Available online at www.sciencedirect.com
SCIENCE DIRECT®

Reliability Engineering and System Safety xx (2004) xxx–xxx

RELIABILITY ENGINEERING & SYSTEM SAFETY

www.elsevier.com/locate/ress

Approximate estimation of system reliability via fault trees

Y. Dutuit[a,*], A. Rauzy[b]

[a]*LAP-ADS, IUT, Université Bordeaux 1, 33405 Talence Cedex France*
[b]*IML/CNRS, 169, avenue de Luminy, 13288 Marseille Cedex 9, France*

Received 27 June 2003; accepted 21 February 2004

Abstract

In this article, we show how fault tree analysis, carried out by means of binary decision diagrams (BDD), is able to approximate reliability of systems made of independent repairable components with a good accuracy and a good efficiency. We consider four algorithms: the Murchland lower bound, the Barlow-Proschan lower bound, the Vesely full approximation and the Vesely asymptotic approximation. For each of these algorithms, we consider an implementation based on the classical minimal cut sets/rare events approach and another one relying on the BDD technology. We present numerical results obtained with both approaches on various examples.

Keywords: System reliability; Fault tree; Binary decision diagrams

1. Introduction

In the RAMS (reliability, availability, maintainability and safety) domain, fault tree (FT) technique is a well known engineering approach [9,16,18]. It is one of the most widely used by practitioners. However, because their limited expressive power, FTs cannot be used to assess the exact value of system reliability. Consequently, only approximate computations are used to get this latter quantity [10]. This article discusses these methods, their implementations, their accuracies and their efficiencies.

FTs make it possible to assess availability at time t for any system made of independent components, i.e. the probability that the system is working at time t. If the system is made only of non-repairable components, system availability is same thing as system reliability, i.e. the probability that the system works continuously from time 0 to time t. Otherwise, these two parameters differ, in general by orders of magnitude. There are some cases where the assessment of system reliability can be reduced to the assessment of system availability, even if components are repairable. This is for instance the case when systems under study are periodically tested [2]. If components are repairable and their repair times are randomly distributed these techniques do not apply and no algorithm exists to assess the exact value of system reliability.

Several approximate computations of system reliability have been proposed in the literature. These methods involve basically two ideas: First, to determine system reliability it suffices to know system failure rate, i.e. the probability that the system fails between t and $t + \mathrm{d}t$, given that it worked continuously from 0 to t. Second, a good approximation of system failure rate can be obtained by assessing system conditional failure intensity, i.e. the probability that the system fails between t and $t + \mathrm{d}t$, given it was working at t. System conditional failure intensity can be in turn assessed by adapting algorithms to compute system availability. In this article, we study four different algorithms based on these two ideas. Namely, we consider the Murchland lower bound, the Barlow–Proschan lower bound, the Vesely full approximation and the Vesely asymptotic approximation [5,6]. For each of these algorithms, we consider two implementations. The first one is based on the classical minimal cut sets/rare events approach. The second one relies on the binary decision diagrams (BDD) technology.

In order to test these algorithms, we compared their results with a Markovian analysis on various examples. These experiments showed that approximations are accurate and that algorithms are efficient in terms of computation times.

[*] Corresponding author. Tel.: +33-5-56-84-58-34; fax: +33-5-56-84-58-29.

E-mail addresses: dutuit@hse.iuta.u-bordeaux.fr (Y. Dutuit), arauzy@iml.univ-mrs.fr (A. Rauzy).

0951-8320/$ - see front matter © 2004 Published by Elsevier Ltd.
doi:10.1016/j.ress.2004.02.008

The contribution of this article is as follows. First, we review mathematical methods to assess system reliability from a FT. Second, we propose efficient implementations of these methods. Third, we show, by means of various examples, that these algorithms give accurate results and are efficient in terms of computation time. We show also their limitations.

The remainder of the article is organized as follows. Section 2 gives some definitions and assumptions. Section 3 presents the four methods under study. Section 4 discusses their implementation. Finally, Section 5 reports results of an experimental study.

2. Definitions and assumptions

2.1. Assumptions

Throughout this article, we make the following assumptions.

- Systems under study are made of repairable and non-repairable components.
- Each component c has two modes (working and failed), a failure rate λ_c and repair rate μ_c. If the component is non repairable, μ_c is null. λ_c and μ_c are constant through the time.
- Components are independent, i.e. both their failures and their repairs are statistically independent.
- Components are as good as new after a repair. They are as good as new at time 0.
- Failures of systems under study are modelled by means of coherent FTs. In the sequel, we assimilate systems with their FTs.

As a consequence, systems under study can be represented also as Markov models.

2.2. System reliability

Let S denote the system under study. Let T denote the date of the first failure of S. T is a random variable. It is called the lifetime of S. We assume that components of S were as good as new at time 0 and that they are as good as new after a repair.

Reliability $R_S(t)$ and unreliability $F_S(t)$: the reliability of S at t is the probability that S experiences no failure during time interval $[0,t]$, given that all its components were working at 0. Formally,

$$R_S(t) \overset{\text{def}}{=} \Pr\{t < T\} \tag{1}$$

The unreliability, or cumulative distribution function $F_S(t)$, is just the opposite.

$$F_S(t) \overset{\text{def}}{=} \Pr\{t \geq T\} = 1 - R_S(t) \tag{2}$$

The curve $R_S(t)$ is a survival distribution. This distribution is monotonically decreasing. Moreover, the following asymptotic properties hold.

$$\lim_{t\to 0} R_S(t) = 1 \tag{3}$$

$$\lim_{t\to\infty} R_S(t) = 0 \tag{4}$$

Failure density $f_S(t)$: The failure density refers to the probability density function of the law of T. It is the derivative of $F_S(f)$:

$$f_S(t) \overset{\text{def}}{=} \frac{\mathrm{d}F_S(t)}{\mathrm{d}t} \tag{5}$$

For sufficiently small dt's, $f_S(t)\mathrm{d}t$ expresses the probability that the system fails between t and $t+\mathrm{d}t$, given its was working at time 0.

Failure rate $r_S(t)$: the failure rate or hazard rate is the probability the system fails for the first time per unit of time at age t. Formally,

$$r_S(t) \overset{\text{def}}{=} \lim_{\mathrm{d}t\to 0} \frac{\Pr\{\text{the system fails between } t+\mathrm{d}t/C\}}{\mathrm{d}t} \tag{6}$$

where C denotes the event 'the system experienced no failure during the time interval $[0,t]$'. As before, for sufficiently small dt's, one can deduce from definition (6), the following expression.

$$r_S(t)\mathrm{d}t = \frac{\Pr[(t < T \leq t+\mathrm{d}t) \cap (t < T)]}{\Pr(t < T)}$$

$$= \frac{\Pr(t < T \leq t+\mathrm{d}t)}{\Pr(t < T)} = \frac{f_S(t)}{R_S(t)} = \frac{\left(\dfrac{\mathrm{d}R_S(t)}{\mathrm{d}t}\right)}{R_S(t)} \tag{7}$$

By integrating each member of equality (7), one obtains immediately the following property.

$$R_S(t) = \exp\left[-\int_0^t r_S(u)\mathrm{d}u\right] \tag{8}$$

2.3. System availability

Availability $A_S(t)$ and unavailability $Q_S(t)$: the availability of S at t is the probability that S is working at t, given that all its components were working at 0.

$$A_S(t) \overset{\text{def}}{=} \Pr\{S \text{ is working at } t\} \tag{9}$$

The unavailability is just the opposite.

$$Q_S(t) \overset{\textit{def}}{=} 1 - A_S(t) \tag{10}$$

The following properties hold.

$$A_S(t) \geq R_S(t), \quad \text{for general systems.} \tag{11}$$

$$A_S(t) = R_S(t), \quad \text{for systems with only non-repairable components.} \tag{12}$$

Conditional failure intensity $\lambda_S(t)$: the conditional failure intensity refers to the probability that the system fails per unit time at time t, given that it was working at time 0 and is working at time t. Formally,

$$\lambda_S(t) \overset{\text{def}}{=} \lim_{dt \to 0} \frac{\Pr\{\text{the system fails between } t \text{ and } t+dt/D\}}{dt} \tag{13}$$

where D denotes the event 'the system S was working at time 0 and is working at time t.' The conditional failure intensity is sometimes called Vesely rate. $\lambda_S(t)$ is an indicator of how the system is likely to fail.

Unconditional failure intensity $w_S(t)$: the unconditional failure intensity refers to the probability that the system fails per unit of time at time t, given it was working at time 0. Formally,

$$w_S(t) \overset{\text{def}}{=} \lim_{dt \to 0} \frac{\Pr\{\text{the system fails between } t \text{ and } t+dt/E\}}{dt} \tag{14}$$

where E denotes the event 'the system was working at time 0.' This parameter is called 'failure frequency' by some authors [1,17].

In the case of systems with non-repairable components, the following property holds.

$$w_S(t) = f_S(t), \quad \text{for systems with only non-repairable components.} \tag{15}$$

Equalities (13) and (14) induce, respectively, properties (16) and (17).

$$\begin{aligned}\lambda_S(t)dt &= \Pr\{\text{the system fails between } t \text{ and } t + dt/D\} \\ &= \Pr\{A/D\} = \Pr\{A/E \cap F\} = \Pr\{(A/E)/F\}\end{aligned} \tag{16}$$

where F denotes the event 'the system is working at time t.'

$$\begin{aligned}w_S(t)dt &= \Pr\{\text{the system fails between } t \text{ and } t + dt/E\} \\ &= \Pr\{A/E\}\end{aligned} \tag{17}$$

Let B be the conditional event (A/E). B can be expressed as follows.

$$B = (B \cap F) \cup (B \cap \bar{F}) \tag{18}$$

Now, if we consider that at most one failure can occur during the small time interval dt, the event $(B \cap \bar{F})$ is not realizable (it corresponds to a repair followed with a failure). From equality (18), we can conclude that the compound event $(B \cap F)$ reduces to event B. Property (16) can be rewritten as follows.

$$\begin{aligned}\lambda_S(t)dt = \Pr\{B/F\} &= \frac{\Pr\{B \cap F\}}{\Pr\{F\}} = \frac{\Pr\{B\}}{\Pr\{F\}} = \frac{\Pr\{A/E\}}{\Pr\{F\}} \\ &= \frac{w_S(t)dt}{A_S(t)}\end{aligned}$$

Therefore, the following property holds.

$$\lambda_S(t) = \frac{w_S(t)}{A_S(t)} \tag{19}$$

Marginal importance factor of the component c ($\mathrm{MIF}_{S,c}(t)$) : The marginal importance factor is often called Birnbaum importance factor [4]. It can be interpreted, when S is a monotone function, as the conditional probability that, given that c occurred, the system S is failed and c is critical, i.e. a repair of c makes the system working. Formally,

$$\mathrm{MIF}_{S,c}(t) \overset{\text{def}}{=} \frac{\partial Q_S(t)}{\partial Q_c(t)} \tag{20}$$

Shannon decomposition: The Marginal importance factor can be reinterpreted by means of the Shannon decomposition. Let ϕ be any Boolean function and let v be a variable. Then, the following equality holds.

$$\phi = v\phi[1/v] + \bar{v}\phi[0/v] \tag{21}$$

where $\phi[i/v]$ denotes the function ϕ evaluated at $v = i$. In terms of probabilities, equality (18) can be rewritten as follows.

$$\begin{aligned}\Pr(\phi) &= \Pr(v)\Pr(\phi[1/v]) + (1 - \Pr(v))\Pr(\phi[0/v]) \\ &= \Pr(v)(\Pr(\phi[1/v]) - \Pr(\phi[0/v])) + \Pr(\phi[0/v])\end{aligned} \tag{22}$$

The following equality holds from definition (20) and equality (22).

$$\mathrm{MIF}_{S,c}(t) = \Pr(S[1/c]) - \Pr(S[0/c]) \tag{23}$$

The set of states in which the system S is failed can be decomposed in three subsets: the set S_1 of states in which the repair of the component c repairs the system. The set S_0 of states in which the failure of c repairs the system. Finally, the set S_2 of states in which the system is failed, whatever is the state of the component c. Since the system is coherent, $S_0 = \varnothing$. It follows that $S[1/c]$ describes $S_1 \cup S_2$ and $S[0/c]$ describes S_2. Let $\mathrm{CRIT}_{S,c}(t)$ denote the probability that is system S is in a critical state w.r.t. the component c at time t, i.e. a state in which S is not failed and a failure of c induces a failure of S. From the above developments, the following equality holds.

$$\mathrm{CRIT}_{S,c}(t) = A_c(t)\mathrm{MIF}_{S,c}(t) \tag{24}$$

For sufficiently small value of dt, the probability that the system fails between t and dt, is as follows.

$$\Pr\{\text{the system fails between } t \text{ and } t + dt\} \approx \sum_{c \in S} dt \lambda_{c0} \mathrm{CRIT}_{S,c}(t) \tag{25}$$

Therefore, assuming that the system was perfect at time 0, the following equality holds.

$$w_S(t) = \sum_{c \in S} \mathrm{MIF}_{S,c}(t) w_c(t) \tag{26}$$

where $w_c(t) = \lambda_c A_c(t)$.

3. Approximate computations

If the system S under study is made only of non-repairable components, $R_S(t) = Q_S(t)$ and $r_S(t) = \lambda_S(t)$. In the general case, this equality does not hold.

3.1. Murchland lower bound

Let $N_S(t)$ be the number of failures the system experimented between time 0 and t. Let $E[X]$ denote the mathematical expectation of a random variable X. Then, according to Markov inequality, the following property holds.

$$F_S(t) = \Pr(N_S(t) \geq 1) \geq E[N_S(t)] \tag{27}$$

According to Eqs. (25) and (26), $w_S(t)$ be interpreted as the derivative of $E[N_S(t)]$. Hence, the Murchland lower bound of the reliability.

$$F_S^{[M]} \geq \int_0^t w_S(t)\mathrm{d}t \tag{28}$$

Indeed, $F_S^{[M]}(t)$ is close to $F_S(t)$ only for small values of t.

3.2. Barlow–Proschan lower bound

In Ref. [3], Barlow and Proschan remark that the mean time to failure (MTTF) is always greater than the mean up time (MUT). They show also the following equality.

$$\mathrm{MUT} = \frac{A_S(\infty)}{w_s(\infty)} = \frac{1}{\lambda_S(\infty)} \tag{29}$$

From equality (29), they derive the following upper bound of the unreliability.

$$F_S^{[\mathrm{BP}]} \geq t\lambda_S(\infty) \tag{30}$$

3.3. Vesely approximations

The underlying idea of both Vesely approximations of the reliability is to substitute $\lambda_S(t)$ for $r_S(t)$ in Eq. (8). The full Vesely approximation $F_S^{[V]}(t)$ is defined as follows.

$$F_S^{[V]}(t) = 1 - \exp\left[-\int_0^t \lambda_S(u)\mathrm{d}u\right] \tag{31}$$

The asymptotic Vesely approximation $F_S^{[V,\infty]}(t)$ is defined as follows.

$$F_S^{[V,\infty]}(t) = 1 - \mathrm{e}^{-\lambda_S(\infty)t} \tag{32}$$

This latter approximation works for large values of t only.

4. Implementation

This section presents algorithms to assess reliability according to the previous mathematical developments. We consider two kinds of implementations:

- The classical approach based on minimal cut sets and rare event approximation.
- The BDD approach.

We would not discuss here methods to get minimal cut sets. We assume minimal cut sets are given.

4.1. Preliminaries

The unavailability at time t of a repairable component is determined according to the well-known following equation [11].

$$Q_c(t) = \frac{\lambda_c}{\lambda_c + \mu_c} \times (1 - \mathrm{e}^{-(\lambda_c+\mu_c)t}) \tag{33}$$

In order to implement approximate computations, we need basically two algorithms.

- An algorithm to assess $Q_S(t)$, or equivalently $A_S(t)$.
- An algorithm to assess $\mathrm{MIF}_{S,c}(t)$ or $w_S(t)$.

Integrals are computed numerically (in our implementation, using a triangular approximation).

4.2. Classical approach

The rare event approximation is as follows.

$$Q_S(t) \approx \sum_{\pi \in \mathrm{MCS}[S]} Q_\pi(t) \tag{34}$$

where MCS[S] denotes the set of minimal cut sets of S and $Q_\pi(t)$ is the product over the basic events c that occurs in π of the $Q_c(t)'s$.

$Q_{S[0/c]}(t)$ and $Q_{S[1/c]}(t)$ can be determined in the same way. Since S is assumed to be coherent, MCS[S] can be splitted into two disjoint subsets: the set of the cut sets that contain c and the set of the cut sets that do not contain c. Let $\mathrm{MCS}_{1/c}[S]$ and $\mathrm{MCS}_{0/c}[S]$ denote, respectively, the sets $\{\pi \in \mathrm{MCS}[S]; c \in \pi\}$ and $\{\pi \in \mathrm{MCS}[S]; c \notin \pi\}$. The following properties hold.

$$Q_{S[1/c]}(t) \approx \sum_{\pi \in \mathrm{MCS}_{1/c}[S]} \frac{Q_\pi(t)}{Q_c(t)} + \sum_{\pi \in \mathrm{MCS}_{0/c}[S]} Q_\pi(t) \tag{35}$$

$$Q_{S[0/c]}(t) \approx \sum_{\pi \in \mathrm{MCS}_{0/c}[S]} Q_\pi(t) \tag{36}$$

From approximation of Eqs. (35) and (36), the following property holds.

$$\mathrm{MIF}_{S,c}(t) \approx \sum_{\pi \in \mathrm{MCS}_{1/c}[S]} \frac{Q_\pi(t)}{Q_c(t)} \tag{37}$$

Approximation Eq. (37) gives a two steps algorithm to compute $w_S(t)$. First, the probability of each cut set is computed (in one pass through MCS[S]). Second, the $w_S(t)$

is assessed using property (37) (again in one pass through MCS[S]). Therefore, the whole algorithm is in $O(|\mathrm{MCS}[S]|)$, where $|\mathrm{MCS}[S]|$ denotes the size of the encoding of MCS[S].

4.3. Binary decision diagrams: principles

BDD are the state-of-the-art date structure to encode and manipulate Boolean functions. They are nowadays used in a wide range of areas. Since their introduction in the RAMS field, they have proved to be the most efficient tool to assess FTs [7,12–15].

The BDD representation is based on the Shannon decomposition: Let ϕ be a Boolean function that depends on the variable v. By choosing a total order over the variables and applying recursively the Shannon decomposition, the truth table of any formula can be graphically represented as a binary tree. The nodes are labelled with variables and have two outedges: a *then*-outedge, pointing to the node that encodes $\phi[1/v]$, and an *else*-outedge, pointing to the node that encodes $\phi[0/v]$. The leaves are labelled with either 0 or 1. The value of the formula for a given variable assignment is obtained by descending along the corresponding branch of the tree.

Indeed such a representation is very space consuming. It is however possible to shrink it by means of the following two reduction rules.

- Isomorphic subtrees merging. Since two isomorphic subtrees encode the same formula, at least one is useless.
- Useless nodes deletion. A node with two equal sons is useless since it is equivalent to its son ($\phi = v\phi + \bar{v}\phi$).

By applying these two rules as far as possible, one get the BDD associated with the formula. A BDD is therefore a directed acyclic graph. It is unique, up to an isomorphism. This process is illustrated in Fig. 1.

Logical operations (and, or, x or, …) can be directly performed on BDDs. This results from the orthogonality of usual connectives and the Shannon decomposition:

$$(v\phi_1 + \bar{v}\phi_0)\oplus(v\varphi_1 + \bar{v}\varphi_0) = v(\phi_1\oplus\varphi_1) + \bar{v}(\phi_0\oplus\varphi_0) \quad (38)$$

where $\oplus$ is any binary connective.

Among other consequences, this means that the complete binary tree is never built and then shrunk: the BDD encoding a formula is obtained by composing the BDDs encoding its subformulae. Moreover, a caching principle is used to store intermediate results of computations. This makes the usual logical operations (conjunction, disjunction) polynomial in the sizes of their operands.

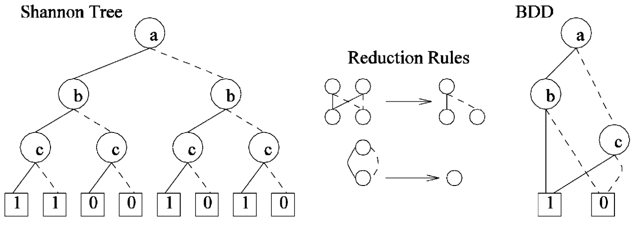

Fig. 1. From the Shannon Tree to the BDD.

```
AssessPr(F: BDD)
   if (F==0) return 0
   if (F==1) return 1
   if (the cache has an entry for F) return cache(F)
   /* F = x.F1 + (not x).F0 */
   Pr1 = AssessPr(F1)
   Pr0 = AssessPr(F0)
   Pr  = Pr(x).Pr1 + (1-Pr(x)).Pr0
   add <F,Pr> to the cache
   return Pr
```

Fig. 2. Algorithm to assess a probability from a BDD.

4.4. Binary decision diagrams: quantification

In order to assess $Q_S(t)$ given a BDD that encodes S, it suffices to apply the Shannon decomposition (22) at each node. This idea, together with the caching mechanism, gives a linear time algorithm [12]. This algorithm is sketched Fig. 2.

The algorithm of Fig. 2 is in $O(|\phi|)$. $\mathrm{MIF}_{\mathrm{S,c}}(t)$ can be assessed in the same way, according to the following decomposition [8].

$$MIF_{1,\mathrm{c}}(t)0$$

$$MIF_{0,c}(t)0$$

$$MIF_{cS_1\bar{c}S_0,c}(t)Q_{S_1}(t)Q_{S_0}(t) \quad (39)$$

$$MIF_{dS_1\bar{d}S_0,c}(t)Q_d(t)MIF_{S_1}(t)(1Q_d(t))MIF_{S_0}(t))$$

Decomposition (39) together with the caching mechanism make it possible to design an $O(|BDD(\mathsf{S})|)$ algorithm. This algorithm works in two traversals of the BDD: a first traversal to compute unavailability at each node and a second pass to compute MIF at each node.

The above algorithm could be used for approximate computations. However, the same idea can be applied to get $w_{\mathrm{S}}(t)w_{\mathrm{S}}(t)$ is obtained by two traversals of the BDD which avoids to perform a computation of $MIF_{\mathrm{S,c}}(t)$ for each basic event c. The corresponding decomposition is as follows.

$$w_1(t) = 0$$

$$w_0(t) = 0$$

$$w_{\mathrm{cS}_1+\bar{\mathrm{c}}\mathrm{S}_0}(t) = w_{\mathrm{c}}(t)\Big[Q_{\mathrm{S}_1}(t) - Q_{\mathrm{S}_0}(t)\Big] + Q_{\mathrm{c}}(t)\times w_{\mathrm{S}_1}(t)$$
$$+ [1 - Q_{\mathrm{c}}(t)]w_{\mathrm{S}_0}(t)) \quad (40)$$

The algorithm derived from decomposition (40) is in $O(|\mathrm{BDD}|)$ which is to be compared to the $O(n|\mathrm{MCS}[S]|)$ of the corresponding classical algorithm. This linear time complexity is of great interest to assess Murchland lower bound and Vesely full approximation: these two methods require to perform a numerical integration which in turn requires a lot of points to be accurate.

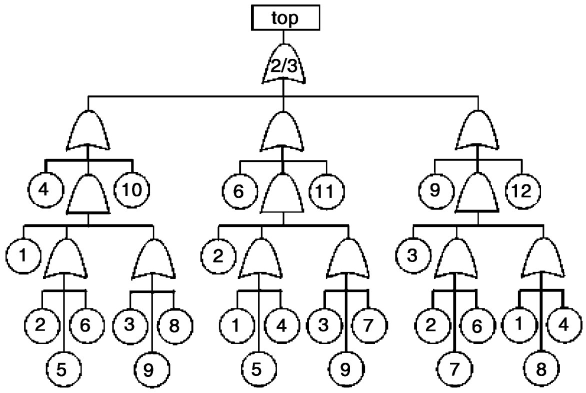

Fig. 3. A fault tree.

5. Experimental results

5.1. Accuracy

As an illustrative example, we consider the FT is pictured Fig. 3. Its reliability parameters are given in Table 1. This test case is very representative of what can be observed on real-life models. We performed dozens of experiments on different models that gave similar results. The FT of Fig. 3 admits 12 MCS of order 2, 10 of order 3 and 21 of order 4. The asymptotic conditional failure intensity $\lambda_S(\infty)$ for this test case is 2.32×10^{-4}. Its MUT is 4312 h.

Fig. 4 shows $F_{top}(t)$ assessed by means of a Markov analysis. The curve consists of 200 points ($F_{top}(t)$ has been computed at $t = 100, 200, 300, \ldots, 20{,}000$ h).

Fig. 5 shows the relative error $\rho_S^{[Murchland]}(t)$ of the Murchland lower bound computed at the same points as the curve drawn Fig. 4. The relative error is defined as follows.

Table 1
Reliability parameters for the FT pictureFig. 3

Basic events	1, 2, 3 (h^{-1})	4, 6, 9 (h^{-1})	5, 6, 8 (h^{-1})	10, 11, 12 (h^{-1})
λ	1.0×10^{-4}	2.0×10^{-4}	1.0×10^{-3}	2.0×10^{-3}
μ	0.05	0.08	0.1	0.125

$$\rho_S^{[Murchland]}(t) \overset{\text{def}}{=} \frac{F_S^{[Markov]}(t) - F_S^{[Murchland]}(t)}{F_S^{[Markov]}(t)} \tag{41}$$

Figs. 6–8 do the same for the Barlow–Proschan lower bound, the asymptotic Vesely approximation and the full Vesely approximation. The curve named BDD gives the results of BDD algorithm while the curve named SoP gives the results of the Sum-Of-Products algorithm, i.e. the classical minimal cut sets/rare event approach.

Several remarks can be made about these curves.

- The four methods give quite accurate results. The Full Vesely Approximation gives especially good results, with a relative error that never exceeds 6%.
- The curve of the classical Sum-Of-Products algorithm is always above the curve of the BDD algorithm. This is due to the rare-event approximation, which is optimistic. The distance between the two curves decreases as the probabilities of basic events (i.e. their λ's) decrease.
- The relative error of Murchland and Barlow–Proschan lower bounds increases up to $t = 4000$ h and then decreases (this threshold indeed varies according with the model).
- The methods show a different behavior close to the origin. A zoom on the curves is shown for each method Figs. 9–12. This different behavior can be explained by the fact that numerical values are very small close to the origin. Therefore, they can impacted strongly by rounding errors (this is especially true for the Markov assessment).
- The Barlow–Proschan lower bound is never better than the asymptotic Vesely approximation. Since both methods are of the same complexity, the latter should be used rather than the former.
- The full Vesely approximation gives in most of the cases more accurate results than the Murchland lower bound. This is indeed true when t is large. This is also true for small values of t. Since the two methods are of the same complexity (both require a numerical integration), the former should be used preferably to the latter.

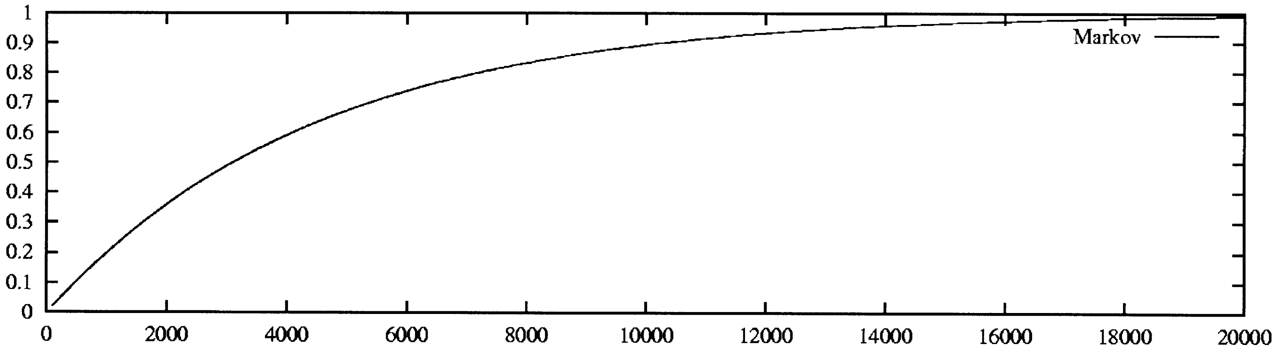

Fig. 4. $F_{top}(t)$ assessed by means of a Markov analysis.

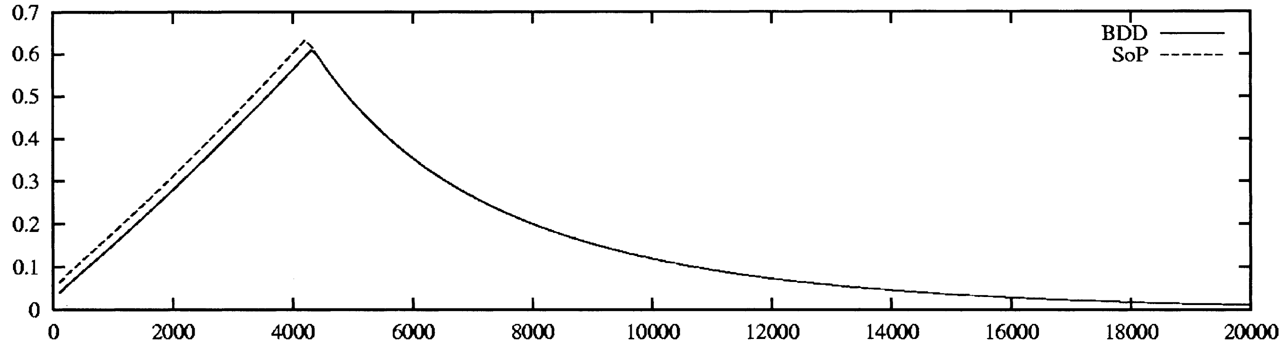

Fig. 5. Relative error of the Murchland lower bound.

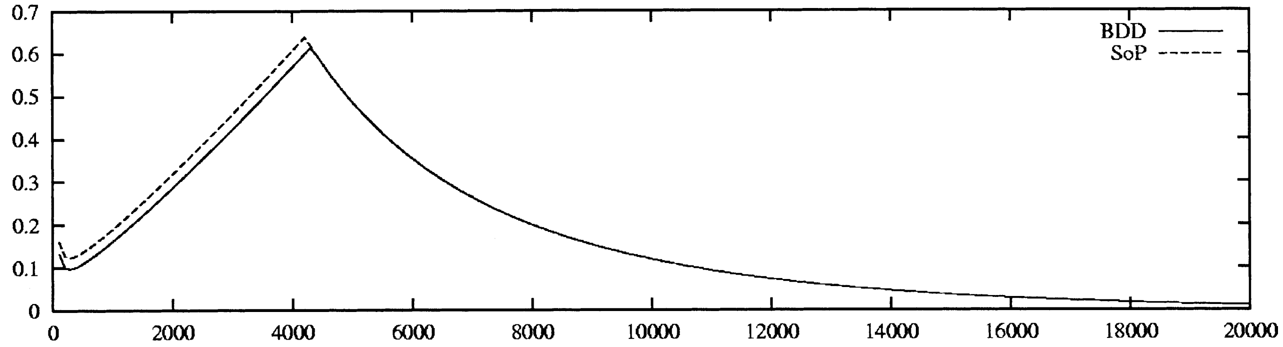

Fig. 6. Relative error of the Barlow–Proschan lower bound.

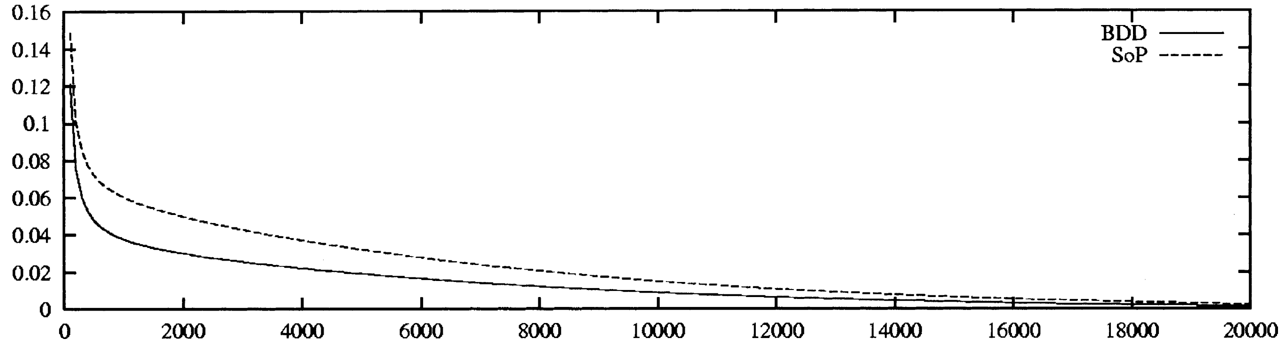

Fig. 7. Relative error of the asymptotic Vesely approximation.

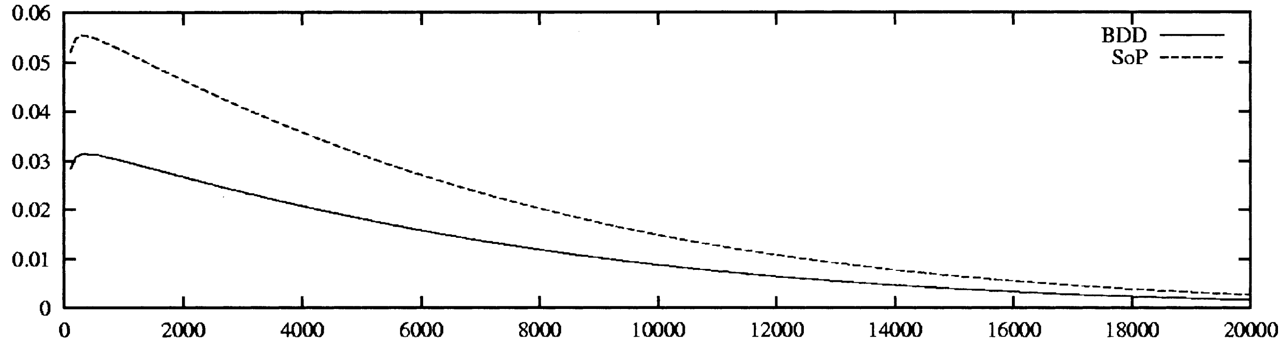

Fig. 8. Relative error of the full Vesely approximation.

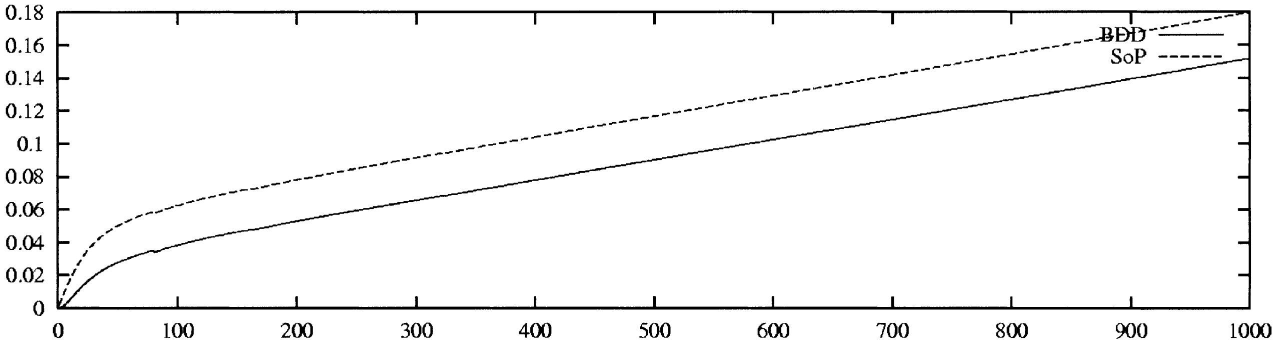

Fig. 9. Relative error of the Murchland lower bound (zoom).

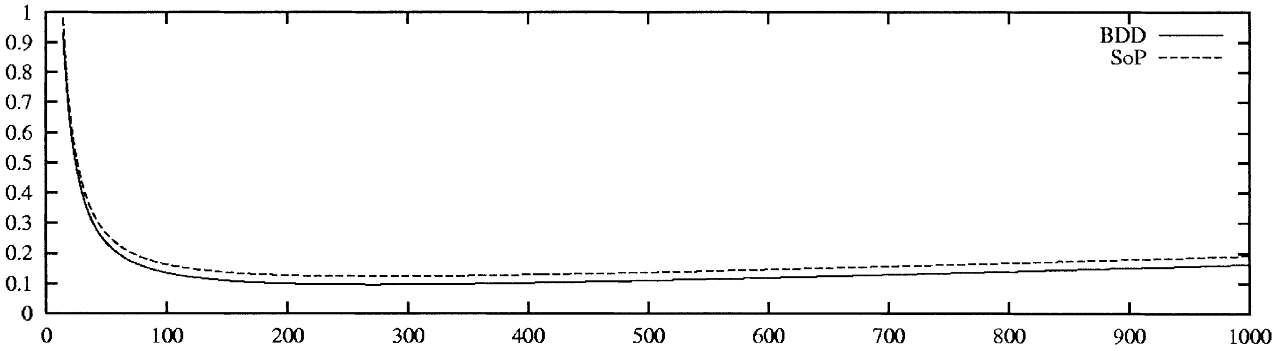

Fig. 10. Relative error of the Barlow–Proschan lower bound (zoom).

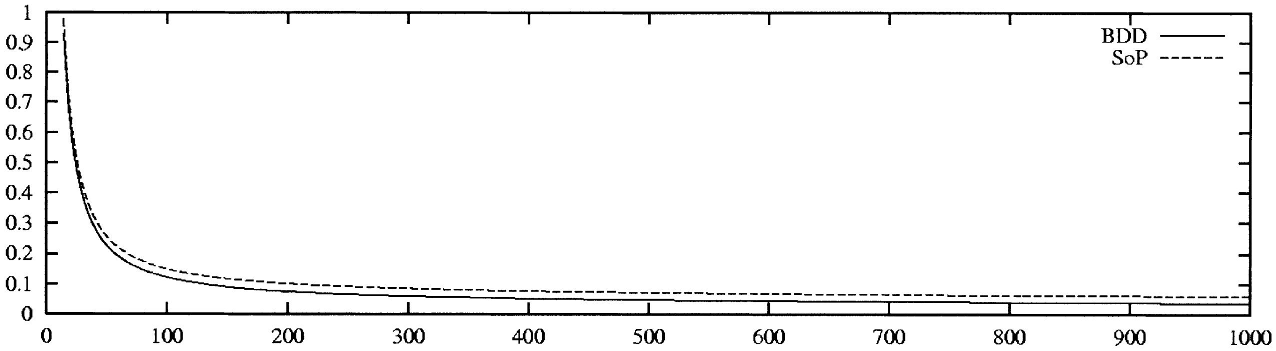

Fig. 11. Relative error of the asymptotic Vesely approximation (zoom).

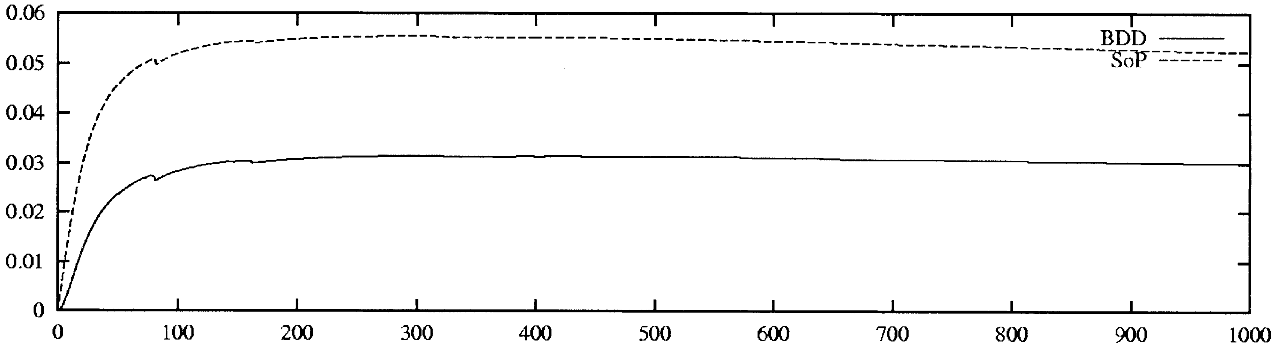

Fig. 12. Relative error of the full Vesely approximation (zoom).

Table 2
Running times in second to assess the reliability with the different methods

Name	# Gates	# Variables	|BDD|	# MCS	Running times (s)							
					$F^{[M,\mathrm{BDD}]}$	$F^{[M,\mathrm{SoP}]}$	$F^{[\mathrm{BP,BDD}]}$	$F^{[\mathrm{BP,SoP}]}$	$F^{[\mathrm{V,BDD}]}$	$F^{[\mathrm{V,SoP}]}$	$F^{[V(\infty),\mathrm{BDD}]}$	$F^{[V(\infty),\mathrm{SoP}]}$
baobab1	84	61	7362	2684	7.99	0.80	0.06	0.02	10.37	1.81	0.06	0.02
baobab2	40	32	197	4805	0.18	1.25	0.01	0.02	0.24	2.91	0.00	0.02
baobab3	107	80	11,789	1527	49.26	0.41	0.29	0.02	53.20	0.87	0.29	0.02
das9201	82	122	690	13,949	0.68	2.70	0.02	0.04	0.90	6.17	0.02	0.04
das9202	36	49	70	578	0.01	0.02	0.00	0.01	0.01	0.03	0.01	0.01
das9204	30	53	87	13,248	0.22	9.63	0.01	0.07	0.27	22.09	0.00	0.07
edf9201	132	183	2607	346,696	0.27	8.96	0.03	0.80	0.43	24.25	0.03	0.80
elf9601	242	145	32,682	2642	1.86	0.16	1.05	0.10	2.00	0.23	1.06	0.10
isp9601	104	143	1511	107,693	0.78	14.34	0.02	0.31	1.04	34.74	0.03	0.31
isp9602	122	116	1159	25,563	0.16	0.91	0.03	0.09	0.22	2.19	0.03	0.09
isp9603	95	91	4727	3136	5.02	0.78	0.05	0.02	6.44	1.71	0.04	0.02
isp9604	132	215	706	491,655	0.13	17.10	0.03	1.29	0.17	42.17	0.03	1.29
isp9605	40	32	748	590	0.78	0.20	0.01	0.01	1.07	0.42	0.01	0.00
isp9606	41	89	297	1776	0.03	0.04	0.01	0.01	0.04	0.08	0.01	0.01
isp9607	65	74	344	6100	0.52	3.14	0.01	0.03	0.68	7.64	0.00	0.03
jbd9601	315	533	82,017	14,007	9.59	17.69	0.90	1.90	13.17	30.06	0.90	1.90

All the above remarks apply to almost all systems we dealt with.

5.2. *Efficiency*

In order to test the efficiency of the four methods, we applied them on real-life FTs of various sizes (and coming from various industries). Table 2 gives the results. The first five columns give some information about the trees (name, number of gates, number of basic events, size of the BDD, number of MCS considered). The actual number of cut sets is almost always bigger than the given number, but we considered here only the most important MCS. The last height columns give the running times of both the classical and the BDD approach for the four methods under study. The running times are those to assess the reliability at both 24, 680, 8760 and 43,800 h.

Several remarks can be made about these results.

- $F^{[\mathrm{BP}]}$ and $F^{[V(\infty)]}$ are much easier to compute than $F^{[M]}$ and $F^{[V]}$. This holds for both the classical and the BDD approaches.

All of the methods are quite efficient. None of them takes more 60 s on a laptop computer.

When the number of cut sets is low, the classical approach is often faster than the BDD approach, although less precise.

6. Conclusion

The exact value of system reliability cannot be computed from a FT. In this article, we studied four different methods to compute approximate values. We considered implementations for both the classical minimal cut sets/rare-event approach and the BDD approach. We show, by means of examples, that these methods are accurate and efficient. With that respect, the full and asymptotic Vesely approximations are especially interesting. The full Vesely approximation gives almost always the most accurate results. The asymptotic Vesely approximation is less precise but much faster.

Throughout this article, we assumed that the FTs under study are coherent. Several important properties we used here are true only for such systems. However, one has sometimes to handle non-coherent Boolean models, for instance when dealing with success branches of event trees. The mathematical framework to design approximate computations of the reliability of non-coherent systems is still to develop. This development requires almost certainly to revisit a number of central notions of FT analysis, including the notion of importance factors.

References

[1] Amari SV. Generic rules to evaluate system failure frequency. IEEE Trans Reliab 2000;49:85–7.

[2] Apostolakis G, Chu TL. The unavailability of systems under periodic test and maintenance. Nucl Technol 1980;50:5–15.

[3] Barlow RE, Proschan F. Theory for maintained system: distribution of time to first failure. Math Oper Res 1976;1:32–42.

[4] Birnbaum ZW. On the importance of different components and a multicomponent system. In: Korishnaiah PR, editor. Multivariable analysis II. New York: Academic Press; 1969.

[5] Cocozza-Thivent C. Processus stochastiques et fiabilité des systèmes. Berlin: Springer; 1997. ISBN 3-540-63390-1.

[6] Cocozza-Thivent C, Kalashnikov V. The failure rate in reliability: numerical treatment. J Appl Math Stoch Anal 1997; 10(1):21–45.

[7] Coudert O, Madre J-C. Metaprime: an iteractive fault tree analyser. IEEE Trans Reliab 1994;43(1):121–7.

[8] Dutuit Y, Rauzy A. Efficient algorithms to assess components and gates importances in fault tree analysis. Reliab Engng Syst Safety 2000;72(2):213–22.

[9] Dutuit Y, Rauzy A. Approche analytique évenementielle: l'arbre de défaillance in Maîtrise des risques et sûreté de fonctionnement des systèmes de production. In: Niel E, Craye E, editors. Hermès-Lavoisier, collection IC2; 2002.

[10] Dutuit Y, Rauzy A, Signoret J-P. Evaluation of systems reliability by means of binary decision diagram. Proceedings of the Probabilistic Safety Assessment Conference, PSA'99, vol. 1. American Nuclear Society; 1999. ISBN 0-89448-640-3, p. 521–8.

[11] Kumamoto H, Henley EJ. Probabilistic risk assessment and management for engineers and scientists. New York: IEEE Press; 1996. ISBN 0-7803-6017-6.

[12] Rauzy A. New algorithms for fault trees analysis. Reliab Engng Syst Safety 1993;05(59):203–11.

[13] Rauzy A. Mathematical foundation of minimal cut sets. IEEE Trans Reliab 2001;50(4):389–96.

[14] Sinnamon RM, Andrews JD. Improved accuracy in qualitative fault tree analysis. Qual Reliab Engng Int 1997;13:285–92.

[15] Sinnamon RM, Andrews JD. Improved efficiency in qualitative fault tree analysis. Qual Reliab Engng Int 1997;13: 293–8.

[16] Vesely WE, Goldberg FF, Robert NH, Haasl DF. Fault tree handbook. Technical report NUREG 0492, US Nuclear Regulatory Commission; 1981.

[17] Schneeweiss WG. Computing failure frequency, MTBF and MTTR via mixed products of availability and unvailability. IEEE Trans Reliab 1981;R-30(4):362–3.

[18] Schneeweiss WG. The fault tree method (in the field of reliability and system safety technology). Hagen: LiLoLe; 1999.