can help us clarify the control flow and data flow issues.

NOTATIONAL EVOULTION:

The control flow graph is simplified representation of the program's structure.
The notation changes made in creation of control flow graphs:

- The process boxes weren't really needed. There is an implied process on every line joining junctions and decisions.
- We don't need to know the specifics of the decisions, just the fact that there is a branch.
- The specific target label names aren't important-just the fact that they exist. So we can replace them by simple numbers.

To understand this, we will go through an example (Figure 1.2) written in a FORTRAN like programming language called **Programming Design Language (PDL)**. The program's corresponding flowchart (Figure 1.3) and flowgraph (Figure 1.4) were also provided below for better understanding.

The first step in translating the program to a flowchart is shown in Figure 1.3, where we have the typical one-for-one classical flowchart. Note that complexity has increased, clarity has decreased, and that we had to add auxiliary labels (LOOP, XX, and YY), which have no actual program counterpart. In Figure 1.4 we merged the process steps and replaced them with the single process box. We now have a control flowgraph. But this representation is still too busy. We simplify the notation further to achieve Figure 1.5, where for the first time we can really see what the control flow looks like.

CODE* (PDL)

```
      INPUT X, Y                      V(U−1):=V(U+1) + U(V−1)
      Z := X + Y                ELL:V(U+U(V)) := U + V
      V := X − Y                      IF U = V GOTO JOE
      IF Z >=ø GOTO SAM               IF U > V THEN U := Z
 JOE: Z := Z − 1                      Z := U
SAM:  Z := Z + V                      END
      FOR U = ø TO Z
      V(U),U(V) := (Z + V)*U
      IF V(U)= ø GOTO JOE
      Z := Z − 1
      IF Z = ø GOTO ELL
      U := U + 1
      NEXT U
```

* A contrived horror

Figure 1.2: Program Example (PDL)

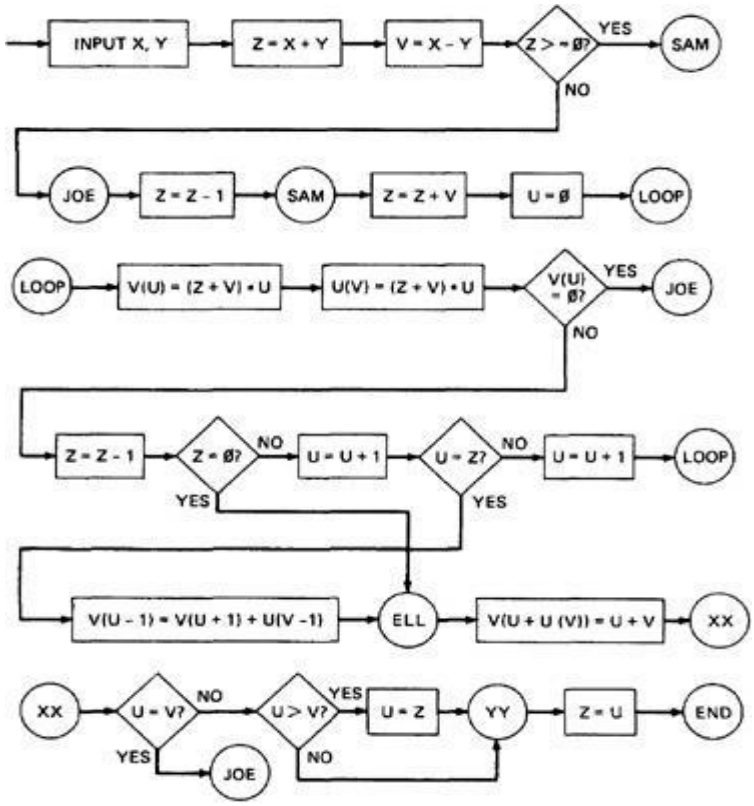


Figure 1.3: One-to-one flowchart for example program in Figure1.2

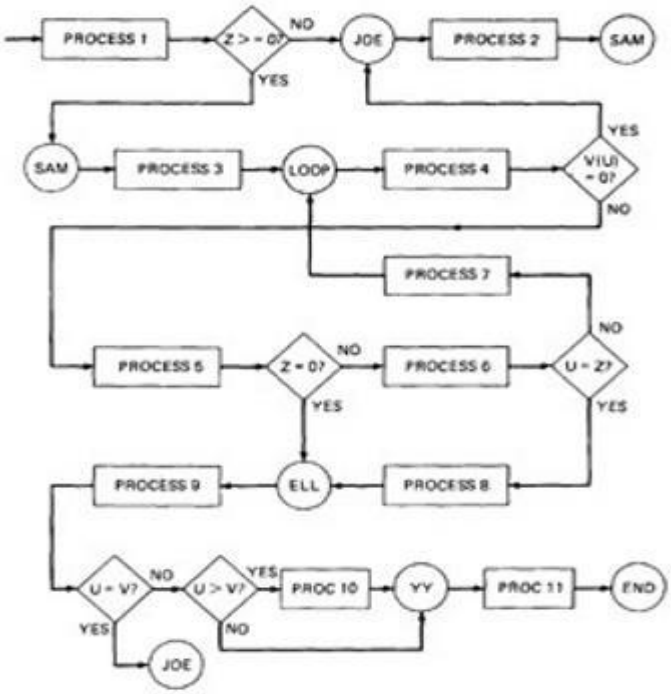


Figure 1.4: Control Flowgraph for example in Figure 1.2

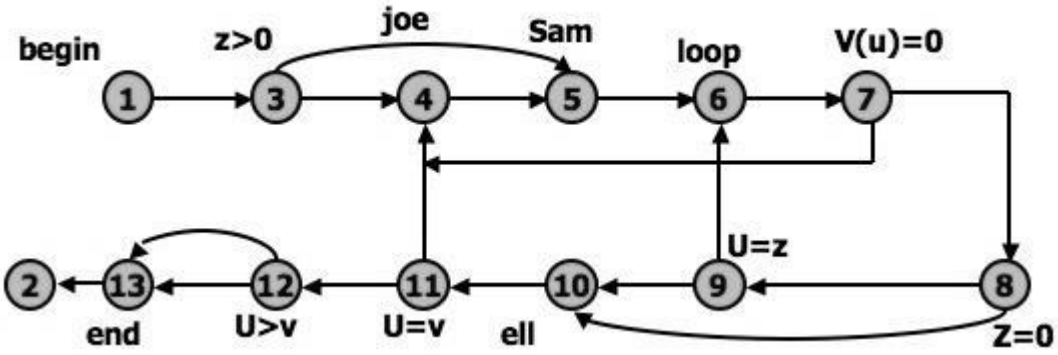


Figure 1.5: Simplified Flowgraph Notation

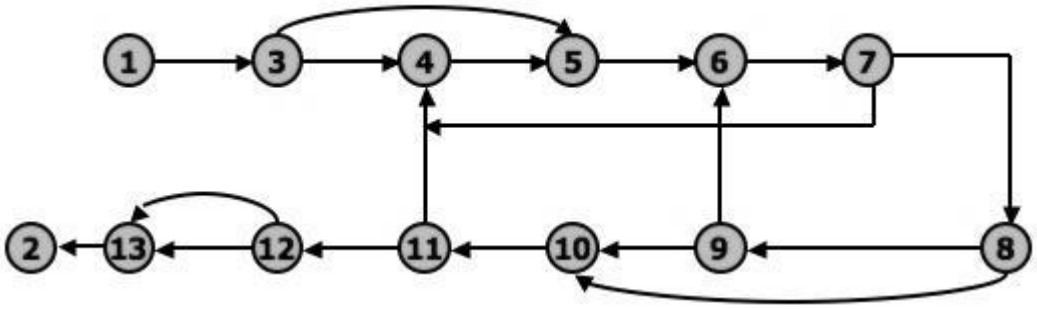


Figure 1.6: Even Simplified Flowgraph Notation

The final transformation is shown in Figure 1.6, where we've dropped the node numbers to achieve an even simpler representation. The way to work with control flowgraphs is to use the simplest possible representation - that is, no more information than you need to correlate back to the source program or PDL.

LINKED LIST REPRESENTATION:

Although graphical representations of flowgraphs are revealing, the details of the control flow inside a program they are often inconvenient.

In linked list representation, each node has a name and there is an entry on the list for each link in the flow graph. only the information pertinent to the control flow is shown.

Linked List representation of Flow Graph:

```
1  (BEGIN)     : 3
2  (END)       :              Exit, no outlink
3  (Z>Ø?)      : 4 (FALSE)
               : 5 (TRUE)
4  (JOE)       : 5
5  (SAM)       : 6
6  (LOOP)      : 7
7  (V(U)=Ø?)   : 4 (TRUE)
               : 8 (FALSE)
8  (Z=Ø?)      : 9 (FALSE)
               :10 (TRUE)
9  (U=Z?)      : 6 (FALSE) = LOOP
               :10 (TRUE) = ELL
10 (ELL)       :11
11 (U=V?)      : 4 (TRUE) = JOE
               :12 (FALSE)
12 (U>V?)      :13 (TRUE)
               :13 (FALSE)
13             : 2 (END)
```

Figure 1.7: Linked List Control Flowgraph Notation

FLOWGRAPH - PROGRAM CORRESPONDENCE:

A flow graph is a pictorial representation of a program and not the program itself, just as a topographic map.

You cant always associate the parts of a program in a unique way with flowgraph parts because many program structures, such as if-then-else constructs, consists of a combination of decisions, junctions, and processes.

The translation from a flowgraph element to a statement and vice versa is not always unique. (See Figure 1.8)

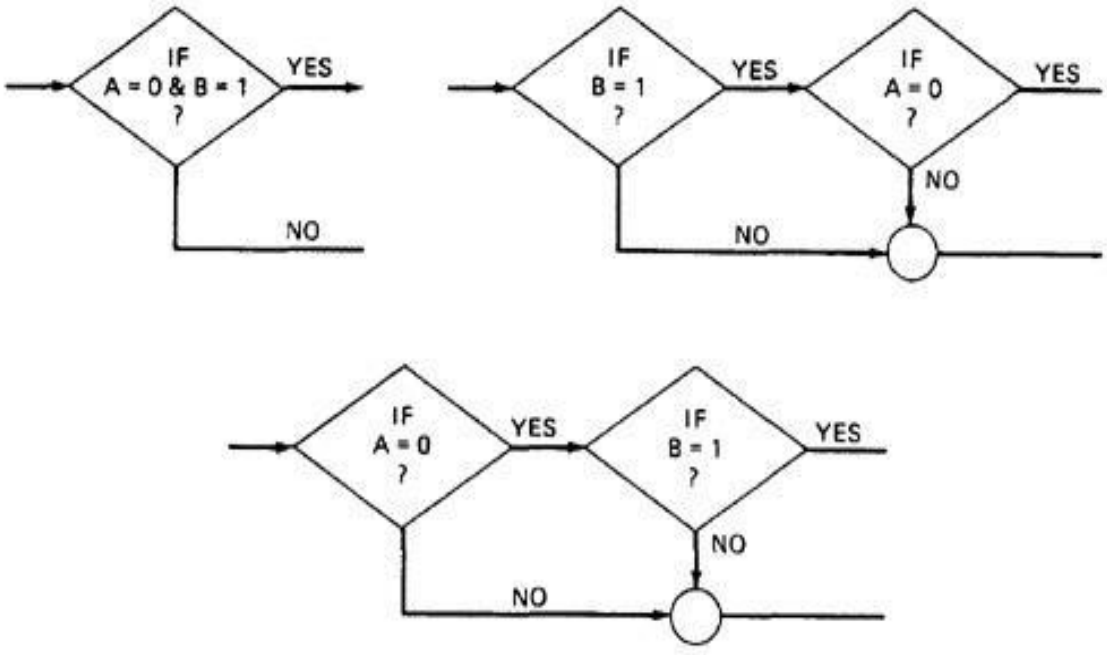


Figure 1.8: Alternative Flowgraphs for same logic (Statement "IF (A=0) AND (B=1) THEN . . .").

An improper translation from flowgraph to code during coding can lead to bugs, and improper translation during the test design lead to missing test cases and causes undiscovered bugs.

FLOWGRAPH AND FLOWCHART GENERATION:

Flowcharts can be

1. Handwritten by the programmer.
2. Automatically produced by a flowcharting program based on a mechanical analysis of the source code.
3. Semi automatically produced by a flow charting program based in part on structural analysis of the source code and in part on directions given by the programmer.

There are relatively few control flow graph generators.

PATH TESTING - PATHS, NODES AND LINKS:

Path: a path through a program is a sequence of instructions or statements that starts at an entry, junction, or decision and ends at another, or possibly the same junction, decision, or exit. A path may go through several junctions, processes, or decisions, one or more times.

- Paths consists of segments.
- The segment is a link - a single process that lies between two nodes.
- A path segment is succession of consecutive links that belongs to some path.
- The length of path measured by the number of links in it and not by the number of the instructions or statements executed along that path.
- The name of a path is the name of the nodes along the path.

FUNDAMENTAL PATH SELECTION CRITERIA:

There are many paths between the entry and exit of a typical routine.

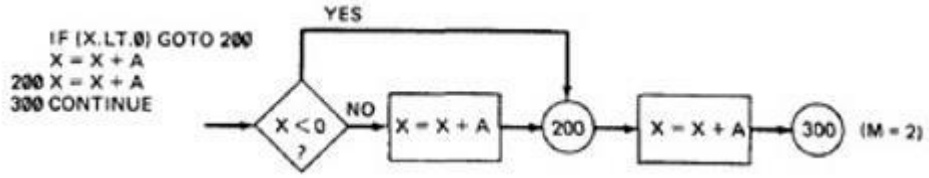
Every decision doubles the number of potential paths. And every loop multiplies the number of potential paths by the number of different iteration values possible for the loop.

Defining complete testing:

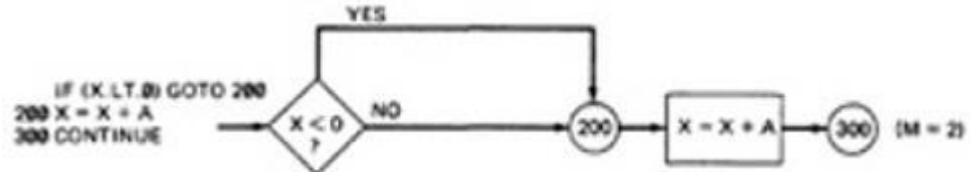
1. Exercise every path from entry to exit
2. Exercise every statement or instruction at least once
3. Exercise every branch and case statement, in each direction at least once

If prescription 1 is followed then 2 and 3 are automatically followed. But it is impractical for most routines. It can be done for the routines that have no loops, in which it is equivalent to 2 and 3 prescriptions.

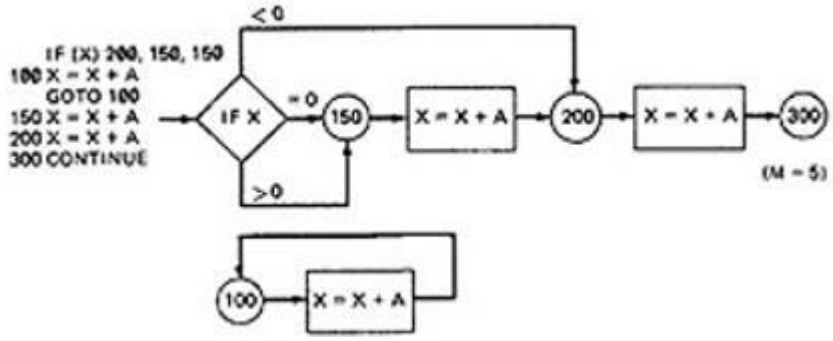
***EXAMPLE:*Here is the correct version.**



For X negative, the output is X + A, while for X greater than or equal to zero, the output is X + 2A. Following prescription 2 and executing every statement, but not every branch, would not reveal the bug in the following incorrect version:



A negative value produces the correct answer. Every statement can be executed, but if the test cases do not force each branch to be taken, the bug can remain hidden. The next example uses a test based on executing each branch but does not force the execution of all statements:



The hidden loop around label 100 is not revealed by tests based on prescription 3 alone because no test forces the execution of statement 100 and the following GOTO statement. Furthermore,

label 100 is not flagged by the compiler as an unreferenced label and the subsequent GOTO does not refer to an undefined label.

A **Static Analysis** (that is, an analysis based on examining the source code or structure) cannot determine whether a piece of code is or is not reachable. There could be subroutine calls with parameters that are subroutine labels, or in the above example there could be a GOTO that targeted label 100 but could never achieve a value that would send the program to that label.

Only a **Dynamic Analysis** (that is, an analysis based on the code's behavior while running - which is to say, to all intents and purposes, testing) can determine whether code is reachable or not and therefore distinguish between the ideal structure we think we have and the actual, buggy structure.

PATH TESTING CRITERIA:

Any testing strategy based on paths must at least both exercise every instruction and take branches in all directions.

A set of tests that does this is not complete in an absolute sense, but it is complete in the sense that anything less must leave something untested.

So we have explored three different testing criteria or strategies out of a potentially infinite family of strategies.

1. **Path Testing (P_{inf})**:
    - Execute all possible control flow paths through the program: typically, this is restricted to all possible entry/exit paths through the program.
    - If we achieve this prescription, we are said to have achieved 100% path coverage. This is the strongest criterion in the path testing strategy family: it is generally impossible to achieve.
1. **Statement Testing (P_1)**:
    - Execute all statements in the program at least once under some test. If we do enough tests to achieve this, we are said to have achieved 100% statement coverage.
    - An alternate equivalent characterization is to say that we have achieved 100% node coverage. We denote this by C1.
    - This is the weakest criterion in the family: testing less than this for new software is unconscionable (unprincipled or can not be accepted) and should be criminalized.
2. **Branch Testing (P_2)**:
    - Execute enough tests to assure that every branch alternative has been exercised at least once under some test.
    - If we do enough tests to achieve this prescription, then we have achieved 100% branch coverage.
    - An alternative characterization is to say that we have achieved 100% link coverage.

- For structured software, branch testing and therefore branch coverage strictly includes statement coverage.
- We denote branch coverage by C2.

Commonsense and Strategies:

- Branch and statement coverage are accepted today as the minimum mandatory testing requirement.
- The question "why not use a judicious sampling of paths?, what is wrong with leaving some code, untested?" is ineffectual in the view of common sense and experience since: **(1.)** Not testing a piece of a code leaves a residue of bugs in the program in proportion to the size of the untested code and the probability of bugs. **(2.)** The high probability paths are always thoroughly tested if only to demonstrate that the system works properly.
- **Which paths to be tested?** You must pick enough paths to achieve C1+C2. The question of what is the fewest number of such paths is interesting to the designer of test tools that help automate the path testing, but it is not crucial to the pragmatic (practical) design of tests. It is better to make many simple paths than a few complicated paths.

LOOPS:

- **Cases for a single loop:** A Single loop can be covered with two cases: Looping and Not looping. But, experience shows that many loop-related bugs are not discovered by C1+C2. Bugs hide themselves in corners and congregate at boundaries - in the cases of loops, at or around the minimum or maximum number of times the loop can be iterated. The minimum number of iterations is often zero, but it need not be.

CASE 1: Single loop, Zero minimum, N maximum, No excluded values

1. Try bypassing the loop (zero iterations). If you can't, you either have a bug, or zero is not the minimum and you have the wrong case.
2. Could the loop-control variable be negative? Could it appear to specify a negative number of iterations? What happens to such a value?
3. One pass through the loop.
4. Two passes through the loop.
5. A typical number of iterations, unless covered by a previous test.
6. One less than the maximum number of iterations.
7. The maximum number of iterations.
8. Attempt one more than the maximum number of iterations. What prevents the loop-control variable from having this value? What will happen with this value if it is forced?

CASE 2: Single loop, Non-zero minimum, No excluded values

1. Try one less than the expected minimum. What happens if the loop control variable's value is less than the minimum? What prevents the value from being less than the minimum?
2. The minimum number of iterations.
3. One more than the minimum number of iterations.
4. Once, unless covered by a previous test.
5. Twice, unless covered by a previous test.
6. A typical value.
7. One less than the maximum value.
8. The maximum number of iterations.
9. Attempt one more than the maximum number of iterations.

CASE 3: Single loops with excluded values

- Treat single loops with excluded values as two sets of tests consisting of loops without excluded values, such as case 1 and 2 above.
- Example, the total range of the loop control variable was 1 to 20, but that values 7,8,9,10 were excluded. The two sets of tests are 1-6 and 11-20.
- The test cases to attempt would be 0,1,2,4,6,7 for the first range and 10,11,15,19,20,21 for the second range.

Kinds of Loops: There are only three kinds of loops with respect to path testing:

Nested Loops:

- The number of tests to be performed on nested loops will be the exponent of the tests performed on single loops.
- As we cannot always afford to test all combinations of nested loops' iterations values. Here's a tactic used to discard some of these values:
    1. Start at the inner most loop. Set all the outer loops to their minimum values.
    2. Test the minimum, minimum+1, typical, maximum-1 , and maximum for the innermost loop, while holding the outer loops at their minimum iteration parameter values. Expand the tests as required for out of range and excluded values.
    3. If you've done the outmost loop, GOTO step 5, else move out one loop and set it up as in step 2 with all other loops set to typical values.
    4. Continue outward in this manner until all loops have been covered.
    5. Do all the cases for all loops in the nest simultaneously.

Concatenated Loops:

- Concatenated loops fall between single and nested loops with respect to test cases. Two loops are concatenated if it's possible to reach one after exiting the other while still on a path from entrance to exit.

- If the loops cannot be on the same path, then they are not concatenated and can be treated as individual loops.

Horrible Loops:

- A horrible loop is a combination of nested loops, the use of code that jumps into and out of loops, intersecting loops, hidden loops, and cross connected loops.
- Makes iteration value selection for test cases an awesome and ugly task, which is another reason such structures should be avoided.

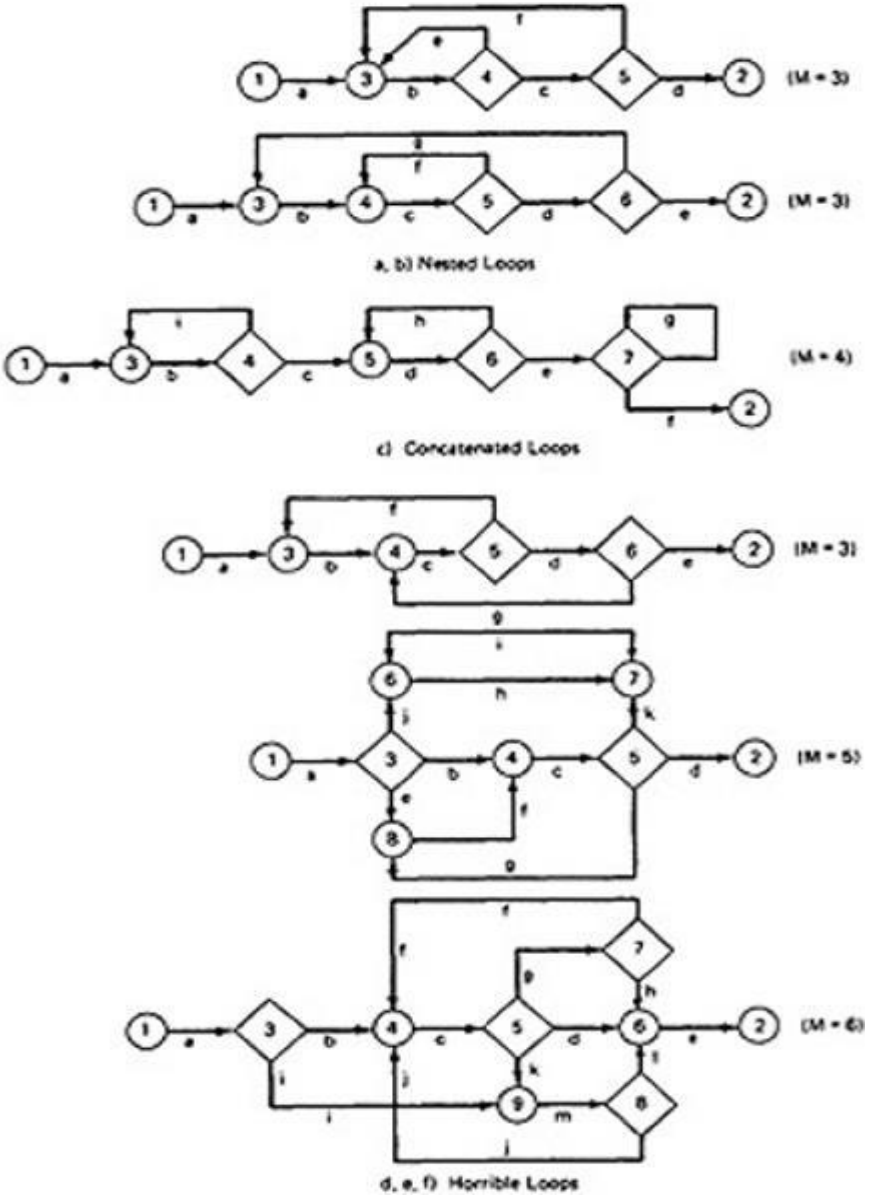


Figure 2.10: Example of Loop types

- **Loop Testing TIme:**
  - Any kind of loop can lead to long testing time, especially if all the extreme value cases are to attempted (Max-1, Max, Max+1).
  - This situation is obviously worse for nested and dependent concatenated loops.
  - Consider nested loops in which testing the combination of extreme values lead to long test times. Several options to deal with:
    - Prove that the combined extreme cases are hypothetically possible, they are not possible in the real world
    - Put in limits or checks that prevent the combined extreme cases. Then you have to test the software that implements such safety measures.

2. PREDICATES, PATH PREDICATES AND ACHIEVABLE PATHS:

PREDICATE: The logical function evaluated at a decision is called Predicate. The direction taken at a decision depends on the value of decision variable. Some examples are: A>0, x+y>=90.....

PATH PREDICATE: A predicate associated with a path is called a Path Predicate. For example, "x is greater than zero", "x+y>=90", "w is either negative or equal to 10 is true" is a sequence of predicates whose truth values will cause the routine to take a specific path.

MULTIWAY BRANCHES:

- The path taken through a multiway branch such as a computed GOTO's, case statement, or jump tables cannot be directly expressed in TRUE/FALSE terms.
- Although, it is possible to describe such alternatives by using multi valued logic, an expedient (practical approach) is to express multiway branches as an equivalent set of if..then..else statements.
- For example a three way case statement can be written as: If case=1 DO A1 ELSE (IF Case=2 DO A2 ELSE DO A3 ENDIF)ENDIF.

INPUTS:

- In testing, the word input is not restricted to direct inputs, such as variables in a subroutine call, but includes all data objects referenced by the routine whose values are fixed prior to entering it.
- For example, inputs in a calling sequence, objects in a data structure, values left in registers, or any combination of object types.
- The input for a particular test is mapped as a one dimensional array called as an Input Vector.

PREDICATE INTERPRETATION:

- The simplest predicate depends only on input variables.
- For example if x1,x2 are inputs, the predicate might be x1+x2>=7, given the values of x1 and x2 the direction taken through the decision is based on the predicate is determined at input time and does not depend on processing.
- Another example, assume a predicate x1+y>=0 that along a path prior to reaching this predicate we had the assignement statement y=x2+7. although our predicate depends on processing, we can substitute the symbolic expression for y to obtain an equivalent predicate x1+x2+7>=0.
- The act of symbolic substitution of operations along the path in order to express the predicate solely in terms of the input vector is called **predicate interpretation.**
- Some times the interpretation may depend on the path; for example,

```
INPUT X
ON X GOTO A, B, C, ...
A: Z := 7 @ GOTO HEM
B: Z := -7 @ GOTO HEM
C: Z := 0 @ GOTO HEM
.....
HEM: DO SOMETHING
.....
HEN: IF Y + Z > 0 GOTO ELL ELSE GOTO EMM
```

The predicate interpretation at HEN depends on the path we took through the first multiway branch. It yields for the three cases respectively, if Y+7>0, Y-7>0, Y>0.

The path predicates are the specific form of the predicates of the decisions along the selected path after interpretation.

INDEPENDENCE OF VARIABLES AND PREDICATES:

- The path predicates take on truth values based on the values of input variables, either directly or indirectly.
- If a variable's value does not change as a result of processing, that variable is independent of the processing.
- If the variable's value can change as a result of the processing, the variable is process dependent.
- A predicate whose truth value can change as a result of the processing is said to be **process dependent** and one whose truth value does not change as a result of the processing is **process independent.**
- Process dependence of a predicate does not always follow from dependence of the input variables on which that predicate is based.

CORRELATION OF VARIABLES AND PREDICATES:

- Two variables are correlated if every combination of their values cannot be independently specified.
- Variables whose values can be specified independently without restriction are called uncorrelated.
- A pair of predicates whose outcomes depend on one or more variables in common are said to be correlated predicates.
  For example, the predicate X==Y is followed by another predicate X+Y == 8. If we select X and Y values to satisfy the first predicate, we might have forced the 2nd predicate's truth value to change.
- Every path through a routine is achievable only if all the predicates in that routine are uncorrelated.

PATH PREDICATE EXPRESSIONS:

- A path predicate expression is a set of boolean expressions, all of which must be satisfied to achieve the selected path.
- Example:

  X1+3X2+17>=0
  X3=17
  X4-X1>=14X2

- Any set of input values that satisfy all of the conditions of the path predicate expression will force the routine to the path.
- Some times a predicate can have an OR in it.
- Example:

A: X5 > 0	E: X6 < 0
B: X1 + 3X2 + 17 >= 0	B: X1 + 3X2 + 17 >= 0
C: X3 = 17	C: X3 = 17
D: X4 - X1 >= 14X2	D: X4 - X1 >= 14X2

- Boolean algebra notation to denote the boolean expression:

  ABCD+EBCD=(A+E)BCD

PREDICATE COVERAGE:

- **Compound Predicate:** Predicates of the form A OR B, A AND B and more complicated boolean expressions are called as compound predicates.
- Some times even a simple predicate becomes compound after interpretation. Example: the predicate if (x=17) whose opposite branch is if x.NE.17 which is equivalent to x>17 . Or. X<17.
- Predicate coverage is being the achieving of all possible combinations of truth values corresponding to the selected path have been explored under some test.

- As achieving the desired direction at a given decision could still hide bugs in the associated predicates.

TESTING BLINDNESS:

- Testing Blindness is a pathological (harmful) situation in which the desired path is achieved for the wrong reason.
- There are three types of Testing Blindness:

0. **Assignment Blindness:**
    - Assignment blindness occurs when the buggy predicate appears to work correctly because the specific value chosen for an assignment statement works with both the correct and incorrect predicate.
    - For Example:

Correct	**Buggy**
X = 7 ..... if Y > 0 then ...	X = 7 ..... if X+Y > 0 then ...

    - If the test case sets Y=1 the desired path is taken in either case, but there is still a bug.

2. **Equality Blindness:**
    - Equality blindness occurs when the path selected by a prior predicate results in a value that works both for the correct and buggy predicate.
    - For Example:

Correct	**Buggy**
if Y = 2 then ..... if X+Y > 3 then ...	if Y = 2 then ..... if X > 1 then ...

    - The first predicate if y=2 forces the rest of the path, so that for any positive value of x. the path taken at the second predicate will be the same for the correct and buggy version.

3. **Self Blindness:**
    - Self blindness occurs when the buggy predicate is a multiple of the correct predicate and as a result is indistinguishable along that path.
    - For Example:

Correct	**Buggy**
X = A ..... if X-1 > 0 then ...	X = A ..... if X+A-2 > 0 then ...

    - The assignment (x=a) makes the predicates multiples of each other, so the direction taken is the same for the correct and buggy version.

3. PATH SENSITIZING:

REVIEW: ACHIEVABLE AND UNACHIEVABLE PATHS:

- We want to select and test enough paths to achieve a satisfactory notion of test completeness such as C1+C2.
- Extract the programs control flowgraph and select a set of tentative covering paths.
- For any path in that set, interpret the predicates along the path as needed to express them in terms of the input vector. In general individual predicates are compound or may become compound as a result of interpretation.
- Trace the path through, multiplying the individual compound predicates to achieve a boolean expression such as

  (A+BC) (D+E) (FGH) (IJ) (K) (l) (L).
- Multiply out the expression to achieve a sum of products form:

  ADFGHIJKL+AEFGHIJKL+BCDFGHIJKL+BCEFGHIJKL
- Each product term denotes a set of inequalities that if solved will yield an input vector that will drive the routine along the designated path.
- Solve any one of the inequality sets for the chosen path and you have found a set of input values for the path.
- If you can find a solution, then the path is achievable.
- If you cant find a solution to any of the sets of inequalities, the path is un achievable.
- The act of finding a set of solutions to the path predicate expression is called **PATH SENSITIZATION**.

HEURISTIC PROCEDURES FOR SENSITIZING PATHS:

- This is a workable approach, instead of selecting the paths without considering how to sensitize, attempt to choose a covering path set that is easy to sensitize and pick hard to sensitize paths only as you must to achieve coverage.
- Identify all variables that affect the decision.
- Classify the predicates as dependent or independent.
- Start the path selection with un correlated, independent predicates.
- If coverage has not been achieved using independent uncorrelated predicates, extend the path set using correlated predicates.
- If coverage has not been achieved extend the cases to those that involve dependent predicates.
- Last, use correlated, dependent predicates.

4. PATH INSTRUMENTATION

PATH INSTRUMENTATION:

- Path instrumentation is what we have to do to confirm that the outcome was achieved by the intended path.
- **Co-incidental Correctness:** The coincidental correctness stands for achieving the desired outcome for wrong reason.

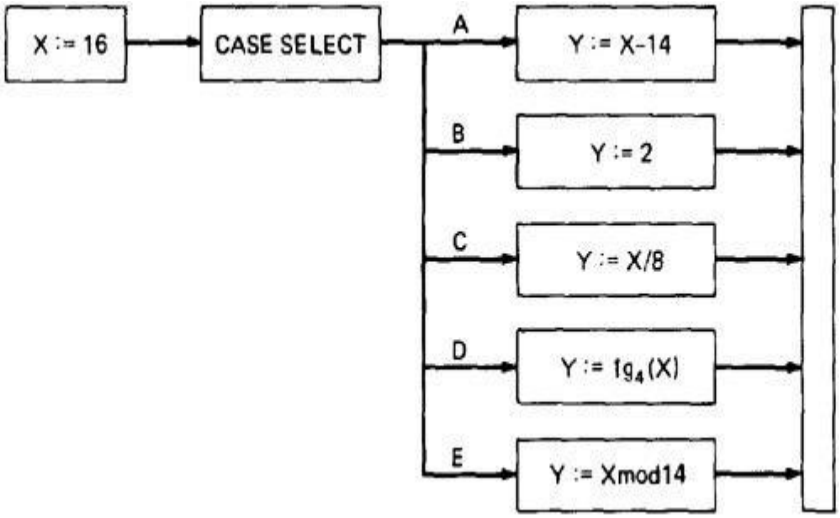


Figure 1.11: Coincidental Correctness

The above figure is an example of a routine that, for the (unfortunately) chosen input value (X = 16), yields the same outcome (Y = 2) no matter which case we select. Therefore, the tests chosen this way will not tell us whether we have achieved coverage. For example, the five cases could be totally jumbled and still the outcome would be the same. **Path Instrumentation** is what we have to do to confirm that the outcome was achieved by the intended path.

The types of instrumentation methods include:

1. **Interpretive Trace Program:**
   - An interpretive trace program is one that executes every statement in order and records the intermediate values of all calculations, the statement labels traversed etc.
   - If we run the tested routine under a trace, then we have all the information we need to confirm the outcome and, furthermore, to confirm that it was achieved by the intended path.
   - The trouble with traces is that they give us far more information than we need. In fact, the typical trace program provides so much information that confirming

the path from its massive output dump is more work than simulating the computer by hand to confirm the path.

2. **Traversal Marker or Link Marker:**
   - A simple and effective form of instrumentation is called a traversal marker or link marker.
   - Name every link by a lower case letter.
   - Instrument the links so that the link's name is recorded when the link is executed.
   - The succession of letters produced in going from the routine's entry to its exit should, if there are no bugs, exactly correspond to the path name.

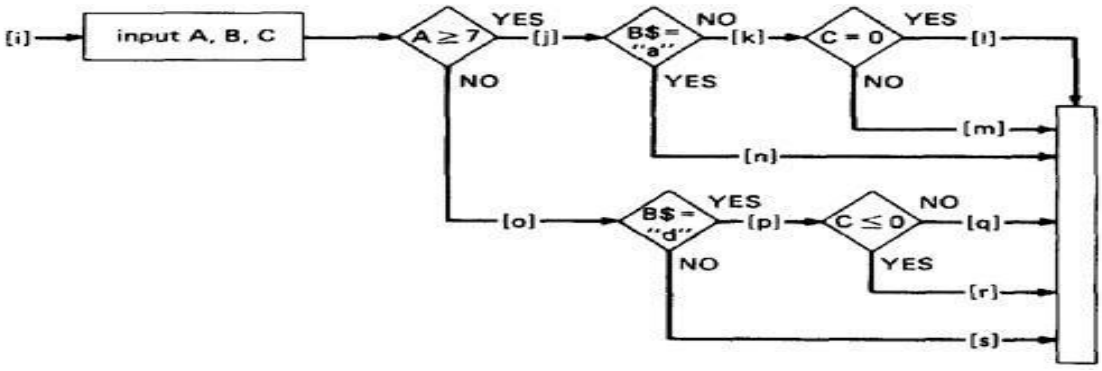


Figure 1.12: Single Link Marker Instrumentation

- **Why Single Link Markers aren't enough:** Unfortunately, a single link marker may not do the trick because links can be chewed by open bugs.

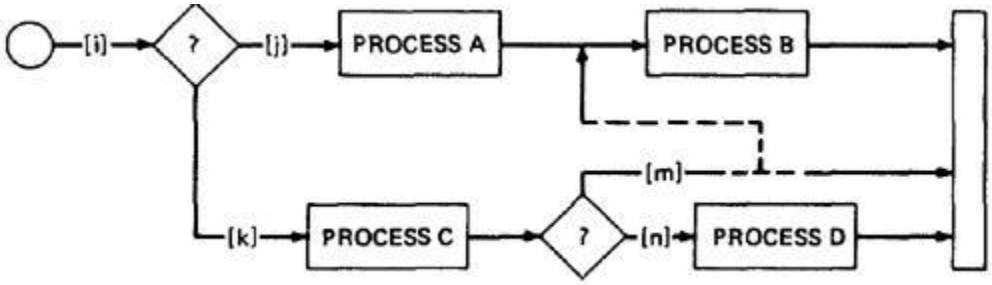


Figure 2.13: Why Single Link Markers aren't enough.

We intended to traverse the ikm path, but because of a rampaging GOTO in the middle of the m link, we go to process B. If coincidental correctness is against us, the outcomes will be the same and we won't know about the bug.

3. **Two Link Marker Method:**
   - The solution to the problem of single link marker method is to implement two markers per link: one at the beginning of each link and on at the end.
   - The two link markers now specify the path name and confirm both the beginning and end of the link.

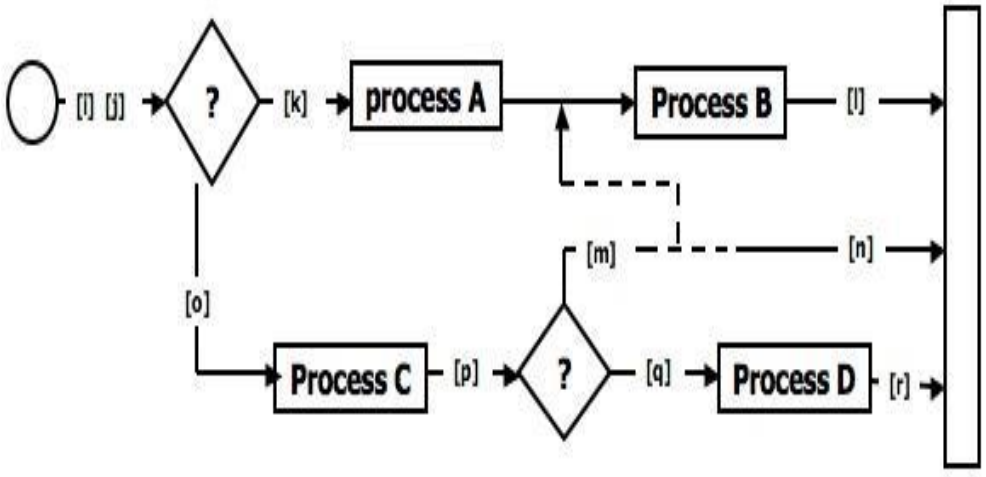


Figure 2.14: Double Link Marker Instrumentation.

4. **Link Counter:** A less disruptive (and less informative) instrumentation method is based on counters. Instead of a unique link name to be pushed into a string when the link is traversed, we simply increment a link counter. We now confirm that the path length is as expected. The same problem that led us to double link markers also leads us to double link counters.

UINIT-I

Assignment Questions:

1. a) Why is it impossible for a tester to find all the bugs in a system? Why might it not be necessary for program to be completely free of defects before it is delivered to its customer?
   b) To what extent can testing be used to validate that the program is fit for its purpose? Discuss.

2. a) What is meant by integration testing? Discuss the goals of integration testing and consequences of Bugs.
   (b) State whether the designer and tester are same? If not in what phases of testing the designer and tester will be different? Why?

3. a) State and explain various dichotomies in software testing.
   b) What are the Structural bugs, Coding bugs, data bugs and System bugs? Discuss how these bugs can be caught

4. (a) What are the various approaches for creation of good software? Discuss them clearly.
   (b) Distinguish between testing and debugging.

5. (a) An organization must define own nightmare on bugs. Explain how should you go about quantifying the nightmare?
   (b) Discuss clearly about code bugs.

6. (a) Discuss how software testing will ensure the quality of path instrumentation.
   (b) Discuss the trade-off between quality assurance and manufacturing costs.
7. (a). Define loop? Explain the variable loops with an example?
   (b). Explain the concatenated loops with an example.

8. (a).State and explain various kinds of predicates blindness with suitable examples.
   (b). What are link counters? Discuss their use in path testing.

9. (a) what is meant by program's control flow ? how it is useful for path testing?
   (b) Discuss various flow graph elements with their notations.

10. (a) Discuss clearly how the path sensitizing can be done.
    (b) what is the need for path instrumentation? Explain any one method for path instrumentation?

11. (a) Explain with a suitable Example how to convert a multi-exit routine to an equivalent single-
    exit routine.
    (b). Discuss the path testing strategy for multi-entry/multi –exit routines?

12. Discuss the following terms in detail(a) Predicates (b) Path predicates (c) Achievable paths

Short Answer Type Questions:

1. Why is it impossible for a tester to find all the bugs in a system?
2. To what extent can testing be used to validate that the program is fit for its purpose?
3. What is meant by integration testing?
4. Discuss the goals of integration testing and consequences of Bugs.
5. State whether the designer and tester are same? If not in what phases of testing the designer and tester will be different? Why?
6. What are the various approaches for creation of good software?
7. Distinguish between testing and debugging.
8. An organization must define own nightmare on bugs. Explain how should you go about quantifying the nightmare?
9. Discuss clearly about code bugs.
10. Discuss the trade-off between quality assurance and manufacturing costs.
11. Discuss how software testing will ensure the quality of path instrumentation.
12. Discuss the trade-off between quality assurance and manufacturing costs.
13. Define loop? Explain the variable loops with an example?
14. Explain the concatenated loops with an example.
15. State and explain various kinds of predicates blindness with suitable examples.
16. What are link counters? Discuss their use in path testing.
17. What is meant by program's control flow ?
18. Discuss various flow graph elements with their notations.
19. What is the need for path instrumentation?
20. Explain with a suitable Example how to convert a multi-exit routine to an equivalent single-exit routine.
21. Discuss the following terms in detail (a) Predicates (b) Path predicates (c) Achievable paths

Essay Type Questions:

1. Why is it impossible for a tester to find all the bugs in a system? Why might it not be necessary for a program to be completely free of defects before it is delivered to its customers?

2. To what extent can testing be used to validate that the program is fit for its purpose. Discuss?
3. What is meant by integration testing? Goals of Integration Testing?
4. Explain white-box testing and behavioral testing?
5. State and explain various dichotomies in software testing?
6. Discuss about requirements, features and functionality bugs.
7. What are control and sequence bugs? How they can be caught?
8. Consider the following flow - graph? Select optimal number of paths to achieve C1+C2 (statement coverage + branch coverage).
9. Explain various loops with an example?
10. Explain concatenated loops with an example?
11. State and explain various kinds of predicate blindness with examples?
12. What are link counters? Discuss their use in path testing?
13. Discuss Traversal marker with an example. (Link marker)
14. What is meant by Co - incidental Correctness with example.
15. What is meant by statement testing and branch testing with an example.
16. State and explain various path selection rules.
17. What is meant by program‘s control flow? How is it useful for path testing?
18. Discuss various flow graph elements with their notations.

Objective Questions:

Choose the correct answer

1. According to phase 1 of testers mental ife
   a)testing shows software works
   b)testing shows software doesn‘t work
   c)testing=debugging
   d)testing is not an act

2. Syntax errors are
   a)data bugs
   b)logic bugs
   c)coding bugs
   d)structure bugs

3. The first goal of testing is
   a)bug detection
   b)bug prevention
   c)bug correction
   d)to calculate the cost of the bug

4. the abbreviation of SQA is
   a)system quality assistance
   b)software quality assistance
   c)system quality assurance
   d)software quality assurance

5. what is the purpose of testing
   a)to find the error
   b)to show program has bugs
   c)to correct the error
   d)none of these

6. functional testing is also known as
   a)black box
   b)white box
   c)glass box
   d)open box

7. the language syntax and semantics eliminates most of the bugs this belief is known as
   a)control bug dominance
   b)data separation
   c)lingua salvator estimate
   d)angelic testers

8. _____ is not the consequence of bugs.
   a)serious
   b)extreme
   c)infectious
   d)none

9. the pesticide paradox testing is
   a)testing shows all bugs
   b)complexity of software grows to the limit of managerial ability
   c)a method to find bugs leaves subtler bugs
   d)testing doesn‘t show all bugs

10. the remedies for testbugs bugs doesn‘t include
    a)debugging
    b)design automation
    c)test execution automation
    d)test consequences

11. incorrect design of test cases is an example of
    a)logic bugs
    b)data bugs
    c)processing bugs
    d)requirement bugs

12. the methods to prevent bugs other than testing are
    a)reviews
    b)syntax checking
    c)inspections
    d)all the above

13. the program staff for the project should be
    a)10-20
    b)20-30
    c)25-45
    d)15-20

14. the process of testing entire system is
    a)system testing
    b)complete testing
    c)integration testing
    d)software testing

15. acceptance test is done
    a)after accepting a system
    b)to know users need
    c)to know whether to accept a system or not
    d)to know the ability of the programmer

16. _____is the graphical representation of programs control structure
    a)flowchart
    b)control flowgraph
    c)graphic matrix
    d)none

17. junction is generally denoted
    a)rectangle
    b)rhombus
    c)circle
    d)line

18. _____ are more preferred in process design
    a)flow charts
    b)algorithms
    c)flow graphs
    d)none

19. 100% statement coverage is denoted by
    a)C1
    b)C2
    c)C1+C2
    d)C1-C2

20. the path seleted doesn‘t follow the rule of
    a)from entry to exit
    b)simple
    c)short
    d)containing loops

21. which is true in the case of flow charts a)there are fixed rules in desigining b)there are no rules for desigining c)detai;s of process blocks are not shown
    d)it ignores all process steps

22. path segments are also known
    a)sub paths
    b)off paths
    c)subways
    d)path parameters

23. path testing with C1+C2 is tool for rehosting
    a)new software
    b)old software
    c)off shelf software
    d)component based software

24. the _____ is what we expect to happen as a result of test
    a)outcome
    b)output
    c)result
    d)none

25. the Boolean expression associated with the path is
    a)predicate
    b)Boolean path
    c)path expression
    d)predict expression

26. the methods of instrumentation in path testing does not include
    a)link markers
    b)link counters
    c)bitmap
    d)none of these

27. if every combination of values of two variables cannot be independently specified thenthey are said to be
    a)correlated
    b)independent
    c)dependent
    d)uncorrelated

28. the last step in heuristic procedure for path sensitizing is
    a)examining the predicates
    b)usage of predicates
    c)identifying the variables
    d)satisfying the inequalities

Feeling the blanks

29. can a bug free product delivery be guaranteed with testing? _____
30. structural testing is also known as _____
31. the final recipient of the system is known as _____
32. no two systems would be identical but they can have ____ %of code in common
33. main()
    {
    int a,b;
    c=a+b;
    }
    the above is example of _____ bugs
34. the most important criteria for designing interface is _____
35. _____ and _____ are considered as programs environment
36. consequences of bugs range from _____to _____
37. _____ is the process in which components are combined to form a larger component
38. two goals fo testing are _____ and _____
39. two types of test cases are _____and _____
40. _____ is the sequence of the program sequence of program statements which do not have any decisions or junctions

41. a point where control flow can merge is _____
42. the arrows in the control flow graph graph are _____
43. if all the paths in the program are convered then it is known as _____
44. in path testing,the path should be taken in such a way to achieve _____
45. three kinds of loops _____
46. path testing is first used on _____component in case of maintainence
47. path testing is used in _____ testing for new software
48. link marker is the effective form of _____
49. a predicate associated with a path is _____
50. the situation where a desired path is achieved for wrong reasons is _____

KEY

UNIT - I

Q.No.	Answer	Q.No.	Answer	Q.No.	Answer
1	a	18	c	35	Hardware, software
2	c	19	a	36	Mild, catastrophic
3	b	20	d	37	Integration
4	d	21	c	38	Bug Prevetion , Bug Dtection
5	b	22	a	39	Formal , Informal
6	a	23	b	40	Process block
7	c	24	a	41	Junction
8	d	25	d	42	Links
9	c	26	d	43	100% path coverage
10	d	27	a	44	C1+C2
11	a	28	d	45	Nested, concocted, horrible

12	**d**	**29**	**No**	**46**	**Modified**
13	**b**	**30**	**White box testing**	**47**	**Unit**
14	**a**	**31**	**User**	**48**	**Instrumentation**
15	**c**	**32**	**75%**	**49**	**Path predicate**
16	**b**	**33**	**Initialization**	**50**	**Testing blindness**
17	**c**	**34**	**Robustness**		

UNIT – 2

UNIT – 2: TRANSACTION FLOW TESTING AND DATA FLOW TESTING

TRANSACTION FLOWS:

- **INTRODUCTION:**
  - A transaction is a unit of work seen from a system user's point of view.
  - A transaction consists of a sequence of operations, some of which are performed by a system, persons or devices that are outside of the system.
  - Transaction begin with Birth-that is they are created as a result of some external act.
  - At the conclusion of the transaction's processing, the transaction is no longer in the system.
  - **Example of a transaction:** A transaction for an online information retrieval system might consist of the following steps or tasks:
    - Accept input (tentative birth)
    - Validate input (birth)
    - Transmit acknowledgement to requester
    - Do input processing
    - Search file
    - Request directions from user
    - Accept input
    - Validate input
    - Process request
    - Update file
    - Transmit output
    - Record transaction in log and clean up (death)
- **TRANSACTION FLOW GRAPHS:**
  - Transaction flows are introduced as a representation of a system's processing.
  - The methods that were applied to control flow graphs are then used for functional testing.
  - Transaction flows and transaction flow testing are to the independent system tester what control flows are path testing are to the programmer.
  - The transaction flow graph is to create a behavioral model of the program that leads to functional testing.
  - The transaction flowgraph is a model of the structure of the system's behavior (functionality).
  - An example of a Transaction Flow is as follows:

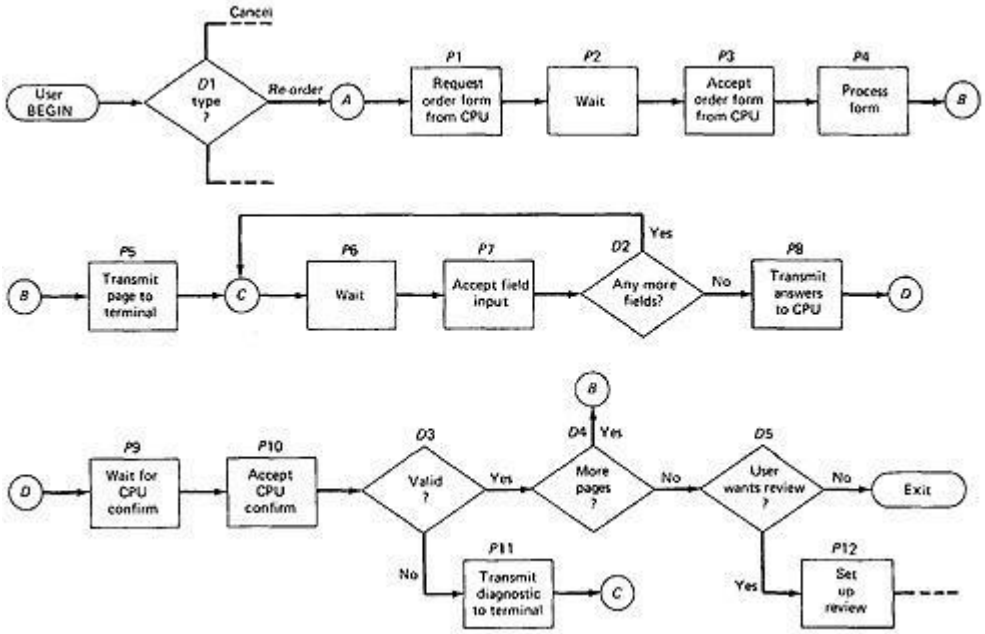


Figure 3.1: An Example of a Transaction Flow

- **USAGE:**
  - Transaction flows are indispensable for specifying requirements of complicated systems, especially online systems.
  - A big system such as an air traffic control or airline reservation system, has not hundreds, but thousands of different transaction flows.
  - The flows are represented by relatively simple flowgraphs, many of which have a single straight-through path.
  - Loops are infrequent compared to control flowgraphs.
  - The most common loop is used to request a retry after user input errors. An ATM system, for example, allows the user to try, say three times, and will take the card away the fourth time.
- **COMPLICATIONS:**
  - In simple cases, the transactions have a unique identity from the time they're created to the time they're completed.
  - In many systems the transactions can give birth to others, and transactions can also merge.
  - **Births:**There are three different possible interpretations of the decision symbol, or nodes with two or more out links. It can be a Decision, Biosis or a Mitosis.
    1. **Decision:**Here the transaction will take one alternative or the other alternative but not both. (See Figure 3.2 (a))
    2. **Biosis:**Here the incoming transaction gives birth to a new transaction, and both transaction continue on their separate paths, and the parent retains it identity. (See Figure 3.2 (b))
    3. **Mitosis:**Here the parent transaction is destroyed and two new transactions are created.(See Figure 3.2 (c))

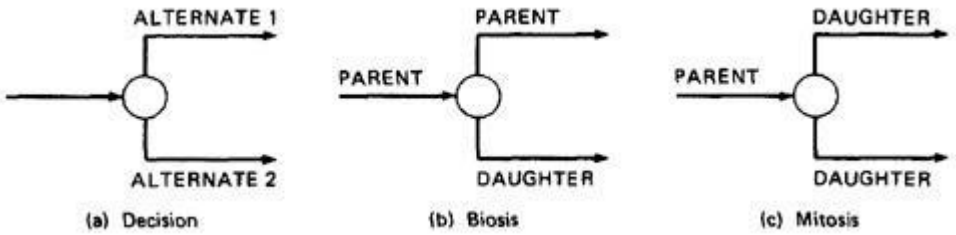


Figure 3.2: Nodes with multiple outlinks

Mergers: Transaction flow junction points are potentially as troublesome as transaction flow splits. There are three types of junctions: (1) Ordinary Junction (2) Absorption (3) Conjugation

0. **Ordinary Junction:** An ordinary junction which is similar to the junction in a control flow graph. A transaction can arrive either on one link or the other. (See Figure 3.3 (a))
1. **Absorption:** In absorption case, the predator transaction absorbs prey transaction. The prey gone but the predator retains its identity. (See Figure 3.3 (b))
2. **Conjugation:** In conjugation case, the two parent transactions merge to form a new daughter. In keeping with the biological flavor this case is called as conjugation.(See Figure 3.3 (c))

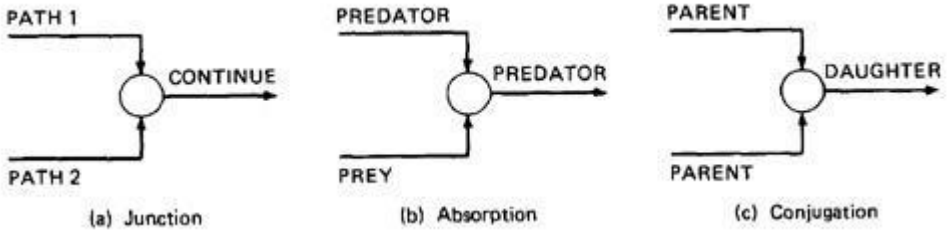


Figure 3.3: Transaction Flow Junctions and Mergers

We have no problem with ordinary decisions and junctions. Births, absorptions, and conjugations are as problematic for the software designer as they are for the software modeler and the test designer; as a consequence, such points have more than their share of bugs. The common problems are: lost daughters, wrongful deaths, and illegitimate births.

TRANSACTION FLOW TESTING TECHNIQUES:

- **GET THE TRANSACTIONS FLOWS:**
  - Complicated systems that process a lot of different, complicated transactions should have explicit representations of the transactions flows, or the equivalent.
  - Transaction flows are like control flow graphs, and consequently we should expect to have them in increasing levels of detail.
  - The system's design documentation should contain an overview section that details the main transaction flows.
  - Detailed transaction flows are a mandatory pre requisite to the rational design of a system's functional test.
- **INSPECTIONS, REVIEWS AND WALKTHROUGHS:**
  - Transaction flows are natural agenda for system reviews or inspections.
  - In conducting the walkthroughs, you should:
    - Discuss enough transaction types to account for 98%-99% of the transaction the system is expected to process.
    - Discuss paths through flows in functional rather than technical terms.
    - Ask the designers to relate every flow to the specification and to show how that transaction, directly or indirectly, follows from the requirements.
  - Make transaction flow testing the corner stone of system functional testing just as path testing is the corner stone of unit testing.
  - Select additional flow paths for loops, extreme values, and domain boundaries.
  - Design more test cases to validate all births and deaths.
  - Publish and distribute the selected test paths through the transaction flows as early as possible so that they will exert the maximum beneficial effect on the project.
  -
- **PATH SELECTION:**
  - Select a set of covering paths (c1+c2) using the analogous criteria you used for structural path testing.
  - Select a covering set of paths based on functionally sensible transactions as you would for control flow graphs.
  - Try to find the most tortuous, longest, strangest path from the entry to the exit of the transaction flow.
- **PATH SENSITIZATION:**
  - Most of the normal paths are very easy to sensitize-80% - 95% transaction flow coverage (c1+c2) is usually easy to achieve.
  - The remaining small percentage is often very difficult.
  - Sensitization is the act of defining the transaction. If there are sensitization problems on the easy paths, then bet on either a bug in transaction flows or a design bug.
- **PATH INSTRUMENTATION:**
  - Instrumentation plays a bigger role in transaction flow testing than in unit path testing.
  - The information of the path taken for a given transaction must be kept with that transaction and can be recorded by a central transaction dispatcher or by the individual processing modules.
  - In some systems, such traces are provided by the operating systems or a running

log.

- **DATA FLOW TESTING:**
  - Data flow testing is the name given to a family of test strategies based on selecting paths through the program's control flow in order to explore sequences of events related to the status of data objects.
  - For example, pick enough paths to assure that every data object has been initialized prior to use or that all defined objects have been used for something.
  - **Motivation:**

    it is our belief that, just as one would not feel confident about a program without executing every statement in it as part of some test, one should not feel confident about a program without having seen the effect of using the value produced by each and every computation.

- **DATA FLOW MACHINES:**
  - There are two types of data flow machines with different architectures. (1) Von Neumann machnes (2) Multi-instruction, multi-data machines (MIMD).
  - **Von Neumann Machine Architecture:**
    - Most computers today are von-neumann machines.
    - This architecture features interchangeable storage of instructions and data in the same memory units.
    - The Von Neumann machine Architecture executes one instruction at a time in the following, micro instruction sequence:
      1. Fetch instruction from memory
      2. Interpret instruction
      3. Fetch operands
      4. Process or Execute
      5. Store result
      6. Increment program counter
      7. GOTO 1
  - **Multi-instruction, Multi-data machines (MIMD) Architecture:**
    - These machines can fetch several instructions and objects in parallel.
    - They can also do arithmetic and logical operations simultaneously on different data objects.
    - The decision of how to sequence them depends on the compiler.
- **BUG ASSUMPTION:**
  - The bug assumption for data-flow testing strategies is that control flow is generally correct and that something has gone wrong with the software so that data objects are not available when they should be, or silly things are being done to data objects.
  - Also, if there is a control-flow problem, we expect it to have symptoms that can be detected by data-flow analysis.
  - Although we'll be doing data-flow testing, we won't be using data flowgraphs as such. Rather, we'll use an ordinary control flowgraph annotated to show what happens to the data objects of interest at the moment.
- **DATA FLOW GRAPHS:**
  - The data flow graph is a graph consisting of nodes and directed links.

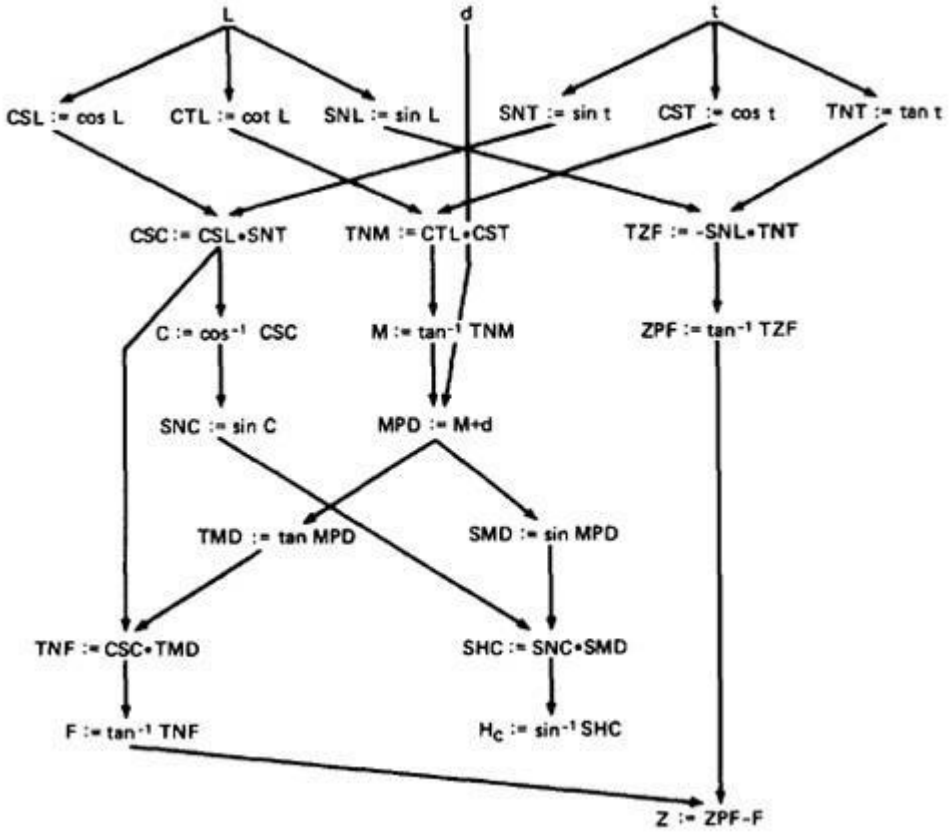


Figure 3.4: Example of a data flow graph

- We will use an control graph to show what happens to data objects of interest at that moment.
- Our objective is to expose deviations between the data flows we have and the data flows we want.
- **Data Object State and Usage:**
  - Data Objects can be created, killed and used.
  - They can be used in two distinct ways: (1) In a Calculation (2) As a part of a Control Flow Predicate.
  - The following symbols denote these possibilities:
    1. **Defined:** d - defined, created, initialized etc
    2. **Killed or undefined:** k - killed, undefined, released etc
    3. **Usage:** u - used for something (c - used in Calculations, p - used in a predicate)
  - **1. Defined (d):**
    - An object is defined explicitly when it appears in a data declaration.
    - Or implicitly when it appears on the left hand side of the assignment.
    - It is also to be used to mean that a file has been opened.
    - A dynamically allocated object has been allocated.
    - Something is pushed on to the stack.

- A record written.

2. Killed or Undefined (k):

- An object is killed on undefined when it is released or otherwise made unavailable.
- When its contents are no longer known with certitude (with aboslute certainity / perfectness).
- Release of dynamically allocated objects back to the availability pool.
- Return of records.
- The old top of the stack after it is popped.
- An assignment statement can kill and redefine immediately. For example, if A had been previously defined and we do a new assignment such as A : = 17, we have killed A's previous value and redefined A

3. Usage (u):

- A variable is used for computation (c) when it appears on the right hand side of an assignment statement.
- A file record is read or written.
- It is used in a Predicate (p) when it appears directly in a predicate.

DATA FLOW ANOMALIES:

An anomaly is denoted by a two-character sequence of actions.

For example, ku means that the object is killed and then used, where as dd means that the object is defined twice without an intervening usage.

What is an anomaly is depend on the application.

There are nine possible two-letter combinations for d, k and u. some are bugs, some are suspicious, and some are okay.

0. **dd** :- probably harmless but suspicious. Why define the object twice without an intervening usage?
1. **dk** :- probably a bug. Why define the object without using it?
2. **du** :- the normal case. The object is defined and then used.
3. **kd** :- normal situation. An object is killed and then redefined.
4. **kk** :- harmless but probably buggy. Did you want to be sure it was really killed?
5. **ku** :- a bug. the object doesnot exist.
6. **ud** :- usually not a bug because the language permits reassignment at almost any time.
7. **uk** :- normal situation.
8. **uu** :- normal situation.

In addition to the two letter situations, there are six single letter situations.

We will use a leading dash to mean that nothing of interest (d,k,u) occurs prior to the action noted along the entry-exit path of interest.

A trailing dash to mean that nothing happens after the point of interest to the exit.

They possible anomalies are:

0. **-k** :- possibly anomalous because from the entrance to this point on the path, the variable had not been defined. We are killing a variable that does not exist.
1. **-d** :- okay. This is just the first definition along this path.
2. **-u** :- possibly anomalous. Not anomalous if the variable is global and has been previously defined.
3. **k-** :- not anomalous. The last thing done on this path was to kill the variable.
4. **d-** :- possibly anomalous. The variable was defined and not used on this path. But this could be a global definition.

5. **u-** :- not anomalous. The variable was used but not killed on this path. Although this sequence is not anomalous, it signals a frequent kind of bug. If d and k mean dynamic storage allocation and return respectively, this could be an instance in which a dynamically allocated object was not returned to the pool after use.

DATA FLOW ANOMALY STATE GRAPH:

Data flow anomaly model prescribes that an object can be in one of four distinct states:

0. **K** :- undefined, previously killed, doesnot exist
1. **D** :- defined but not yet used for anything
2. **U** :- has been used for computation or in predicate
3. **A** :- anomalous

These capital letters (K,D,U,A) denote the state of the variable and should not be confused with the program action, denoted by lower case letters.

Unforgiving Data - Flow Anomaly Flow Graph: Unforgiving model, in which once a variable becomes anomalous it can never return to a state of grace.

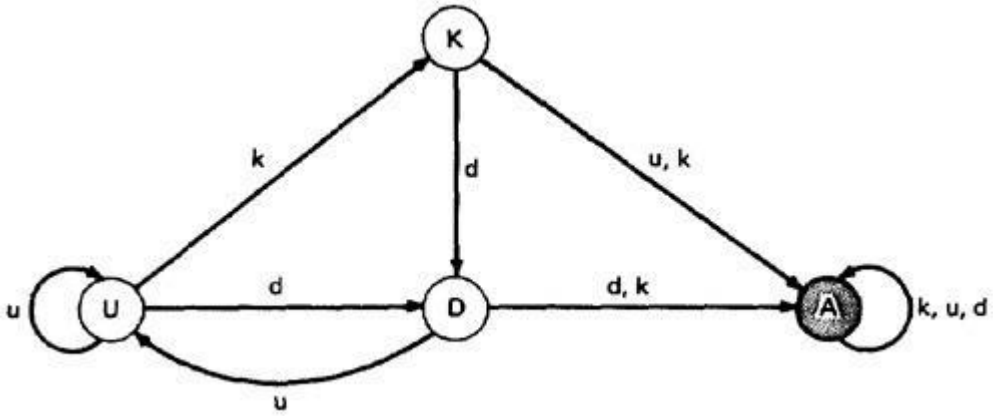


Figure 3.5: Unforgiving Data Flow Anomaly State Graph

Assume that the variable starts in the K state - that is, it has not been defined or does not exist. If an attempt is made to use it or to kill it (e.g., say that we're talking about opening, closing, and using files and that 'killing' means closing), the object's state becomes anomalous (state A) and, once it is anomalous, no action can return the variable to a working state. If it is defined (d), it goes into the D, or defined but not yet used, state. If it has been defined (D) and redefined (d) or killed without use (k), it becomes anomalous, while usage (u) brings it to the U state. If in U, redefinition (d) brings it to D, u keeps it in U, and k kills it.

Forgiving Data - Flow Anomaly Flow Graph: Forgiving model is an alternate model where redemption (recover) from the anomalous state is possible.

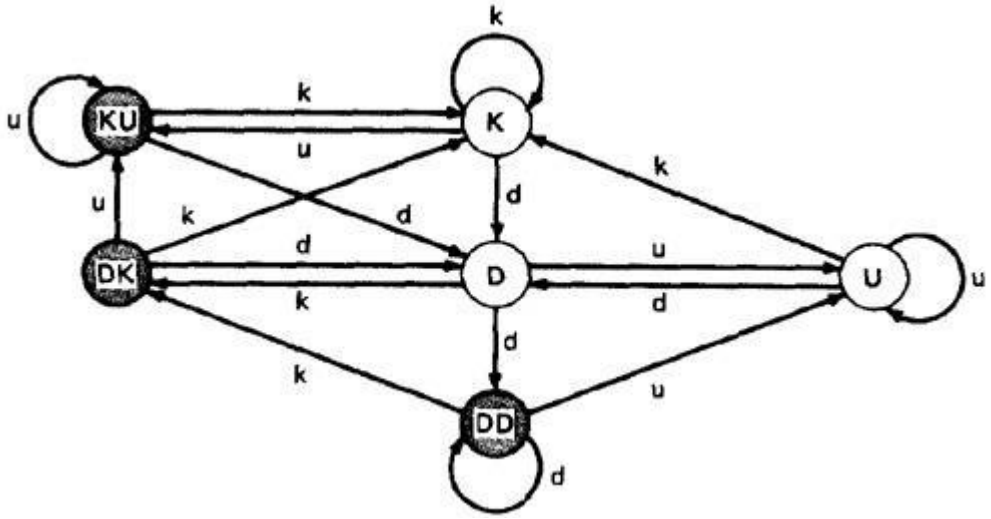


Figure 3.6: Forgiving Data Flow Anomaly State Graph

This graph has three normal and three anomalous states and he considers the kk sequence not to be anomalous. The difference between this state graph and Figure 3.5 is that redemption is possible. A proper action from any of the three anomalous states returns the variable to a useful working state.

The point of showing you this alternative anomaly state graph is to demonstrate that the specifics of an anomaly depends on such things as language, application, context, or even your frame of mind. In principle, you must create a new definition of data flow anomaly (e.g., a new state graph) in each situation. You must at least verify that the anomaly definition behind the theory or imbedded in a data flow anomaly test tool is appropriate to your situation.

STATIC Vs DYNAMIC ANOMALY DETECTION:

Static analysis is analysis done on source code without actually executing it. For example: source code syntax error detection is the static analysis result.

Dynamic analysis is done on the fly as the program is being executed and is based on intermediate values that result from the program's execution. For example: a division by zero warning is the dynamic result.

If a problem, such as a data flow anomaly, can be detected by static analysis methods, then it doesnot belongs in testing - it belongs in the language processor.

There is actually a lot more static analysis for data flow analysis for data flow anomalies going on in current language processors.

For example, language processors which force variable declarations can detect (-u) and (ku) anomalies.

But still there are many things for which current notions of static analysis are INADEQUATE.

Why Static Analysis isn't enough? There are many things for which current notions of static analysis are inadequate. They are:

- **Dead Variables:** Although it is often possible to prove that a variable is dead or alive at a given point in the program, the general problem is unsolvable.

- **Arrays:**Arrays are problematic in that the array is defined or killed as a single object, but reference is to specific locations within the array. Array pointers are usually dynamically calculated, so there's no way to do a static analysis to validate the pointer value. In many languages, dynamically allocated arrays contain garbage unless explicitly initialized and therefore, -u anomalies are possible.
- **Records and Pointers:**The array problem and the difficulty with pointers is a special case of multipart data structures. We have the same problem with records and the pointers to them. Also, in many applications we create files and their names dynamically and there's no way to determine, without execution, whether such objects are in the proper state on a given path or, for that matter, whether they exist at all.
- **Dynamic Subroutine and Function Names in a Call:**subroutine or function name is a dynamic variable in a call. What is passed, or a combination of subroutine names and data objects, is constructed on a specific path. There's no way, without executing the path, to determine whether the call is correct or not.
- **False Anomalies:**Anomalies are specific to paths. Even a "clear bug" such as ku may not be a bug if the path along which the anomaly exist is unachievable. Such "anomalies" are false anomalies. Unfortunately, the problem of determining whether a path is or is not achievable is unsolvable.
- **Recoverable Anomalies and Alternate State Graphs:**What constitutes an anomaly depends on context, application, and semantics. How does the compiler know which model I have in mind? It can't because the definition of "anomaly" is not fundamental. The language processor must have a built-in anomaly definition with which you may or may not (with good reason) agree.
- **Concurrency, Interrupts, System Issues:**As soon as we get away from the simple single-task uniprocessor environment and start thinking in terms of systems, most anomaly issues become vastly more complicated. How often do we define or create data objects at an interrupt level so that they can be processed by a lower-priority routine? Interrupts can make the "correct" anomalous and the "anomalous" correct. True concurrency (as in an MIMD machine) and pseudoconcurrency (as in multiprocessing) systems can do the same to us. Much of integration and system testing is aimed at detecting data-flow anomalies that cannot be detected in the context of a single routine.

Although static analysis methods have limits, they are worth using and a continuing trend in language processor design has been better static analysis methods, especially for data flow anomaly detection. That's good because it means there's less for us to do as testers and we have far too much to do as it is.

DATA FLOW MODEL:

The data flow model is based on the program's control flow graph - Don't confuse that with the program's data flowgraph..

Here we annotate each link with symbols (for example, d, k, u, c, p) or sequences of symbols (for example, dd, du, ddd) that denote the sequence of data operations on that link with respect to the variable of interest. Such annotations are called link weights.

The control flow graph structure is same for every variable: it is the weights that change.

Components of the model:

0. To every statement there is a node, whose name is unique. Every node has at least one outlink and at least one inlink except for exit

nodes and entry nodes.

1. Exit nodes are dummy nodes placed at the outgoing arrowheads of exit statements (e.g., END, RETURN), to complete the graph. Similarly, entry nodes are dummy nodes placed at entry statements (e.g., BEGIN) for the same reason.
2. The outlink of simple statements (statements with only one outlink) are weighted by the proper sequence of data-flow actions for that statement. Note that the sequence can consist of more than one letter. For example, the assignment statement A:= A + B in most languages is weighted by cd or possibly ckd for variable A. Languages that permit multiple simultaneous assignments and/or compound statements can have anomalies within the statement. The sequence must correspond to the order in which the object code will be executed for that variable.
3. Predicate nodes (e.g., IF-THEN-ELSE, DO WHILE, CASE) are weighted with the p - use(s) on every outlink, appropriate to that outlink.
4. Every sequence of simple statements (e.g., a sequence of nodes with one inlink and one outlink) can be replaced by a pair of nodes that has, as weights on the link between them, the concatenation of link weights.
5. If there are several data-flow actions on a given link for a given variable, then the weight of the link is denoted by the sequence of actions on that link for that variable.
6. Conversely, a link with several data-flow actions on it can be replaced by a succession of equivalent links, each of which has at most one data-flow action for any variable.

Let us consider the example:

CODE* (PDL)

```
      INPUT X, Y                    V(U-1):=V(U+1) + U(V-1)
      Z := X + Y                ELL:V(U+U(V)) := U + V
      V := X - Y                    IF U = V GOTO JOE
      IF Z >=Ø GOTO SAM             IF U > V THEN U := Z
JOE:  Z := Z - 1                    Z := U
SAM:  Z := Z + V                    END
      FOR U = Ø TO Z
      V(U),U(V) := (Z + V)*U
      IF V(U)= Ø GOTO JOE
      Z := Z - 1
      IF Z = Ø GOTO ELL
      U := U + 1
      NEXT U
```

* A contrived horror

Figure 3.7: Program Example (PDL)

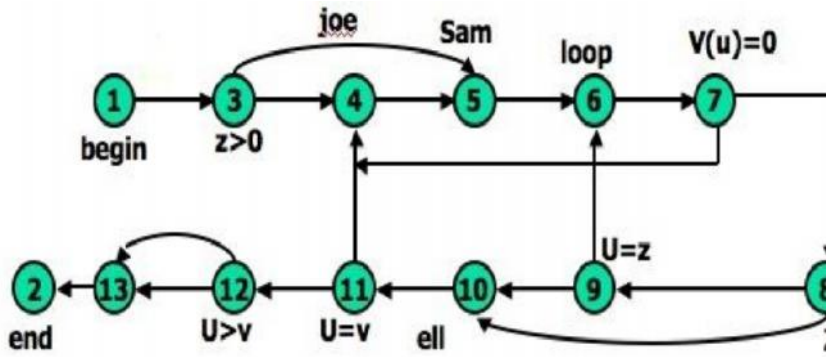


Figure 3.8: Unannotated flowgraph for example program in Figure 3.7

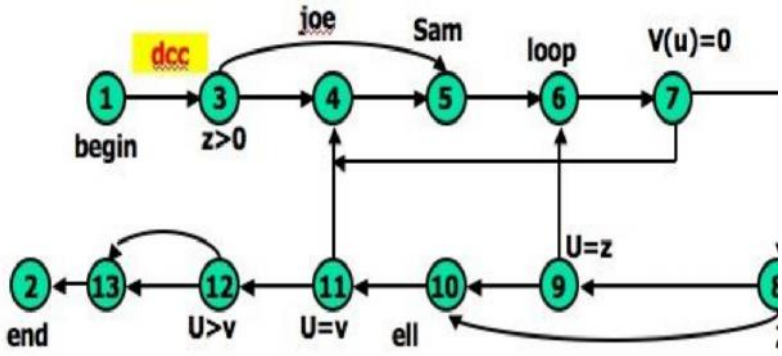


Figure 3.9: Control flowgraph annotated for X and Y data flows.

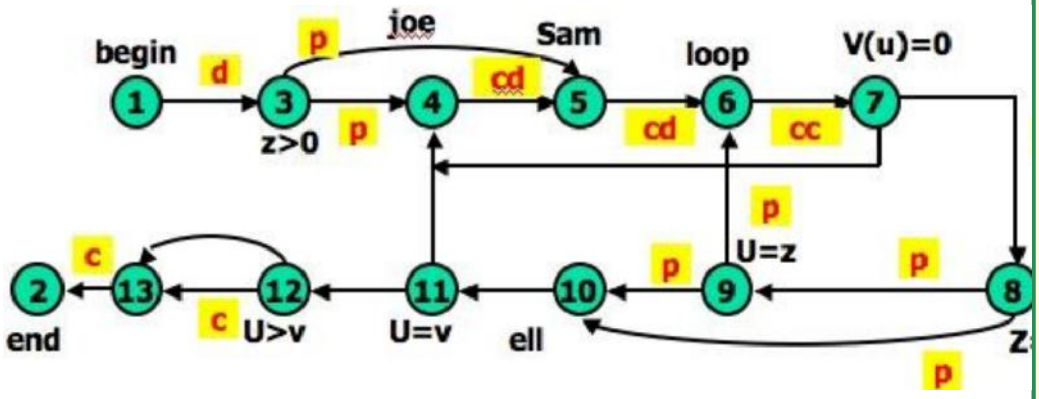


Figure 3.10: Control flowgraph annotated for Z data flow.

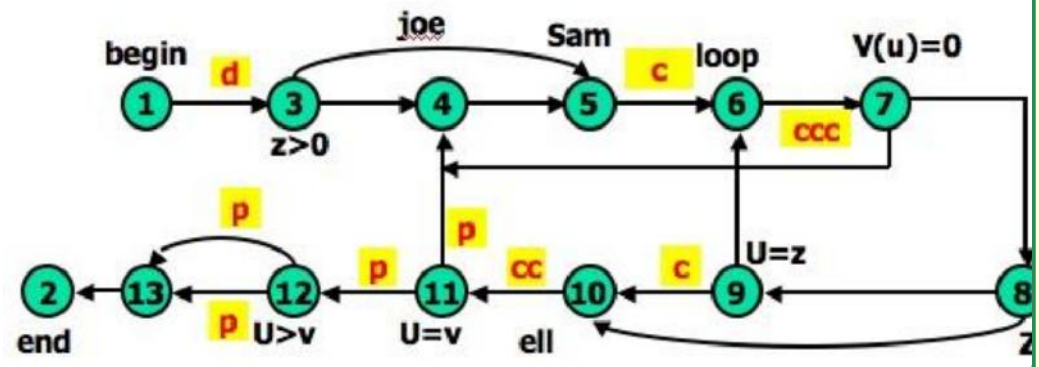


Figure 3.11: Control flowgraph annotated for V data flow.

STRATEGIES OF DATA FLOW TESTING:

- **INTRODUCTION:**
  - Data Flow Testing Strategies are structural strategies.
  - In contrast to the path-testing strategies, data-flow strategies take into account what happens to data objects on the links in addition to the raw connectivity of the graph.
  - In other words, data flow strategies require data-flow link weights (d,k,u,c,p).
  - Data Flow Testing Strategies are based on selecting test path segments (also called **sub paths**) that satisfy some characteristic of data flows for all data objects.
  - For example, all subpaths that contain a d (or u, k, du, dk).
  - A strategy X is **stronger** than another strategy Y if all test cases produced under Y are included in those produced under X - conversely for **weaker**.
- **TERMINOLOGY:**
  1. **Definition-Clear Path Segment**, with respect to variable X, is a connected sequence of links such that X is (possibly) defined on the first link and not redefined or killed on any subsequent link of that path segment. ll paths in Figure 3.9 are definition clear because variables X and Y are defined only on the first link (1,3) and not thereafter. In Figure 3.10, we have a more complicated situation. The following path segments are definition-clear: (1,3,4), (1,3,5), (5,6,7,4), (7,8,9,6,7), (7,8,9,10), (7,8,10), (7,8,10,11). Subpath (1,3,4,5) is not definition-clear because the variable is defined on (1,3) and again on (4,5). For practice, try finding all the definition-clear subpaths for this routine (i.e., for all variables).
  2. **Loop-Free Path Segment** is a path segment for which every node in it is visited atmost once. For Example, path (4,5,6,7,8,10) in Figure 3.10 is loop free, but path (10,11,4,5,6,7,8,10,11,12) is not because nodes 10 and 11 are each visited twice.
  3. **Simple path segment** is a path segment in which at most one node is visited twice. For example, in Figure 3.10, (7,4,5,6,7) is a simple path segment. A simple path segment is either loop-free or if there is a loop, only one node is involved.
  4. A **du path** from node i to k is a path segment such that if the last link has a computational use of X, then the path is simple and definition-clear; if the penultimate (last but one) node is j - that is, the path is (i,p,q,...,r,s,t,j,k) and link (j,k) has a predicate use - then the path from i to j is both loop-free and definition-clear.

STRATEGIES: The structural test strategies discussed below are based on the program's control flowgraph. They differ in the extent to which predicate uses and/or computational uses of variables are included in the test set. Various types of data flow testing strategies in decreasing order of their effectiveness are:

0. **All - du Paths (ADUP):** The all-du-paths (ADUP) strategy is the strongest data-flow testing strategy discussed here. It requires that every du path from every definition of every variable to every use of that definition be exercised under some test.

For variable X and Y:In Figure 3.9, because variables X and Y are used only on link (1,3), any test that starts at the entry satisfies this criterion (for variables X and Y, but not for all variables as required by the strategy).

For variable Z: The situation for variable Z (Figure 3.10) is more complicated because the variable is redefined in many places. For the definition on link (1,3) we must exercise paths that include subpaths (1,3,4) and (1,3,5). The definition on link (4,5) is covered by any path that includes (5,6), such as subpath (1,3,4,5,6, ...). The (5,6) definition requires paths that include subpaths (5,6,7,4) and (5,6,7,8).

For variable V: Variable V (Figure 3.11) is defined only once on link (1,3). Because V has a predicate use at node 12 and the subsequent path to the end must be forced for both directions at node 12, the all-du-paths strategy for this variable requires that we exercise all loop-free entry/exit paths and at least one path that includes the loop caused by (11,4). Note that we must test paths that include both subpaths (3,4,5) and (3,5) even though neither of these has V definitions. They must be included because they provide alternate du paths to the V use on link (5,6). Although (7,4) is not used in the test set for variable V, it will be included in the test set that covers the predicate uses of array variable V() and U.

The all-du-paths strategy is a strong criterion, but it does not take as many tests as it might seem at first because any one test simultaneously satisfies the criterion for several definitions and uses of several different variables.

1. **All Uses Startegy (AU):**The all uses strategy is that at least one definition clear path from every definition of every variable to every use of that definition be exercised under some test. Just as we reduced our ambitions by stepping down from all paths (P) to branch coverage (C2), say, we can reduce the number of test cases by asking that the test set should include at least one path segment from every definition to every use that can be reached by that definition.

   For variable V: In Figure 3.11, ADUP requires that we include subpaths (3,4,5) and (3,5) in some test because subsequent uses of V, such as on link (5,6), can be reached by either alternative. In AU either (3,4,5) or (3,5) can be used to start paths, but we don't have to use both. Similarly, we can skip the (8,10) link if we've included the (8,9,10) subpath. Note the hole. We must include (8,9,10) in some test cases because that's the only way to reach the c use at link (9,10) - but suppose our bug for variable V is on link (8,10) after all? Find a covering set of paths under AU for Figure 3.11.

2. **All p-uses/some c-uses strategy (APU+C) :** For every variable and every definition of that variable, include at least one definition free path from the definition to every predicate use; if there are definitions of the variables that are not covered by the above prescription, then add computational use test cases as required to cover every definition.

   For variable Z:In Figure 3.10, for APU+C we can select paths that all take the upper link (12,13) and therefore we do not cover the c-use of Z: but that's okay according to the strategy's definition because every definition is covered. Links (1,3), (4,5), (5,6), and (7,8) must be included because they contain definitions for variable Z. Links (3,4), (3,5), (8,9), (8,10), (9,6), and (9,10) must be included because they contain predicate uses of Z. Find a covering set of test cases under APU+C for all variables in this example - it only takes two tests.

For variable V:In Figure 3.11, APU+C is achieved for V by (1,3,5,6,7,8,10,11,4,5,6,7,8,10,11,12[upper], 13,2) and (1,3,5,6,7,8,10,11,12[lower], 13,2). Note that the c-use at (9,10) need not be included under the APU+C criterion.

3. **All c-uses/some p-uses strategy (ACU+P) :** The all c-uses/some p-uses strategy (ACU+P) is to first ensure coverage by computational use cases and if any definition is not covered by the previously selected paths, add such predicate use cases as are needed to assure that every definition is included in some test.

   For variable Z: In Figure 3.10, ACU+P coverage is achieved for Z by path (1,3,4,5,6,7,8,10, 11,12,13[lower], 2), but the predicate uses of several definitions are not covered. Specifically, the (1,3) definition is not covered for the (3,5) p-use, the (7,8) definition is not covered for the (8,9), (9,6) and (9, 10) p-uses.

   The above examples imply that APU+C is stronger than branch coverage but ACU+P may be weaker than, or incomparable to, branch coverage.

4. **All Definitions Strategy (AD) :** The all definitions strategy asks only every definition of every variable be covered by atleast one use of that variable, be that use a computational use or a predicate use.

   For variable Z: Path (1,3,4,5,6,7,8, . . .) satisfies this criterion for variable Z, whereas any entry/exit path satisfies it for variable V.

   From the definition of this strategy we would expect it to be weaker than both ACU+P and APU+C.

5. **All Predicate Uses (APU), All Computational Uses (ACU) Strategies :** The all predicate uses strategy is derived from APU+C strategy by dropping the requirement that we include a c-use for the variable if there are no p-uses for the variable. The all computational uses strategy is derived from ACU+P strategy by dropping the requirement that we include a p-use for the variable if there are no c-uses for the variable.

   It is intuitively obvious that ACU should be weaker than ACU+P and that APU should be weaker than APU+C.

ORDERING THE STRATEGIES:

- Figure 3.12 compares path-flow and data-flow testing strategies. The arrows denote that the strategy at the arrow's tail is stronger than the strategy at the arrow's head.

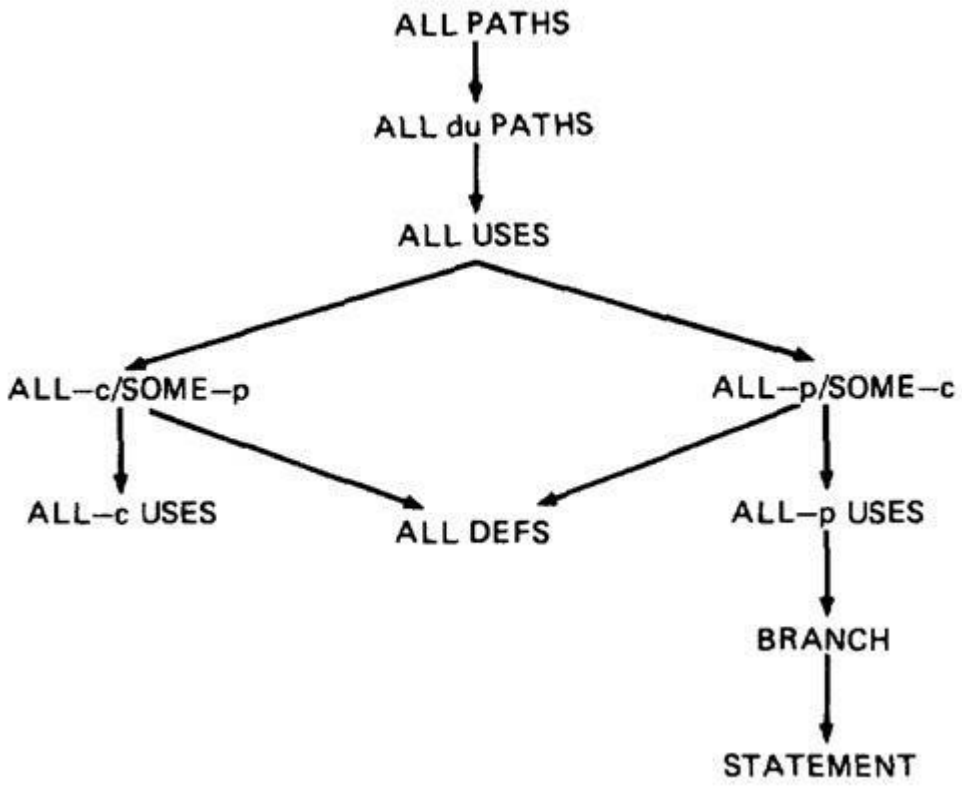


Figure 3.12: Relative Strength of Structural Test Strategies.

- The right-hand side of this graph, along the path from "all paths" to "all statements" is the more interesting hierarchy for practical applications.
- Note that although ACU+P is stronger than ACU, both are incomparable to the predicate-biased strategies. Note also that "all definitions" is not comparable to ACU or APU.

SLICING AND DICING:

- A (static) program **slice** is a part of a program (e.g., a selected set of statements) defined with respect to a given variable X (where X is a simple variable or a data vector) and a statement i: it is the set of all statements that could (potentially, under static analysis) affect the value of X at statement i - where the influence of a faulty statement could result from an improper computational use or predicate use of some other variables at prior statements.
- If X is incorrect at statement i, it follows that the bug must be in the program slice for X with respect to i
- A program **dice** is a part of a slice in which all statements which are known to be correct have been removed.
- In other words, a dice is obtained from a slice by incorporating information obtained through testing or experiment (e.g., debugging).
- The debugger first limits her scope to those prior statements that could have caused the faulty value at statement i (the slice) and then eliminates from further

consideration those statements that testing has shown to be correct.

- Debugging can be modeled as an iterative procedure in which slices are further refined by dicing, where the dicing information is obtained from ad hoc tests aimed primarily at eliminating possibilities. Debugging ends when the dice has been reduced to the one faulty statement.
- **Dynamic slicing** is a refinement of static slicing in which only statements on achievable paths to the statement in question are included.

UNIT II

Transaction Flow Testing and Data Flow Testing

Assignment Questions:

1. (a). Distinguish between control flow and transaction flow?

   (b). What is meant by transaction flow testing? Discuss its Significance

2. a. State and explain various types of data flow anomalies with suitable examples.

   b. discuss about static and dynamic anomaly detection.

3. (a)Discuss the following strategies of data flow testing with suitable examples

   i. All-Predicate uses (APU) strategy

   ii.All-computational (ACU) strategy

   (b)Compare the path flow and data-flow testing strategies.

4. (a) state and explain various transaction flow junctions and mergers.

   (b) explain the terms inspections. Reviews and Walkthroughs.

5. (a) What are the transaction flows? Discuss their complications.

   (b) What is meant by Data-flow testing? Discuss its significance.

6. a. Discuss the three possible interpretations of the decision symbol with two or more out links?

   b. What is meant by transaction flow Structure? Discuss the reasons why the transaction follows are often structured?

Short Answer Type Questions:

1. Distinguish between control flow and transaction flow?
2. What is meant by transaction flow testing? Discuss its Significance.
3. Discuss about static and dynamic anomaly detection.
4. Discuss the following strategies of data flow testing with suitable examples
   i. All-Predicate uses (APU) strategy
   ii.All-computational (ACU) strategy
5. Compare the path flow and data-flow testing strategies.
6. Explain the terms inspections, Reviews and Walkthroughs.
7. What are the transaction flows?
9. What is meant by Data-flow testing?
10. Discuss the three possible interpretations of the decision symbol with two or more out links?
11. What is meant by transaction flow Structure?

Essay Type Questions:

1. Distinguish Control Flow and Transaction flow.
2. What is meant by transaction flow testing. Discuss its significance.
3. Discuss in detail data - flow testing strategies.
4. What are data - flow anomalies? How data flow testing can explore them?
5. What are data-flow anomalies? How data flow testing can explore them?
6. What is meant by a program slice? Discuss about static and dynamic program slicing.
7. Explain the terms Dicing, Data-flow and Debugging.
8. What is meant by data flow model? Discuss various components of it?
9. Compare data flow and path flow testing strategies?
10. Explain data-flow testing with an example. Explain its generalizations and limitations.

Objective Type Questions:

Choose the correct answer

1. absorption can be dealt in a best way by
   a)following the predicator as the primary flow
   b)following the parent flow from the starting o the end
   c)following the birth of each parent
   d)following the additional flow to the daughter

2. C,P in case of data object state and usage are
   a)creation,participation
   b)creation,postulation
   c)calculation,predicate
   d)calculation,postulation

3. the statement that is true in case of transactional flow instrumentation is
   a)dispatchers are needed
   b)pay off is counters
   c)counters are useful
   d)counters are not useful

4. _____ are assumed problematic for software designers.
   a)births
   b)absorptions
   c)conjugations
   d)all the above

5. the methods of sensitization in transaction flows include
   a)using of patches
   b)use break points
   c)counters
   d)processing queue

6. FSM implementation is an example of
   a)recovery
   b)transaction dispatcher
   c)control flow
   d)processing queues
7. the state of dataobjects cannot be
   a)created
   b)killed
   c)used
   d)modified

8. main()

   {
   int a=10; int b=10;

}
the above is the example of
a)dk anomaly
b)du anomaly
c)dd anomaly
d)none

9. direct relation does not exist between processes and decisions in
a)data flow diagram
b)transaction flow diagram
c)both a) and b)
d)none

10. the path segment for which every node is visited atmost once is said to be
a)du path
b)simple path segment
c)loop free pat
d)definition clear path segment

11. every definition of every variable is covered in
a)ad strategy
b)apu strategy
c)au strategy
d)adup strategy

12. sequential machine consists of _____ processes
a)one
b)two
c)many
d)infinite

13. the normal sequence with respect to life time of a variable among following is
a)kk
b)dd
c)dk
d)uu

14. a=0;
b=a;
the statement represents the sequence of
a)du
b)uu
c)ud
d)dd

15. the correct sequence of transaction flow is
a)input,validate,acknowledge,record transaction
b)input,acknowledge,record transaction
c)acknowledge,input,validate record,transaction

d)record transaction,input,validate,acknowledge

fill in the blanks

16. the transaction flow graph is used for _____ testing
17. a _____ is a unit of work done
18. the complications of transaction flows are _____ and _____
19. transaction flows are natural agenda for _____
20. TCB stands for _____
21. static analysis is done at _____ time
22. the three anomaly states are _____
23. to bridge the gap between debugging and testing is the concept of _____
24. in arrays _____ analysis is used
25. if then else,do while are examples of _____nodes
26. maintenance testing is similar to _____
27. _____ is derived from ACP+P by dropping p-use
28. _____ are used in case of hard to sensitize path
29. the strategy in which for variable and every definition of variable includes at least one definition free path from the definition to every predicate is known as all ___
30. _____ machines have the feature of interchangeable storage of instructions

KEY UNIT - II

Q.No	Answer	Q.No.	Answer	Q.No.	Answer
1	**a**	**11**	**a**	**21**	**Compile**
2	**c**	**12**	**a**	**22**	**ku, dk, dd**
3	**d**	**13**	**c**	**23**	**Data flow testing**
4	**d**	**14**	**a**	**24**	**Dynamic**
5	**d**	**15**	**a**	**25**	**Predicate**
6	**b**	**16**	**Functional**	**26**	**Debugging**
7	**d**	**17**	**Transaction**	**27**	**aw**
8	**a**	**18**	**Births & Merges**	**28**	**Break points**
9	**b**	**19**	**Rewiew and Inspection**	**29**	**p uses/ some c uses**
10	**c**	**20**	**Transaction control block**	**30**	**vonneuman**