Reliability Engineering and System Safety 146 (2016) 39–46

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Prime implicants in dynamic reliability analysis

Tero Tyrväinen

VTT Technical Research Centre of Finland, Lifetime Management, P.O. Box 1000, FI-02044 Espoo, Finland

ARTICLE INFO

Article history:
Received 30 May 2014
Received in revised form
3 July 2015
Accepted 5 October 2015
Available online 22 October 2015

Keywords:
Prime implicant
Dynamic reliability analysis
Dynamic flowgraph methodology

ABSTRACT

This paper develops an improved definition of a prime implicant for the needs of dynamic reliability analysis. Reliability analyses often aim to identify minimal cut sets or prime implicants, which are minimal conditions that cause an undesired top event, such as a system's failure. Dynamic reliability analysis methods take the time-dependent behaviour of a system into account. This means that the state of a component can change in the analysed time frame and prime implicants can include the failure of a component at different time points. There can also be dynamic constraints on a component's behaviour. For example, a component can be non-repairable in the given time frame. If a non-repairable component needs to be failed at a certain time point to cause the top event, we consider that the condition that it is failed at the latest possible time point is minimal, and the condition in which it fails earlier non-minimal. The traditional definition of a prime implicant does not account for this type of time-related minimality. In this paper, a new definition is introduced and illustrated using a dynamic flowgraph methodology model.

1. Introduction

1.1. Boolean algebra in reliability analysis

Reliability analyses are often used for identifying the possible root causes of an undesired top event, such as a system's failure [1]. These root causes can be combinations of basic events such as component failures, harmful environmental conditions and human errors. A minimal combination of basic events that is sufficient to cause the top event is called a minimal cut set [2]. Here, the minimality means that if one of the basic events is removed from a minimal cut set, the remaining combination of basic events is no longer sufficient to cause the top event. Minimal cut sets are usually the basic result of a reliability analysis. They are often used as the basis for probabilistic calculations, such as the computation of total probability [1,3] and risk importance measures [1,3,4], uncertainty analysis [3] and sensitivity analysis [3].

The theory of minimal cut sets and prime implicants is based on Boolean algebra. Boolean algebra defines algebraic operations for variables that can have two values: 0 ('false') and 1 ('true'). Boolean variables form Boolean formulas when they are connected using logical connectives, such as + ('OR') and $\cdot$ ('AND'). For example, $F_T = a \cdot b \cdot c + a \cdot d$ is a Boolean formula if a, b, c and d are Boolean variables. A Boolean product is a set of Boolean variables connected by $\cdot$. For instance, $a \cdot b \cdot c$ and $a \cdot d$ are products. The expression can be shortened: $F_T = abc + ad$. The axioms of Boolean algebra are presented in Appendix A.

Let G and H be Boolean formulas. Formula G implies H, if from $G=1$, it follows that $H=1$. Formula F_T has value 1 if and only if a, b and c have value 1, or if a and d have value 1. Hence, products abc and ad imply F_T.

In reliability analysis, a top event can be represented by a Boolean formula of variables that represent basic events and minimal cut sets can be represented by Boolean products that imply the Boolean formula representing the top event. In traditional reliability analysis, basic events are assumed to be independent. In this paper, basic events are assumed to be independent unless dependencies between them are presented. In what follows, the Boolean formula that represents the top event is called a top function. For example, if $F_T = abc + ad$ is a top function and a, b, c and d represent basic events, the top event has two minimal cut sets: abc and ad.

The definition of a minimal cut set is adequate only for coherent reliability models. A reliability model is coherent only if the top function is monotonically increasing with regard to its arguments and all basic events are relevant. In an incoherent reliability model [5], however, failure of a component may actually prevent the top event from occurring, and the act of repairing it could cause the top event. For incoherent reliability models, the concept of a *prime implicant* is used instead of a minimal cut set to represent a minimal combination of conditions that causes the top event [6–8].

E-mail address: tero.tyrvainen@vtt.fi

http://dx.doi.org/10.1016/j.ress.2015.10.007
0951-8320/

A literal is either a Boolean variable a or its negation $\overline{a}$, also called a negative literal. For opposite literals a and $\overline{a}$, it holds that $a \cdot \overline{a} = 0$ and $a + \overline{a} = 1$. It also holds that

$$\overline{a+b} = \overline{a} \cdot \overline{b} \quad (1)$$

and

$$\overline{a \cdot b} = \overline{a} + \overline{b}. \quad (2)$$

A so-called negative basic event is a complement of a regular basic event (e.g. component not failed). In incoherent reliability analysis, negative basic events represented by negative literals can appear in the top function and prime implicants. The definition of a prime implicant is presented in Definition 1 [6].

Definition 1. Let F_T be a top function and π be a product. The product π is an implicant of F_T if π implies F_T.

An implicant π is a prime implicant, if there is no other implicant ρ of F_T such that $\rho \subset \pi$.

To illustrate Definition 1, prime implicants of formula $G = ab + c\overline{d}$ are ab and $c\overline{d}$. For formula $F_T = \overline{a}bc + b\overline{c}d + c\overline{d}f + ce\overline{f}$, the identification of prime implicants is more challenging. It is easy to see that $\overline{a}bc$, $b\overline{c}d$, $c\overline{d}f$ and $ce\overline{f}$ are prime implicants, but $\overline{a}bd$ is also a prime implicant, because, if $c=1$ and $\overline{a}bd = 1$, then $\overline{a}bc = 1$, and if $c=0$ and $\overline{a}bd = 1$, then $b\overline{c}d = 1$. Also, $c\overline{d}e$ is a prime implicant, because if $f=1$ and $c\overline{d}e = 1$, then $c\overline{d}f = 1$, and if $f=0$ and $c\overline{d}e = 1$, then $ce\overline{f} = 1$.

1.2. Dynamic reliability analysis

In dynamic reliability analysis [9,10], there can be causal dependencies between events represented by literals [11]. For example, the failure of a non-repairable component at time point t_1 implies that the component continues to be failed at later time point t_2. If literal f_{t_i} indicates that the component is failed at time step t_i, then f_{t_1} implies f_{t_2}. Fig. 1 presents a fault tree whose prime implicants are af_{t_1}, bf_{t_1} and bf_{t_2} according to Definition 1. However, when analysing implicants bf_{t_1} and bf_{t_2}, it should be noticed that, if $b=1$, then the failure condition represented by f has to start only at time step t_2 to cause the top event. The failure can occur already at time step t_1, but it does not need to. Literal f_{t_1} represents a more restrictive condition than f_{t_2} and on the other hand, if bf_{t_2} implies the top event, then bf_{t_1} also implies the top event.

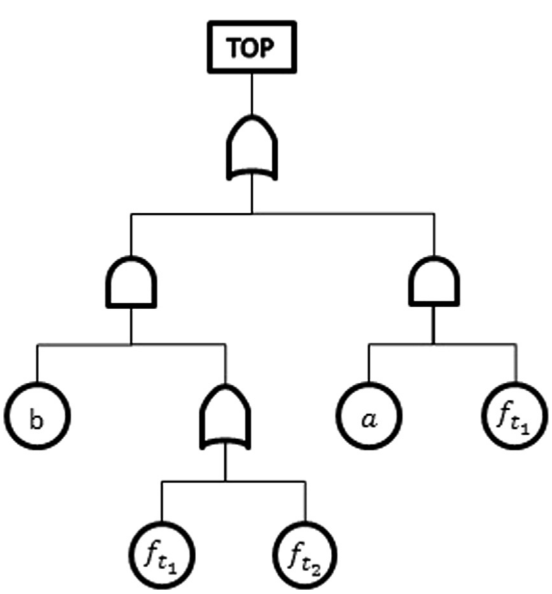

Fig. 1. A fault tree with dependent basic events.

Therefore, bf_{t_1} is not a minimal condition for the top event to occur and is not a prime implicant.

The conclusion of the previous example is that Definition 1 is not adequate when the reliability model contains dynamic dependencies between its variables. A new definition for prime implicants is introduced in Section 2. Section 3 shows how the definition is applicable to multi-state reliability analysis. A dynamic reliability analysis method called dynamic flowgraph methodology (DFM) [10,12–14] is used as an example of a methodology where the new definition is useful. DFM is presented in Section 4. Prime implicants of an example DFM model are identified in Section 5. It is shown that the new definition is logical, supports the computation of the top event probability better and allows the root causes of the top event to be represented by a smaller number of prime implicants. As the prime implicants are the basic result of DFM analysis, their definition and interpretation also affects other areas of the analysis, such as probabilistic reliability models, the computation of risk importance measures [15] and the modelling of common cause failures [16].

2. Definition of a prime implicant

The basis for the development of the new definition is a reliability model that can be represented as a top function and additional constraints. These additional constraints can, in principle, be any Boolean equations between the literals of the model.

The main motivation for the new definition is that it is needed in dynamic flowgraph methodology. A DFM model includes a graph model and constraints for the behaviour of the graph's nodes. This model is converted to a Boolean top function to solve prime implicants. The prime implicants that are solved from the top function need to correspond to the graph model. Definition 1 can easily be applied to literals of DFM, but it does not account such minimality as described in the example of Fig. 1. Minimality that is related to a physical constraint, such as non-repairability, has to be taken into account, and therefore, it is practical to include additional constraints to the reliability model along with the top function.

A more simple approach to account constraints would be to build them directly into the top function so that "the reliability model" would contain only the top function. In that case, the traditional definition could be used as it is, and minimality related to non-repairability of a component could be taken into account, in theory at least. However, prime implicants are a property of a DFM model and they can be identified directly from the graph in simple cases. It has to be possible to apply the prime implicant definition in DFM. Even if correct prime implicants were solved by taking non-repairability constraints into account in the conversion of the DFM model to top function, Definition 1 would not be adequate when identifying prime implicants directly from the DFM model.

Before introducing the new definition, the concept of a minterm needs to be defined. If V is the set of all the Boolean variables in the model, then a minterm is a product consisting of each variable in V or its negation. For example, $ab\overline{c}d$ and $a\overline{b}\,\overline{c}d$ are minterms of example $G = ab + c\overline{d}$ among 14 others.

A new definition of an implicant is presented in Definition 2. Compared to the traditional definition (in Definition 1), the new definition adds a condition that additional constraints cannot be violated (e.g. an implicant cannot include a non-repairable component first failed and then repaired).

Definition 2. Let F_T be the top function representing the top event, π be a product, $\mathbf{A}$ be a vector of Boolean formulas and $\mathbf{A} = \mathbf{1}$ be a set of additional constraints. The product π is an implicant of the