
Peer reviewed version

Link to published version (if available):
10.1109/MTV.2015.15

Link to publication record in Explore Bristol Research
PDF-document

This is the author accepted manuscript (AAM). The final published version (version of record) is available online via IEEE at http://ieeexplore.ieee.org/document/7548935/. Please refer to any applicable terms of use of the publisher.
Novel MC/DC Coverage Test Sets Generation Algorithm, and MC/DC Design Fault Detection Strength Insights

Mohamed A. Salem
Computer Science Department, Faculty of Engineering
University of Bristol, UK
Email:csmams@my.bristol.ac.uk

Kerstin I. Eder
Computer Science Department, Faculty of Engineering
University of Bristol, UK
Email:kerstin.eder@bristol.ac.uk

Abstract—This paper introduces Modified Condition/Decision Coverage (MC/DC), novel MC/DC coverage test sets generation algorithm named OBSRV, and MC/DC design fault detection strength. The paper presents an overview about MC/DC in terms of the MC/DC definition, MC/DC types, and the conventional MC/DC approaches. It introduces a novel algorithm, called OBSRV, for MC/DC coverage test sets generation. OBSRV resolves MC/DC controllability and observability by using principles found in the D-algorithm that is the foundation for state-of-the-art ATPG. It thereby leverages hardware test principles to advance MC/DC for software, and hardware structural coverage. The paper presents an investigation of the introduced OBSRV algorithm scalability, and complexity to prove its suitability for practical designs. The paper investigates MC/DC functional design faults detection strength, and analyzes empirical results conducted on main design fault classes in microprocessors.

I. INTRODUCTION AND MOTIVATION

The main objective of the verification process is to identify design faults that have been introduced during the transformation of design specification into implementation source code, ie RTL. Coverage is a metric of verification progress versus the verification plan objectives as functional coverage, and versus the implementation source code as structural coverage.

Requirements coverage analysis determines the design implementation compliance with the functional requirements, and establishes traceability between the requirements, and the functional tests. Structural coverage analysis aims to establish how well the requirements-based test suite has exercised the design implementation source code structure, and determines code coverage gaps. In practice, especially for safety-critical applications, requirements coverage analysis is combined with structural coverage analysis to ensure high level of confidence that the design implementation has no unintended functions.

MC/DC coverage is a structural coverage metric originally used for the certification of critical software for avionics applications as required by RTCA/DO-178B [1]. MC/DC is a form of expression coverage demonstrating that the implementation has controllable and observable control flow logic [2]. MC/DC introduces cost-effective coverage solution in terms of the linear growth of the size of coverage test set to the exponential growth that requires $2^N$ tests, where $N$ is the number of conditions in a decision statement.

II. PAPER OUTLINE

This paper is organized as follows: Section III introduces the paper definitions and notations, Section IV gives an overview of MC/DC coverage metrics in terms of MC/DC coverage definition, independence pairs, MC/DC coverage types, and MC/DC conventional approaches. Section V introduces the OBSRV usage model, D-algorithm overview, OBSRV procedures, a simple example elaborating the OBSRV usage model, and ends with an investigation of the OBSRV algorithm scalability, and complexity. Section VI experimentally evaluates the MC/DC functional design fault detection strength versus common design fault classes in microprocessors. Finally, Section VII summarizes and concludes with an outlook on future research.

III. DEFINITIONS AND NOTATIONS

The following notational conventions are used throughout the paper: boolean operators are denoted by and, or, xor, not. Boolean conditions and decisions are denoted by bold capitals such as A, B, C, etc. Truth values are written as either true and false, or T and F. A test for a boolean function with n inputs is denoted by $V = (V_1 V_2 \cdots V_n)$, where $V_i$ is T or F. Test vectors can be represented by their equivalent decimal value, ie the test $V = (FTFT)$ is referred to as test 5.
IV. MODIFIED CONDITION DECISION COVERAGE OVERVIEW

A. MC/DC Definition

The Modified Condition/Decision Coverage criterion was developed to achieve many of the benefits of Multiple Condition/Decision testing while retaining a linear growth in required test cases [10]. The formal definition of MC/DC requires that: every point of entry and exit in the design description or software program has been invoked at least once, every condition, and decision has taken all possible values at least once, and each condition in a decision has been shown to independently affect the decision outcome. The independence requirement ensures that the effect of each condition is tested relative to the other conditions [2].

B. MC/DC Independence Pairs

A condition independently affects a decision outcome if that condition alone can determine the value of the decision outcome. Two test cases that show the independent effect of a condition within a decision are referred to as an independence pair [11]. For example, test vectors (FT, TT), and (FF, TF) each form an independence pair for a 2-input and gate, and a 2-input or gate respectively due to the independent effect of the changing condition on the output value.

C. Unique-Cause and Masking MC/DC Approaches

For Unique-Cause MC/DC, a condition is shown to independently affect a decision outcome by varying just that condition while holding all other possible conditions fixed. For Masking MC/DC, a condition is shown to independently affect a decision outcome by applying principles of boolean logic to assure that no other condition influences the outcome, though more than one condition in the decision may change value. The mathematical representation of the unique-cause MC/DC independence pair implies that the boolean difference function \( \delta F(c) / \delta c_i = F(c_1, \ldots, c_i, \ldots, c_n) \oplus F(c_1, \ldots, \neg c_i, \ldots, c_n) \) is always true such that \( F(c) \) is an expression with \( n \) inputs [12].

For Masking MC/DC approach the equation will remain valid taken into account that condition \( c_j \) from \( i = (1, \ldots, n) \) and \( j \neq i \) might change its values but their influence are masked by the logic under investigation. For example, a true input for a 2-input or gate will mask the other input, and similarly a false input will have a dominant effect on a 2-input and gate and mask the other input. However, this requires analysis of the decision statement logic structure [10]. NASA has a special approach for evaluation of the MC/DC coverage fulfillment for software code. It uses the requirements-based testing to check for MC/DC as per software certification requirements in [1], and elaborated in [2].

V. MC/DC COVERAGE TEST SETS GENERATION ALGORITHM: OBSRV

This section presents a novel MC/DC coverage test set generation algorithm, called OBSRV. The main goal of MC/DC coverage is to show the independent effect of each input condition on the value of the decision by controllability and observability aspects as shown in [4], and [13]. Figure 1 shows a complex gate structure comprised of and, or, xor, and

A. OBSRV Usage Model

OBSRV main objective is to generate MC/DC coverage test sets for a single decision statement of control flow logic within the design code structure. The control flow logic analysis based on controllability, and observability aspects is the foundation of OBSRV. This analysis combined with unique, and masking MC/DC concepts enable the determination of all possible test vectors that fulfill the observability requirements for the decision statement input conditions. This process guarantees that OBSRV will generate the maximal number of MC/DC coverage test sets, and the minimal number of tests per particular generated MC/DC coverage test sets. The maximal MC/DC generated test sets will enable an efficient MC/DC coverage closure by the functional regression suite, and determination of the MC/DC coverage gaps. The minimal number of tests per MC/DC test set provides an optimal MC/DC coverage closure. Hence, OBSRV usage model has a potential added value to the efficiency, and the optimization of the MC/DC coverage closure process.

B. D-Algorithm Overview

The D-algorithm is developed to generate tests for fault detection for digital circuits, and this subsection will briefly provide an overview with details found in [5], [6], and [7]. D represents a generic truth value, and the D-cube is a collapsed truth table version of a particular logic operator using D. The D-algorithm starts with representation of the expression by gate level schematic showing the primary input/output, and internal nodes. The next step will be to choose a primary output, determine a path to this output, and propagate the fault to this output. The propagation D-cubes (PDC) of the logic gates of this path. This path is called the D-chain, and the propagation D-cubes (PDC) will enable the propagation of the fault in terms of the logic gate types, and input conditions values. The singular cover is defined as the truth table structure for all the gates that construct the logic circuit. The final step
These consistent D-intersections do not lead to inconsistent line assignments [6].

The assignment through a particular gate to propagate the decision output node. The assignment through a particular gate to propagate the D value represents an imposed implication of other nodes assignment across the logic. For example, a D propagation through an and gate will require a true input, and a false input through an or gate. This phase is completed by the consistency operation which is the completion of the resultant D-cube by D-intersection with the singular cover [5].

Masking MC/DC enables possibilities during the consistency operation. For example, if an output of an and gate is false, there are three possibilities of the input D-coordinates as (FF, FT, TF). Bimodal decision is defined as an expression with D-chains that can observe D which is the negated value of D as well as the D absolute value. The bimodal decisions D-chains must contain at least one negating or inverting logic operator.

C. Conditions Observability Computation

The graph representation of the decision statement as netlist structure is the entry point to the algorithm. This OBSRVphase uses the D-algorithm to define the D-chain(s) of each primary input D value propagation. Each primary input D-chain consists of a listing of all those gates whose primitive D-cube intersections do not lead to inconsistent line assignments [6]. These consistent D-intersections will lead to defining the assignments of the nodes at each gate of the D-chain that will drive the selected primary input D value propagation to the decision output node. The assignment through a particular gate to propagate the D value represents an imposed implication of other nodes assignment across the logic. For example, a D propagation through an and gate will require a true input, and a false input through an or gate. This phase is completed by the consistency operation which is the completion of the resultant D-cube by D-intersection with the singular cover [5].

E. MC/DC Test Sets Combinations, and Prioritization

OBSRV will generate all possible MC/DC coverage test sets by combining one independence pair for each condition (primary input) in the logic expression. The combined independence pairs test vectors will formulate the required MC/DC coverage test set. The ranking of the coverage test sets will be accomplished using a greedy algorithm to rank the coverage set in an ascending order of their test vectors count [9], [14].

F. OBSRV Example

This section presents a manual example of MC/DC coverage test sets generation using the OBSRValgorithm. The example used is the same used in [5] as shown in Figure 3. The primary output function is G, and G = (((A and B) or C) xor A) nand (not ((A and B) or C) or E) The possible D-chains for each primary input will be determined by the D-cube intersections, and the patterns that will lead to observability at the output will be completed by the imposed implications, and the consistency operation as explained in Subsection V-C. The observability matrix is constructed as shown in Table I. The primary input C exhibits bimodal expression processing as the observed primary output could be non-negated as D, or negated as D.
coverage set as explained in V-E. For example, the coverage set (2,3,8,11,12) has 5 tests, which is one of the optimal MC/DC coverage test sets for this example. An elaborated empirical MC/DC study using the OBSRV algorithm, and an associated set of novel MC/DC insights have been deduced [15].

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>E</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>D</td>
</tr>
<tr>
<td>D</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>D</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>D</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>D</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>C</td>
<td>1</td>
<td>0</td>
<td>D</td>
<td>0</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>0</td>
<td>D</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>D</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>D</td>
<td>1</td>
<td>D</td>
</tr>
<tr>
<td>E</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>D</td>
</tr>
<tr>
<td>E</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>D</td>
</tr>
</tbody>
</table>

TABLE I: Observability Matrix

<table>
<thead>
<tr>
<th>Exp.</th>
<th>In</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6-10</th>
<th>11-15</th>
<th>16-20</th>
<th>21-35</th>
<th>36-76</th>
</tr>
</thead>
<tbody>
<tr>
<td>16491</td>
<td>2262</td>
<td>685</td>
<td>391</td>
<td>131</td>
<td>219</td>
<td>35</td>
<td>36</td>
<td>4</td>
<td>2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TABLE III: Avionics complexity: Expressions versus inputs

3) D-drive Options Scalability: The D-drive options scalability defines as the growth of the D-propagation paths per a particular condition of the decision statement. The alternative logic paths or D-drives or D-fronts or D-propagation paths are mainly due to the contribution of the same unique condition or primary input to the various operands or the gates at the different logic levels. This results in the optional different paths to propagate that specific unique input to the output node. This type of scalability does not result in an exponential complexity growth. This results in multiple iterations of the algorithm procedures to address all the Primitive D-cube intersections for each primary input path until they are all exhausted or completed. This scalability will add advantages as the number of generated observability objectives tests will increase. It will enable scalability of the generated MC/DC coverage test sets.

4) Experimental Scalability Investigation: This experiment has been conducted in order to study the scalability aspects of the OBSRV algorithm under its current implementation. The results indicate no considerable negative impact on the scalability of the OBSRV algorithm implementation under the practical spectrum of the number of conditions, and decisions in a specific design under test. The experiment has formulated an incremental growth of the complexity by adding complex concurrent decision statements from the unimodal type, and the bimodal type. The scalability magnitude of order was measured by the quantitative absolute number of logic operands under processing by the MC/DC algorithm implementation. The machine used has quad-core with 16 GB memory size under Linux. The unimodal expression has incrementally grown to a scalability order of magnitude to X1000 times the original design. The elapsed time from the transcript evaluates to zero seconds which is in magnitude of fraction of seconds. The memory, and the debugging information complexity has been growing to 500MB order. The experiment has been conducted using bimodal decision statements. The incremental complexity has been growing until reaching X4000 absolute value of complexity growth. The measured elapsed time is zero, which implies an actual execution run time in the order of fractions of seconds. The memory usage has no limited impact or consumption of the memory resources. The debugging information size from the transcript, and log files grow significantly from 14KB to 1300KB. The experimental investigation shows that the execution run times under a practical number of conditions are manageable. It will not reach the limits that will represent an obstacle to complete the computation of the algorithm. The main impact is represented by the growth of the size of the debugging information represented by the coverage reports, the transcripts, and the debugging log files.
A logical structure change which implies a change in the values of \( B \) indicated MC/DC coverage gaps for not fulfilling MC/DC in this fault. The experiment FEC results first, and second term. The MC/DC coverage test set does not fulfill MC/DC in this fault. The experiment FEC results indicated MC/DC coverage gaps for \( B_1 \) and \( E_1 \) by false input to the or gate, and this was negated by introduction of an inverter after the or at the second logic level. The MC/DC test set detects the introduced fault by presenting MC/DC coverage gaps in the FEC results.

C. Term Negation Fault: TNF

\[ I = \text{not} (A \text{ and } D) \text{ or } (\text{not } A \text{ and } C) \text{ or } (B \text{ and } E) \]

represents the expression with TNF fault applied to the first term. The experiment FEC results indicated MC/DC coverage gaps for \( B_1 \), \( E_0 \), \( E_1 \). MC/DC test set enables detection of the fault, and the logic analysis indicates a change of the logic structure of the expression that impacts the controllability, and observability requirements for input conditions.

D. Term Omission Fault: TOF

\[ I = (\text{not } A \text{ and } C) \text{ or } (B \text{ and } E) \]

represents the expression with TOF fault applied to the first term. The experiment FEC results indicated MC/DC coverage gaps for \( A_1 \). The logic analysis indicates that the omission of the first term resulted in a change of the logic structure such that the expression changed to be a unimodal expression. The original expression is a bimodal expression as it has an inverting and non-inverting path to the output node for the input condition \( A \). The omission of the term \( (A \text{ and } D) \) removed the non-inverting observability path of the input \( A \). MC/DC test set detects the TOF fault by showing the FEC coverage gaps in the results.

E. Literal Omission Fault: LOF

\[ I = D \text{ or } (\text{not } A \text{ and } C) \text{ or } (B \text{ and } E) \]

represents the expression with LOF fault applied to first literal \( A \) of the first term \( (A \text{ and } D) \) by omission of \( A \). The MC/DC test set shows coverage gap in FEC for \( A_1 \). The logical analysis shows an introduced logic structure change as the \( D \) input condition will bypass an and gate and directly pass to the or gate. This will change controllability, and observability requirements of \( A \) that was shown by the MC/DC FEC coverage gap.

F. Literal Insertion Fault: LIF

\[ I = (A \text{ and } D \text{ and } B) \text{ or } (\text{not } A \text{ and } C) \text{ or } (B \text{ and } E) \]

represents the expression with LIF applied to the first term by adding \( B \) to the first and gate. The MC/DC test set detects the introduced fault by showing FEC coverage gaps \( A_1 \), \( D_0 \), \( D_1 \). The logic analysis implies a logic structure change that impacts the controllability, and observability requirements for MC/DC.

G. Literal Negation Fault: LNF

\[ I = \text{not} (A \text{ and } D) \text{ or } (\text{not } A \text{ and } C) \text{ or } (B \text{ and } E) \]

represents the expression with LNF applied to the literal \( A \) of the first term. The MC/DC test set achieves FEC coverage for the expression. The logic analysis shows that there is no substantial change to the expression logic structure, as adding an inverter gate after the primary input \( A \) does not

**VI. MC/DC Design Fault Detection Strength**

This section investigates the MC/DC design fault detection strength in terms of the main design fault classes in microprocessors as stated in [17], and [18]. The experimental investigation conducted on a diverse logic expressions from industrial designs with unimodal, and bimodal expression types, using main logic operators, and variant number of input conditions. The conclusions are elaborated using the case study expression \( I = (A \text{ and } D) \text{ or } (\text{not } A \text{ and } C) \text{ or } (B \text{ and } E) \) of [17], and shown in Figure 4. The MC/DC coverage test sets have been generated using OBSRV procedures stated in Section V, and sample of the generated test sets are \((1,2,3,4,8,16,24),(1,2,4,8,16,19,25)\). The experiment procedure requires each design fault type to be applied to the expression, and the MC/DC coverage results and the functional output of the expression will be evaluated for all fault types as shown in the following Subsections VI-A, VI-B, VI-C, VI-D VI-E, VI-F, VI-G, VI-H, VI-I, VI-J. Questa 10.0 FEC is used for checking MC/DC coverage fulfillment.

**A. Expression Negation Fault: ENF**

\[ I = \text{not} [(A \text{ and } D) \text{ or } (\text{not } A \text{ and } C) \text{ or } (B \text{ and } E)] \]

represents the expression with ENF design fault applied. MC/DC full coverage has been achieved while exercising the expression using the MC/DC test set of the original expression. The logic analysis shows that the logic structure has an additional inverter gate introduced before the primary output node. The expression with full ENF is still controllable, and observable due to the transparent path to the output node. The only difference is the inversion of the output value. MC/DC targets controllability and observability of the input conditions by having an independent effect on the decision, and still this will be applicable. The fault is easily detected as the full ENF type enable transparent propagation of the fault to the output, which will be detected by comparison of the functional output truth value of the original expression which will be negated.

**B. Subexpression Negation Fault**

\[ I = \text{not} ((A \text{ and } D) \text{ or } (\text{not } A \text{ and } C)) \text{ or } (B \text{ and } E) \]

represents the expression with partial ENF applied to the first, and second term. The MC/DC coverage test set does not fulfill MC/DC in this fault. The experiment FEC results indicated MC/DC coverage gaps for \( B_1 \), and \( E_1 \): the true values of \( B \), and \( E \) respectively. The logic analysis indicates a logical structure change which implies a change in the controllability, and observability requirements of the decision statement. The observation of \( B_1 \), and \( E_1 \) will be masked by a true value on the other input to the output or gate in Figure 4. The MC/DC test set for the original expression must enable observability of \( B_1 \), and \( E_1 \) by false input to the or gate, and this was negated by introduction of an inverter after the or at the second logic level. The MC/DC test set detects the introduced fault by presenting MC/DC coverage gaps in the FEC results.
impact the controllability, and observability requirements for MC/DC. The functional coverage suite detects a change in the output truth values of the expression compared to the original expression which enables a detection of an introduced fault.

**H. Literal Reference Fault: LRF**

\[ I = (B \text{ and } D) \text{ or (not } A \text{ and } C \text{) or } (B \text{ and } E) \]

represents the expression with LRF applied to the literal A of the first term by replacing it by the input condition B. MC/DC test set detects the fault by showing FEC coverage gaps for \(A_1\), and \(D_1\). Logic analysis shows that a logic structure change is introduced by LRF due to a change of one primary input by another, which impacts the controllability, and observability requirements for the original expression MC/DC fulfillment.

**I. Disjunctive Operator Reference Fault: ORF(+)**

\[ I = (A \text{ and } D) \text{ or (not } A \text{ and } C \text{) or } (B \text{ and } E) \]

represents the expression with ORF(+) fault by changing the or gate to an and gate at the second logic level. MC/DC test set detects the fault by showing coverage gaps for primary inputs A, C, and D. The logic analysis shows a major change in the logic structure of the expression as it will be simplified to only an and gate between B, and E. MC/DC shows that A, C, and D are redundant inputs by showing these inputs as Not Testable in the FEC report. The logic structure change has an impact on the controllability, and observability requirements of MC/DC, which leads to the fault detection.

**J. Conjunctive Operator Reference Fault: ORF(.)**

\[ I = (A \text{ or } D) \text{ or (not } A \text{ and } C \text{) or } (B \text{ and } E) \]

represents the expression with ORF(.) fault by replacing the and gate by or gate for inputs A, and D at the first logic level. MC/DC test set detects the fault by showing coverage gaps for primary inputs B, and E. The MC/DC FEC coverage results shows gaps for \(B_1\), and \(E_1\). The logic analysis shows a change in the logic structure of the expression which has an impact on the controllability, and observability requirements for MC/DC, which leads to the fault detection.

**VII. Summary and Conclusion**

This paper promotes the adoption of MC/DC in hardware verification as a structural coverage metrics. The hardware verification requirement for an efficient structural coverage metrics, the success of MC/DC in critical software applications, the description of hardware using HDL and the MC/DC computation dependency on logic analysis have been potential motivational factors for this research. The paper has provided an overview about the MC/DC types as unique-cause and masking MC/DC with an explanation of the main concepts of MC/DC represented by the controllability and the observability aspects. The research work has produced OBSRV, which is a novel algorithm for MC/DC coverage test sets generation. The main steps in the procedural computation of OBSRV have been outlined with detailed example. The example presents a manual implementation of OBSRV on selected logic function to enable clear understanding of the algorithm technique. OBSRV is based on path-oriented test generation algorithms as D-algorithm I, II which established the fundamental work of 48 years of state-of-the-art in the application of hardware fault detection test generation. OBSRV represents a potential bridge to portability of this technology advancement to be applied to MC/DC coverage for software, and hardware. The paper has presented an investigation of the OBSRV algorithm scalability, and complexity analysis. The horizontal, and vertical design scalability, operand chain effect, D-drive options scalability, and an experimental scalability investigation have been introduced. The paper has investigated the MC/DC functional design faults detection strength, and the empirical results conducted on the main design fault classes in microprocessors demonstrated sufficient MC/DC detection capability of the various introduced design faults. The paper research results will enable continuity of research in terms of MC/DC adoption as main metric for functional verification coverage closure.

**REFERENCES**