versão impressa ISSN 0101-7438 / versão online ISSN 1678-5142

ESTIMAÇÃO DA COTA INFERIOR PARA A CONFIABILIDADE DE SISTEMAS POR ÁRVORES DE FALHAS

Paulo Renato Alves Firmino *
Departamento de Engenharia de Produção
Universidade Federal de Pernambuco (UFPE)
Recife – PE
praf62@yahoo.com

Enrique López Droguett
Departamento de Engenharia de Produção
Universidade Federal de Pernambuco (UFPE)
Recife – PE
ealopez@ufpe.br

* *Corresponding author* / autor para quem as correspondências devem ser encaminhadas

Recebido em 04/2005; aceito em 12/2005 após 1 revisão
Received April 2005; accepted December 2005 after one revision

Resumo

A técnica de árvores de falhas é uma das principais ferramentas empregadas em confiabilidade e análise de risco para o suporte nas tomadas de decisão e controle de gestores na busca da garantia da execução satisfatória das funções de um dado sistema e seus componentes, considerando as condições ambientais e de operação. Um dos principais problemas referentes à análise de árvores de falhas atualmente enfatizados na literatura refere-se à construção de procedimentos que aliem eficiência computacional e precisão quando do cálculo da probabilidade de ocorrência do evento topo da árvore, probabilidade esta geralmente considerada como a probabilidade de falha do sistema. Este trabalho sugere uma maneira de tratar deste problema de inferência através da remoção prévia das redundâncias da árvore e da subseqüente aplicação de algoritmos recursivos. Demonstra-se também a maior precisão do método proposto em relação a técnicas tradicionais. O procedimento proposto é ilustrado através de um exemplo.

Palavras-chave: confiabilidade; árvores de falhas; redundâncias.

Abstract

The fault tree analysis is an important technique in the context of reliability and risk analysis providing support for decision making and helping managers in assuring that a given system and their components will perform accordingly, given a set of operational and environmental conditions. Nowadays, one of the main problems emphasized in the fault tree related literature is concerned with procedures that contemplate computational efficiency as well as precision in the estimation of the fault tree top event probability. This paper suggests a new approach to tackle this inference problem, which mainly consists of removal of the fault tree redundancies with subsequent application of recursive algorithms. It is also shown the improved precision of the proposed approach when compared to traditional techniques. The proposed approach is then illustrated by means of an example application.

Keywords: reliability; fault trees; redundancies.

1. Introdução

A análise de árvores de falhas permite a obtenção das medidas de confiabilidade, referindo-se aos eventos indesejáveis inerentemente ligados aos sistemas. Na sua montagem, árvores de falhas postulam um provável evento indesejável do sistema, chamado de evento topo da árvore, e representam todas as combinações de eventos causadores do mesmo, através de regras de álgebra booleana. Entre estes eventos causadores, têm-se falhas de subsistemas ou componentes, que em um maior nível de detalhamento são representados por eventos básicos, os quais são fenômenos observáveis que quando ocorridos contribuem para a falha dos subsistemas que os expõem.

A utilização de árvores de falhas para a documentação de causalidades em sistemas com o seu respectivo tratamento probabilístico é uma abordagem já bastante difundida na literatura da engenharia de confiabilidade e análise de risco, sendo em muitos casos parâmetros de entrada para outros métodos cujo nível de detalhamento de informações é mais genérico. Citem-se como exemplos as análises de árvores de eventos e de diagramas de seqüência de eventos, que tratam do comportamento dinâmico do sistema, detalhado em árvores de falhas dos eventos referentes aos seus componentes. Recomenda-se para maiores detalhes sobre árvores de eventos (Modarres *et al.*, 1999) e sobre diagramas de seqüências de eventos (Swaminathan & Smidts, 1999).

Podem-se destacar duas preocupações na análise de árvores de falhas. A primeira consiste em como medir a probabilidade de ocorrência de falha do sistema. A segunda direciona-se a como obter e quantificar os cortes mínimos da árvore (seqüências de eventos sem ordenação cronológica que quando ocorridas levam à falha do sistema, sem a necessidade de ocorrência de qualquer evento adicional). Métodos de cálculo exato para o primeiro caso são, em geral, limitados pela complexidade da árvore (Heger *et al.*, 1995) ou requerem algoritmos complexos que podem comprometer a eficiência computacional ou dedutiva durante sua aplicação. Assim, com o intuito de simplificar os cálculos, são adotados métodos de aproximação, tais como o do evento raro (Modarres *et al.*, 1999), cuja deficiência está na possibilidade de inferências distantes do valor exato.

Diante disto, este artigo apresenta uma maneira alternativa de se inferir sobre a confiabilidade de sistemas via árvores de falhas, baseada em regras de álgebra booleana e algoritmos recursivos, tentando aliar maior precisão e eficiência durante os cálculos. Na seção 2, o artigo faz um apanhado geral sobre o problema da manipulação de árvores de falhas e, mais especificamente, sobre os métodos para o cálculo da probabilidade de ocorrência do seu evento topo. Na seção 3, o trabalho propõe um algoritmo recursivo para o cálculo aproximado da probabilidade de ocorrência do evento topo de uma árvore de falhas coerente. Em seguida, traz uma breve apresentação das técnicas de remoção de redundâncias (seção 4) e apresenta o método de aproximação do evento raro (seção 5). Na seção 6, o artigo compara o método de aproximação do evento raro com o algoritmo proposto na seção 3 e em seguida faz um paralelo entre estes e o método proposto que consiste da combinação entre o algoritmo recursivo e a remoção prévia de redundâncias. É demonstrado analiticamente na mesma seção que o método proposto oferece uma cota inferior para a confiabilidade mais precisa do que a obtida pelo método do evento raro e que a não remoção de redundâncias pode levar a inferências não informativas. Na seção 7, discute-se como se comporta o método proposto diante de uma árvore extraída da literatura. O trabalho conclui-se com a seção 8.

2. Métodos para o Cálculo da Probabilidade de Falha em Árvores de Falhas

A idéia clássica usada para o cálculo da probabilidade de ocorrência do evento topo de uma árvore de falhas é baseada na regra da inclusão-exclusão. Assim, para dois cortes mínimos, sejam eles A e B, de uma dada árvore e sob a suposição de independência entre os eventos envolvidos, tem-se que P(*evento topo*) = P($A \cup B$) = P(A) + P($A^c \cap B$), onde A^c refere-se ao evento complementar de A. Desenvolvendo o último termo da última igualdade, tem-se que P(*evento topo*) = P(A) + [1-P(A)]P(B) = P(A) + P(B) – P(A) P(B). Contudo, quando o problema torna-se complexo, este método mostra-se impraticável, uma vez que o número de termos na regra cresce exponencialmente com o número de cortes mínimos envolvidos. Para aliviar estas dificuldades, muitas variações do método da inclusão-exclusão, tais como o da aproximação do evento raro e o da eliminação de cortes mínimos com probabilidades desprezíveis, foram vastamente difundidas nas análises de confiabilidade e de risco (Heger *et al.*, 1995). Além destas, outras técnicas de aproximação podem ser encontradas. Comente-se Mazumdar (1982), que propõe um procedimento para a obtenção de intervalos para a probabilidade de ocorrência do evento topo de uma árvore de falhas a partir da relação empírica entre o seu logaritmo e os logaritmos das probabilidades dos eventos básicos.

Com a tentativa de desvincular-se da necessidade de técnicas de cálculo aproximado acerca da probabilidade de ocorrência do evento topo, os conceitos de diagramas de decisão binária (BDD) foram introduzidos à análise de árvores de falhas, por autores como Rauzy (1993). De uma maneira geral, BDDs são estruturas de dados que encapsulam e manipulam funções booleanas, que por sua vez traduzem algebricamente a estrutura gráfica de árvores de falhas.

A introdução de BDDs aos problemas de manipulação de árvores de falhas, inclusive o do cálculo exato da probabilidade de ocorrência do seu evento topo, gerou um desinteresse natural sobre os métodos de aproximação. O grande desafio passou a ser o desenvolvimento de técnicas robustas que promovessem a conversão de uma árvore de falhas qualquer ao formato de um BDD ordenado (OBDD) apropriadamente. A importância da conversão de árvores de falhas a OBDDs adequados se dá devido ao fato de que sem uma ordenação apropriada, a manipulação do BDD pode se tornar inviável (ver Bryant, 1992) devido o seu tamanho proibitivo. Contudo, tal desafio não foi, ainda, superado. Vários autores (cite-se Bedford & Cooke, 2001; Barlett & Andrews, 1999 e 2000; Dutuit & Rauzy, 2001; Wegner, 2004; Reay & Andrews, 2002 e Jung *et al.*, 2004) têm se deparado com a dificuldade de encontrar um procedimento robusto de conversão de árvores de falhas a BDDs adequadamente ordenados. Isto faz ressurgir o interesse por métodos de cálculo aproximado, tais como o proposto no presente artigo, cujas vantagens em relação a métodos aproximados difundidos pela literatura são discutidas ao longo do texto.

3. Algoritmo Recursivo para a Probabilidade de Falha em Árvores Coerentes

Em geral, uma árvore de falhas é dita coerente quando não possui o complementar de eventos básicos no seu escopo, ou seja, ela é composta por portas lógicas referentes a operações algébricas booleanas de união e interseção entre eventos, sem a presença de complementares.

Supondo uma árvore de falhas coerente, o cálculo da probabilidade de ocorrência do seu evento topo requer um algoritmo bastante simples. De fato, se determinado subsistema da referida árvore possui k eventos básicos e uma porta lógica de união, então apenas a não-ocorrência de todos os seus eventos ($E_1^c \cap E_2^c \cap \ldots \cap E_k^c$, onde E^c refere-se ao evento

complementar de E) evita a ocorrência da sua falha, $P(\text{falha do subsistema}|E_1^c \cap E_2^c \cap ...\cap E_k^c)=0$, e qualquer outra combinação dos E_i's leva a tal ocorrência. Assim, considerando a suposição de independência entre eventos básicos característica da análise de árvores de falhas,

$$P(\text{falha do subsistema}) = 1 - \prod_{i=1}^{k} P(E^c{}_i)$$

Equação 1

Agora, considerando o mesmo raciocínio e sob a mesma suposição, se a porta lógica representa uma interseção, apenas a ocorrência simultânea de todos os eventos componentes do subsistema em questão leva a sua falha, isto é, apenas $P(\text{falha do subsistema } |E_1 \cap E_2 \cap ... \cap E_k)$ é não-nula, o que resulta em

$$P(\text{falha do subsistema}) = \prod_{i=1}^{k} P(E_i)$$

Equação 2

Aplicando-se este raciocínio recursivamente, dos subsistemas mais distantes até o evento topo da árvore, obtém-se uma estimativa para a probabilidade de ocorrência do evento indesejável postulado, utilizando-se recursos computacionais ou dedutivos razoavelmente baixos (ver Figura 1).

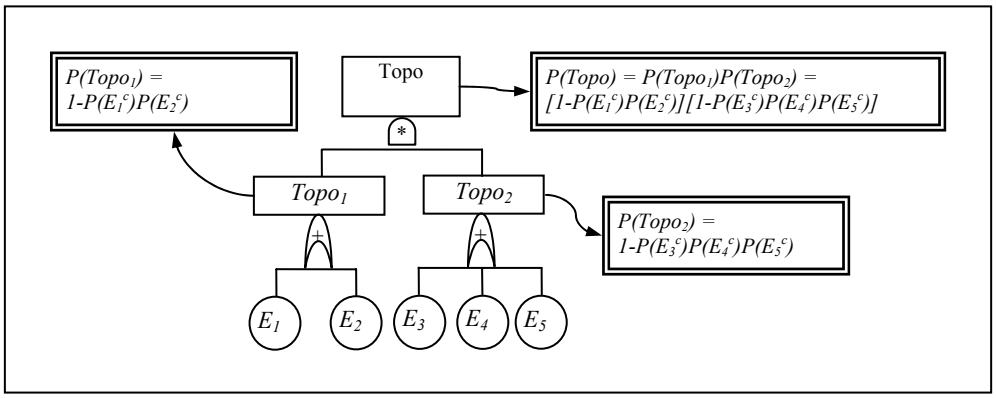

Figura 1 – Algoritmo recursivo para o cálculo da probabilidade de ocorrência do evento topo de árvores de falhas coerentes.

Com a simplicidade do algoritmo acima, o problema a ser resolvido consiste na necessidade de remoção de redundâncias. Pode-se definir como redundância a repetição desnecessária ou indevida de um evento básico, isto é, a repetição de evento básico que venha a gerar cortes não-mínimos ou que leve à repetição de eventos básicos em qualquer corte mínimo da árvore. Se ao invés de E_3 houvesse uma repetição de E_1 no subsistema postulado $topo_2$ (Figura 1), teria-se uma redundância já que da interseção entre $topo_1$ e $topo_2$ seriam gerados cortes como $E_1 \cap E_1$ e $E_1 \cap E_4$. Sem a devida remoção, as redundâncias podem levar a inferências não confiáveis ou não informativas, como será visto posteriormente. Logo, recomenda-se aqui que o procedimento acima seja aplicado apenas após a remoção de todas

as redundâncias da árvore. Será demonstrado que depois de removidas todas as redundâncias da árvore, o algoritmo recursivo comentado nesta seção resulta em uma cota inferior para a confiabilidade.

A seguir são introduzidas algumas técnicas direcionadas à remoção de redundâncias.

4. Técnicas para Remoção de Redundâncias em Árvores Coerentes

O método de remoção de redundâncias proposto por Firmino *et al.* (2004) busca levar uma árvore de falhas coerente a uma compactação que consiste apenas dos seus cortes mínimos. Desta maneira, a álgebra booleana que representa a árvore se constitui ou leva à união dos conjuntos compostos pela interseção de eventos não redundantes, sendo que dentre tais conjuntos não há qualquer um que seja subconjunto de outro. Em outras palavras, após a remoção de suas redundâncias, a árvore de falhas em análise é ou leva à união apenas dos seus cortes mínimos. Vale salientar, contudo, que algumas contrações preliminares da árvore são necessárias. São elas:

C1- a remoção de portas lógicas quando estas são componentes de portas lógicas com a mesma álgebra de eventos;
C2- a remoção de portas lógicas quando estas têm no máximo um componente.

Os métodos de remoção de redundâncias baseiam-se em regras de álgebra booleana tais como as exibidas na Tabela 1. Da tabela, considera-se que antes da primeira igualdade da álgebra de cada regra tem-se o formato sem redundâncias, enquanto que após tais igualdades têm-se as versões com a presença de redundâncias.

Tabela 1 – Regras básicas de álgebra booleana sobre três eventos quaisquer, X, Y, Z.

Regra	*Álgebra*
Distributividade	$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
Idempotência	$X = X \cap X = X \cup X$
Absorção	$X = X \cap (Y \cup X) = X \cup (Y \cap X)$

Após as definições necessárias, são apresentadas algumas das técnicas de remoção de redundâncias. Vale salientar que a remoção de redundâncias se dá apenas após as contrações C1 e C2 comentadas anteriormente nesta seção, e que tais contrações podem ser reutilizadas também após as remoções.

Definição 1 *Seja um evento básico qualquer (EB) e um subsistema raiz de EB (subsistema do qual EB é causa imediata ou não imediata), diga-se R. A geração de EB em relação a R é dada pelo número de subsistemas compreendidos no caminho a percorrer de EB a R, após realizadas as contrações C1 e C2.*

Definição 2 *Seja o topo da ocorrência da redundância (ROT) a raiz da qual o evento básico original (OE) e os redundantes (REs) são descendentes imediatos, isto é, o subsistema descendente do topo da árvore que possui como descendentes o evento original e os redundantes. Seja o evento original da redundância (OE) aquele de menor geração em relação ao ROT e sejam os eventos redundantes (REs) aqueles de maior geração.*

Redundância trivial (*O OE e os REs pertencem à 1ª geração do ROT*): Tem-se que, em álgebra booleana, $ROT = A \cup A = A \cap A = A$, segundo a regra da idempotência. Logo, basta eliminar os *REs* das suas respectivas raízes imediatas (ou topos) ao tratar da árvore de falhas.

Redundância de geração I (*Apenas o OE pertence à 1ª geração do ROT*): Utiliza-se o fato de que $ROT = A \cup (A \cap B) \cup (A \cap D) = A$ (ver Figura 2), assim como $ROT = A \cap (A \cup B) = A$, segundo a regra de álgebra booleana da absorção. Sobre a estrutura da árvore, se os topos do *OE* e do *RE* em análise possuírem álgebras iguais, apenas o *RE* é eliminado do seu topo. Caso contrário, o topo do *RE* é eliminado.

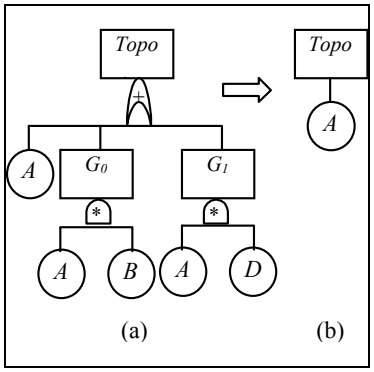

Figura 2 – Presença de redundâncias de geração I.

Redundância de geração II (*O OE pertença à 2ª geração do ROT, o qual possui uma lógica booleana de interseção*): Um *ROT* cuja álgebra booleana é dada por $(A \cup B \cap C) \cap (A \cup D \cap E)$, possui uma redundância de geração II em relação ao evento básico *A* [ver Figura 3(a)]. Após a aplicação das regras da distributividade, idempotência e absorção, tem-se $ROT=A \cup [(B \cap C) \cap (D \cap E)]$. Note-se que a função booleana foi dividida em dois termos:

$$ROT = (G_i \cup G_j) \cap (G_k \cup G_l) = X \cup Y,$$

$$X = G_i \cap (G_k \cup G_l),\ Y = G_j \cap (G_k \cup G_l),$$

Equação 3

Com esta expansão e considerando $G_i = B \cap C$, $G_j = A$, $G_k = A$ e $G_l = D \cap E$, pode-se tratar da redundância de geração I em *Y* [Figura 3(b)]. Para concluir a remoção da redundância de geração II sobre *A*, aplica-se uma lógica inversa ao termo *X* [Figura 3(b)]. Esta lógica inversa remove o topo do evento repetido *A* de *X* quando apenas o evento repetido *A* é removido de *Y*, e remove apenas o evento repetido *A* de *X* quando o topo do evento repetido *A* é removido de *Y*. Esse procedimento foi inicialmente proposto por Firmino *et al.* (2004) sob a nomenclatura de método espiral de eliminação de cortes não-mínimos (MEEC). A Figura **3**(c) ilustra o resultado da remoção da redundância de geração II sobre o evento *A*. É importante perceber que após o tratamento da redundância de geração I e da lógica inversa [Figura 3(b)], a árvore permite a contração C2 tanto para *Y* quanto para $G_k + G_l$ [Figura 3(c)]. Comente-se também que após a contração C2 de $G_k + G_l$, G_1 torna-se passível da contração C1, o que resulta na árvore exibida na Figura 3(d).

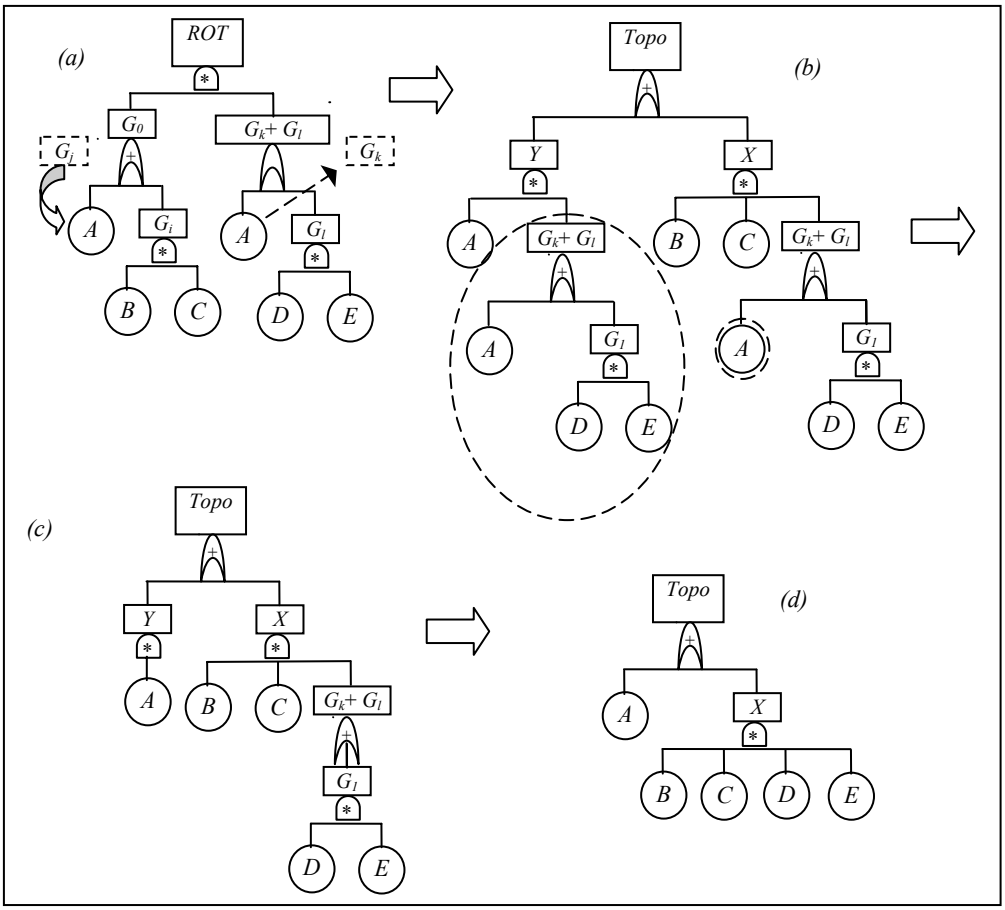

Figura 3 – Presença de redundâncias de geração II.

Redundância de geração II+ (*O OE e os REs pertencem à 2ª geração do ROT, o qual possui uma lógica booleana de união*): Neste tipo de ocorrência de redundâncias, o método de redução de Faunet (Reay & Andrews, 2002) é aplicado. Utilizando álgebra booleana tem-se que $ROT = (X \cap Y) \cup (X \cap Z) = X \cap (Y \cup Z)$ (ver Figura 4).

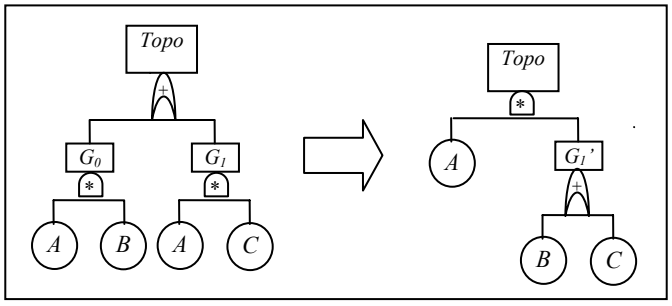

Figura 4 – Presença de redundâncias de geração II+.

Redundância de geração III (*Não há qualquer das relações citadas anteriormente, ao menos o evento original ou os redundantes pertencem à 3ª geração de ramificações do ROT, o qual possui uma lógica booleana de interseção*): Aqui o MEEC é generalizado e são introduzidas duas singularidades. A 1ª é que o MEEC finaliza-se sem a aplicação da lógica inversa. A 2ª indica que antes da utilização do MEEC é preciso a seguinte precaução: quando o evento redundante pertencer à 3ª geração do *ROT*, este deve passar a ser considerado como o evento original, a não ser que o evento original também possua esta característica.

Uma vez compreendido o MEEC, sua generalização passa a ser facilmente desenvolvida. A partir da Equação 3 e considerando que X não contém o evento original, o que conseqüentemente leva Y a o possuir, a mesma lógica de igualdade é aplicada recursivamente em Y, de forma a expandi-la e aproximar o evento original do então *ROT*. Quando o evento original tornar-se uma ramificação do *ROT*, ter-se-á uma redundância de geração I, chegando-se à solução possível.

Redundância de geração elevada (*Não há qualquer das relações citadas anteriormente e a porta lógica do topo da ocorrência das redundâncias é de interseção*): Aqui o método utilizado é, também, o MEEC generalizado de maneira similar à última apresentada, com a aplicação da lógica inversa à última expansão realizada.

Quando se remove redundâncias de geração III ou elevada através do MEEC generalizado, não é possível obter-se uma árvore de falhas sem repetições, mas busca-se promover uma árvore de falhas remanescente que possua apenas cortes mínimos.

O procedimento para a remoção de redundâncias de geração III ou elevada pode ser melhor compreendido analisando-se a árvore de falhas exibida na Figura 5, que possui uma redundância sobre o evento B. Aqui, o MEEC elimina todos os cortes não-mínimos que certamente serão gerados devido o *ROT* ser uma porta lógica de interseção. Observando a Figura 5(c), percebe-se que agora os eventos básicos D, E, e o próprio B possuem uma repetição. Estas repetições são inevitáveis devido às características da árvore proposta, porém são necessárias para que seja garantida a geração de todos os cortes mínimos. Como os seus topos são subsistemas cujas portas lógicas são de união, não haverá problemas com suas permanências na árvore de falhas e suas repetições não devem ser consideradas como redundâncias.

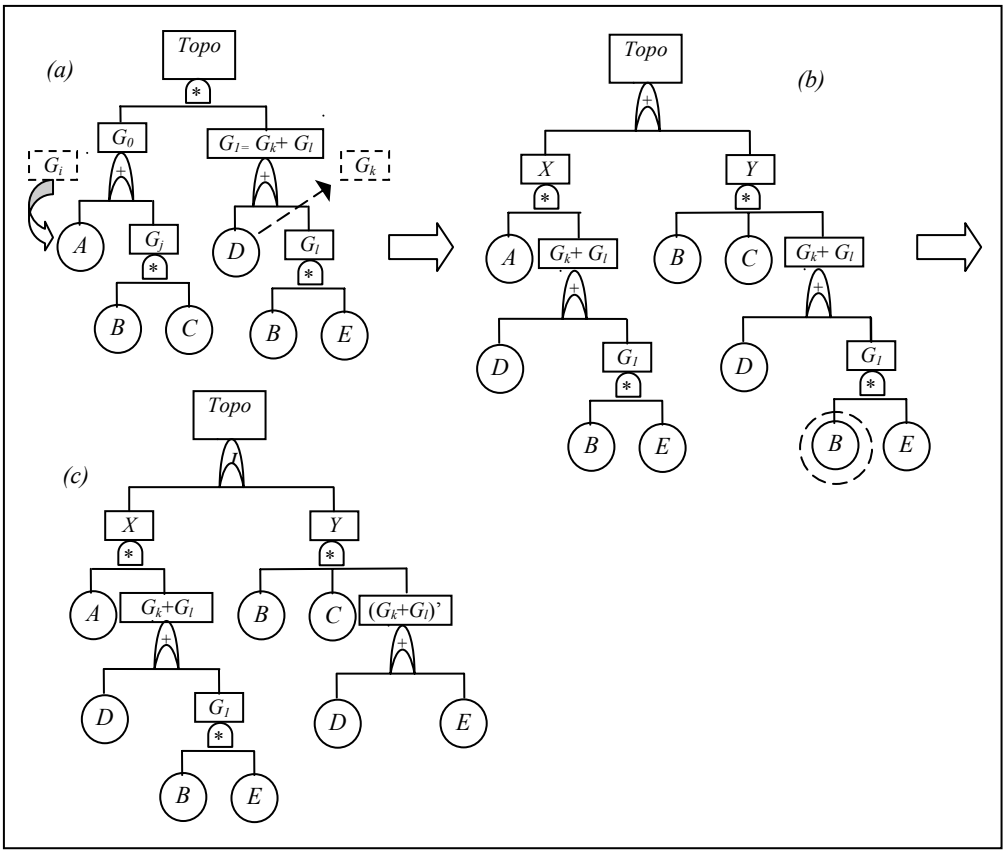

Figura 5 – Presença de redundâncias de geração III.

Os métodos de remoção de redundâncias propostos por Firmino *et al.* (2004) não são robustos a ponto de garantir a remoção de todas as redundâncias presentes em uma dada árvore de falhas até o presente momento. Os próprios autores enfatizam a dificuldade de remoção diante de combinações entre redundâncias, sendo este tipo de redundância ainda alvo de estudos.

5. Método de Aproximação do Evento Raro

O método de aproximação do evento raro supõe que quando as probabilidades individuais de um conjunto de eventos são relativamente baixas, a probabilidade da união de tais eventos pode ser aproximada pelo somatório das suas probabilidades. Formalmente, segundo Modarres *et al.* (1999), aproxima-se $P\left(\bigcup_{i=1}^{n} E_i\right)$ por $\sum_{i=1}^{n} P(E_i)$ quando $P(E_i) \leq (50n)^{-1}$, para $\forall\ i = 1, 2, ..., n$.

O método de aproximação do evento raro é vastamente aplicado em análises de árvores de falhas para o cálculo da probabilidade de ocorrência do evento topo (Heger *et al.*, 1995 e

Hauptmanns, 2002). Como $P\left(\bigcup_{i=1}^{n} E_i\right) \leq \sum_{i=1}^{n} P(E_i)$, a aproximação por evento raro atribui uma cota máxima para a probabilidade de ocorrência do evento topo da árvore, isto é, a falha do sistema. Conseqüentemente, a confiabilidade recebe uma cota mínima por ser o complementar de tal resultado.

A Equação 4, extraída de Firmino & Droguett (2004), mostra como se comporta o erro percentual máximo cometido pelo método de aproximação do evento raro diante de uma árvore de falhas que possui dois cortes mínimos compostos por *n* eventos em comum e apenas *1* diferente. Por exemplo, se *n=2*, então os cortes seriam compostos pelos eventos básicos $A_1 \cap A_2 \cap A_3$ e $A_1 \cap A_2 \cap A_4$, respectivamente. Quando os cortes mínimos possuem eventos básicos em comum, $n \geq 1$, a aproximação por evento raro pode levar a estimativas muito diferentes do valor real, chegando a um erro percentual extremo, assintótico a 100% com *n* suficientemente grande.

$$erro_{\%} = \frac{1}{\left|1 - 2 \cdot 100^{\frac{1}{n+1}}\right|}$$

Equação 4

Na próxima seção será realizada uma comparação entre o método de aproximação do evento raro, o método de aproximação a partir da aplicação recursiva da Equação 1 e da Equação 2 e o método proposto pelo artigo, que combina tais equações com a remoção prévia das redundâncias da árvore.

6. Comparação entre os métodos de aproximação apresentados

Através do método proposto, o cálculo exato da probabilidade de ocorrência do evento topo de uma dada árvore de falhas coerente torna-se bastante simples quando a árvore não possui redundâncias de geração III ou elevada. Nestes casos, basta remover as redundâncias existentes, o que resultará em uma árvore sem qualquer repetição de eventos básicos, e fazer uso da Equação 1 e da Equação 2, aplicando-as recursivamente dos subsistemas mais distantes aos mais próximos do topo da árvore, como visto na seção 3. Assim, o procedimento proposto acumula a probabilidade de ocorrência de falha de cada subsistema até que se chegue ao topo da árvore, levando a um cálculo exato para a probabilidade de sua ocorrência.

Porém, a necessidade de remoção de redundâncias de geração III ou elevada levam a includências entre os cortes mínimos da árvore, uma vez que haverá eventos básicos repetidos neste último caso. Isto torna as interseções entre os cortes mínimos problemáticas, requerendo cuidados dispendiosos para a realização de inferências exatas.

De qualquer forma, torna-se óbvio que quando não há redundâncias de geração III ou elevada, os cálculos tornam-se mais simples e a aplicação do método aqui proposto leva a probabilidades exatas. Faz-se, então, necessária apenas a demonstração de que após a remoção de redundâncias de geração III ou elevada de uma árvore de falhas coerente, os cálculos sobre a probabilidade de ocorrência do evento topo levam a uma cota superior mais precisa do que aquela obtida pelo método de aproximação do evento raro. Além disto, mostra-se pertinente a demonstração de que a não-remoção de redundâncias de geração III

ou elevada compromete uma cota superior para a probabilidade de falha do sistema, podendo inclusive ser não informativa de uma maneira geral.

Demonstração 1 *Considera-se como ponto de partida que* $P(Topo) = P\left(\bigcup_{i=1}^{k} E_i\right) = S + \delta$, *onde* $S = \sum_{i=1}^{k} P(E_i)$ e $\delta = w_1 + w_2 + w_3 + \ldots + w_c$, *cujos valores são dados por*

$$w_1 = -\sum_{i=1}^{k}\sum_{j=i+1}^{k} P(E_i \cap E_j)$$

$$w_2 = \sum_{i=1}^{k}\sum_{j=i+1}^{k}\sum_{l=j+1}^{k} P(E_i \cap E_j \cap E_l)$$

$$w_3 = -\sum_{i=1}^{k}\sum_{j=i+1}^{k}\sum_{l=j+1}^{k}\sum_{m=l+1}^{k} P(E_i \cap E_j \cap E_l \cap E_m)$$

...

$$w_c = (-1)^{k-1} P(E_1 \cap E_2 \cap \ldots \cap E_k),$$

$$c = \left|\sum_{i=2}^{k}\binom{k}{i} - k\right|.$$

Equação 5

Devido à desigualdade de Boole, $P\left(\bigcup_{i=1}^{n} E_i\right) \leq \sum_{i=1}^{n} P(E_i)$ *, demonstrar-se-á que* $\delta \leq 0$ *e que* δ *é sub-estimado.*

Dado que o objetivo da remoção de redundâncias é tornar a álgebra booleana de eventos da árvore de falhas composta (ou geradora) dos seus cortes mínimos, apenas, o termo S da Equação 5 será sempre obtido de maneira exata já que seus componentes são os mesmos.

δ, por sua vez, terá seu valor sub-estimado porque não haverá qualquer tratamento quanto às interseções, isto é, eventos repetidos potencializarão a probabilidade da interseção envolvida. Quanto ao sinal de δ, o que garante que este continuará não-positivo é o fato de que $|w_i| \geq w_j$, $\forall$ *i impar,* $j = i+1$, $0 < i \leq c$. *Logo, ter-se-á uma superestimação da probabilidade exata de ocorrência do evento topo de uma dada árvore de falhas.*

Demonstração 2 *Fazendo uso da Equação 5, tem-se que no método de aproximação do evento raro δ=0. Assim,*

$$P(Topo)_{\text{com remoção}} \leq P(Topo)_{\text{evento raro}}.$$

Retornando à árvore de falhas geradora do erro percentual exibido na Equação 4, seção anterior, tem-se redundâncias de geração II+ e as inferências pelo método proposto são exatas.

Demonstração 3 *Fazendo uso da Equação 5, tem-se que caso a remoção de redundâncias não seja realizada, não se assegura que os componentes de S, os* E_i*'s, estarão isentos de redundâncias e tampouco que não haverá quaisquer deles contidos em quaisquer outros, isto é, cortes não-mínimos. Isto compromete o termo S e não garante uma cota superior para P(Topo).*

A seguir, explica-se dedutivamente a Demonstração 1, a Demonstração 2 e a Demonstração 3 através da árvore de falhas apresentada na Figura 5(a).

A função booleana referente à árvore de falhas da Figura 5(a) é dada pela Equação 6.

$$TOPO = [A \cup (B \cap C)] \cap [D \cup (B \cap E)]$$

Equação 6

Exemplo 1 *Seja uma árvore de falhas que possui uma redundância de geração III, tal qual o evento B na Figura 5(a). A correspondente álgebra de eventos, quando desenvolvida a partir da regra da distributividade sumarizada na Tabela 1, é dada por*

$$\begin{aligned} TOPO &= [A \cup (B \cap C)] \cap [D \cup (B \cap E)] = \\ &= (A \cap D) \cup (A \cap B \cap E) \cup (B \cap C \cap D) \cup (B \cap B \cap C \cap E) \end{aligned}$$

Equação 7

Relacionando a Equação 5 com a Equação 7, tem-se $k=4$, onde $E_1 = A \cap D$, $E_2 = A \cap B \cap E$, $E_3 = B \cap C \cap D$ e $E_4 = B \cap B \cap C \cap E$. Como E_4 possui a repetição do evento B, nos cálculos da probabilidade de ocorrência do evento topo sem qualquer cuidado em relação às interseções e supondo independência entre os eventos, $P(E_4)$ terá seu valor reduzido pela multiplicação por $P(B)$. Isto leva a uma redução de S e a maior imprecisão nos cálculos de δ, de forma que a probabilidade aproximada pelo algoritmo recursivo sem a utilização da remoção de redundâncias não assegura a superestimação da probabilidade exata da ocorrência do evento topo.

Considerando-se agora a aplicação do método de remoção de redundâncias na árvore sugerida pela Figura 5(a), tem-se como resultado a árvore sem redundâncias exposta na Figura 5(c), cuja álgebra de eventos pode ser dada tal como a seguir:

$$TOPO = \{A \cap [D \cup (B \cap E)]\} \cup [(B \cap C) \cap (D \cup E)]$$

Equação 8

Tem-se como resultado final da aplicação da regra da distributividade que:

$$\begin{aligned} TOPO &= \{A \cap [D \cup (B \cap E)]\} \cup [(B \cap C) \cap (D \cup E)] = \\ &= (A \cap D) \cup (A \cap B \cap E) \cup (B \cap C \cap D) \cup (B \cap C \cap E) \end{aligned}$$

Equação 9

Como na Equação 7, $k = 4$, onde E_1, E_2 e E_3 são definidos da mesma maneira. O que muda, de fato, é que agora se tem E_4 de forma ideal. Analisando a Equação 5, garante-se que S será obtido de forma exata nos cálculos da probabilidade da união. A inferência sobre δ será sub-estimada, já que haverá termos reduzidos pelas interseções não tratadas entre os $E_i's$.

Analisando o erro percentual cometido pelos métodos de aproximação por evento raro, com e sem remoção de redundâncias, tem-se, considerando alguns valores para as probabilidades dos eventos básicos envolvidos no exemplo, os resultados da Tabela 2. Na 1ª simulação, avalia-se o sistema sob elevadas probabilidades para os eventos básicos não satisfazendo à condição imposta pelo método de aproximação do evento raro (seção 5), enquanto que nas demais tal condição é satisfeita. Em todos os casos, os procedimentos de remoção de redundâncias seguidos do algoritmo recursivo apresentado na seção 3

apresentam melhores resultados. Pode-se perceber, também, que com tal método todos os erros relativos não-absolutos são negativos, o que implica em uma cota superior para a probabilidade exata.

Tabela 2 – Erro percentual dos métodos de aproximação apresentados diante da árvore tratada no Exemplo **1**.

			Erro % não-absoluto por método de aproximação		
P(A), P(C), P(D)	*P(B), P(E)*	*Probabilidade Exata*	*Com Remoção*	*Sem Remoção*	*Evento Raro*
2,83E-01	*6,84E-01*	*2,82E-01*	*-5,72E-02*	*7,62E-02*	*-4,15E-01*
7,07E-02	*1,71E-01*	*9,50E-03*	*-1,86E-02*	*1,56E-01*	*-5,14E-02*
1,77E-02	*4,27E-02*	*3,89E-04*	*-2,01E-03*	*7,68E-02*	*-4,99E-03*
4,42E-03	*1,07E-02*	*2,07E-05*	*-1,51E-04*	*2,39E-02*	*-3,67E-04*
1,10E-03	*2,67E-03*	*1,24E-06*	*-9,92E-06*	*6,33E-03*	*-2,40E-05*
2,76E-04	*6,68E-04*	*7,66E-08*	*-6,28E-07*	*1,61E-03*	*-1,52E-06*
6,91E-05	*1,67E-04*	*4,77E-09*	*-3,53E-08*	*4,03E-04*	*-9,51E-08*

É importante notar que, embora aparentemente pequeno, o erro cometido ao aplicar-se o método de aproximação do evento raro na última simulação equivale a 2,69 vezes o cometido pelo método proposto na mesma ocasião.

Na próxima seção apresenta-se o método aqui proposto por meio de um exemplo.

7. Exemplo de aplicação

A árvore de falhas exibida na Figura 6 é extraída de Reay & Andrews (2002), que na ocasião propõem uma estratégia de análise baseada em uma rede neural utilizada para selecionar o esquema de ordenação mais adequado para cada módulo independente da árvore, respeitando suas características individuais, de forma a elevar as chances de conversão a um OBDD ótimo.

Obedecendo às propostas sugeridas pelo presente artigo, a primeira etapa a ser realizada é a de contração da árvore. Da Figura 6, vê-se que a álgebra da porta lógica *G1* é idêntica à do seu subsistema topo (o evento *topo*), ambas representam a interseção de eventos. Logo, *G1* deve ser excluído da árvore, levando tanto *G4* quanto *G5* a serem componentes do evento *topo*.

Dando início à remoção de redundâncias, deve-se eliminar, nesta ordem, todas as redundâncias triviais, de geração I (relativas a *A* e *E*, no exemplo), de geração II (sobre o evento *N*), de geração III (sobre *D*) e, enfim, de geração elevada. Esta ordem de remoção eleva a eficiência do processo de remoção de redundâncias, uma vez que redundâncias de geração mais elevada podem ser eliminadas durante a remoção de redundâncias que reduzem a árvore. Perceba-se que apesar de haver uma repetição do evento *K*, esta não deve ser considerada uma redundância uma vez que o seu *ROT* (*G5*) não possui uma álgebra de interseção, não havendo, portanto, problemas com sua permanência.

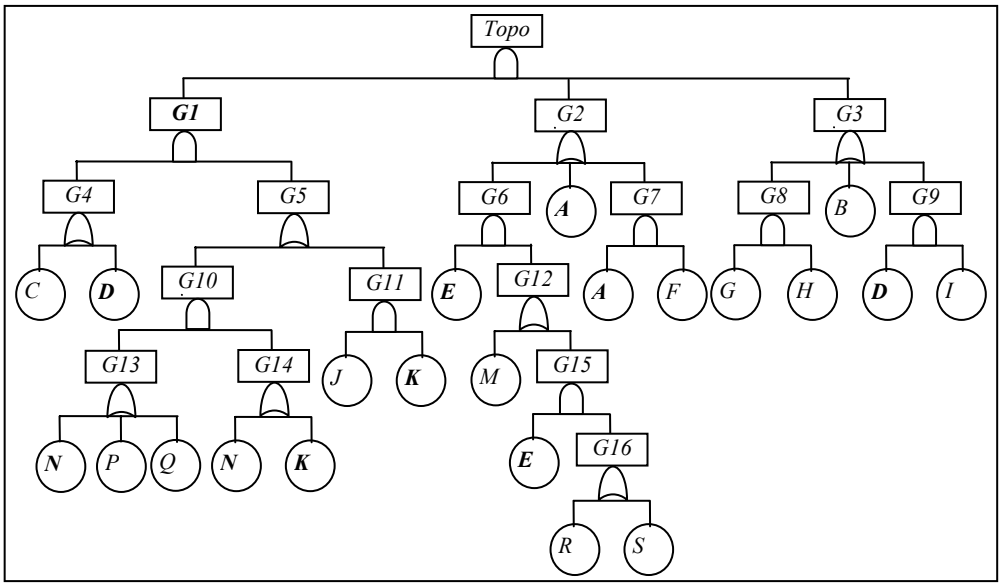

Figura 6 – Árvores de falhas extraída de Reay & Andrews (2002).

Para o tratamento das redundâncias de geração I, relacionadas aos eventos *A* e *E*, tem-se respectivamente a exclusão de *G7* e do evento *E*, componente de *G15* [ver Figura 7(a)]. Com isso, *G15* torna-se passível da contração C2 (seção anterior), que depois de aplicada leva à contração C1 sobre *G16*. Ao final, ter-se-á *G2* tal qual na Figura 7(b).

A próxima redundância a ser tratada é a do evento *N*, de geração II, que após removida leva à árvore exibida na Figura 7(c), onde *G´1* é passível da contração C1. A Figura 7(d) exibe o resultado final do tratamento dessa redundância.

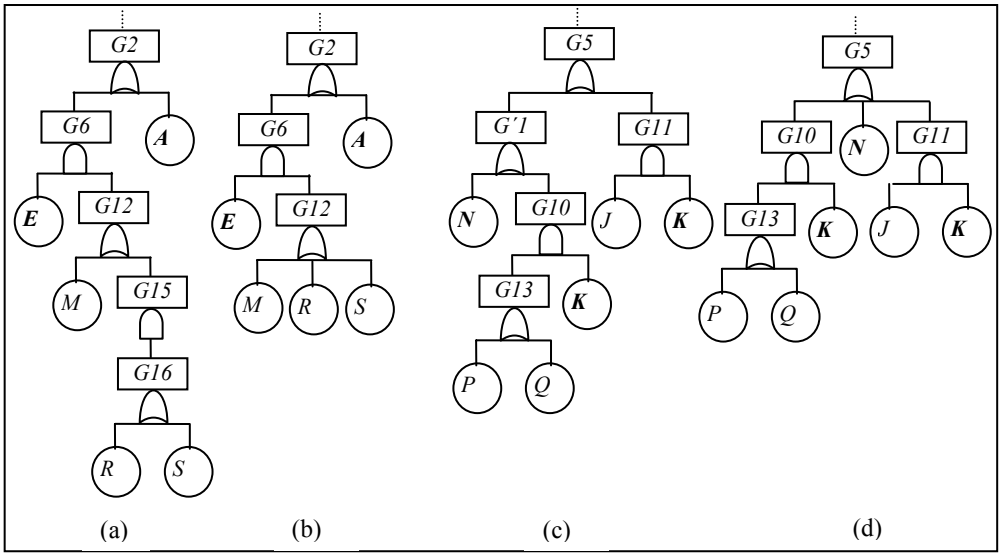

Figura 7 – Remoção de redundâncias de geração I e II do exemplo exibido na Figura 6.

Da Figura 7(d), pode-se constatar que a remoção da redundância acerca de *N* levou a repetição do evento *K* à classificação de redundância de geração II+. A remoção desta nova redundância leva *G5* à estrutura apresentada na Figura 8, após aplicadas as contrações necessárias. Vale salientar que até agora todas as remoções levaram à redução da árvore.

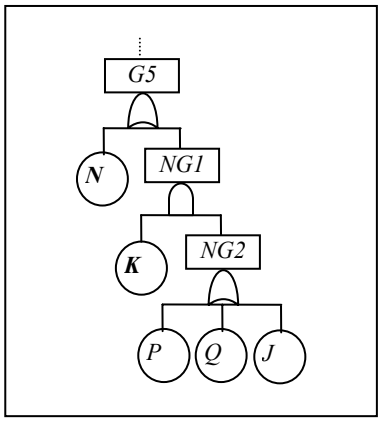

Figura 8 – Remoção de redundância de geração II+, gerada durante as remoções relativas ao exemplo exibido na Figura 6.

Para finalizar o processo de remoção de redundâncias, trata-se da repetição do evento básico *D*, classificada como uma redundância de geração III. Isto decorre do fato de que embora o *OE* (*D*, componente de *G4*) seja de geração 2 em relação ao *ROT* (o evento *topo*), o *RE* (*D*, componente de *G9*) é de geração 3, o que leva o mesmo à condição de evento original. Fazendo uma relação com a Equação 3, considera-se $G_i = G_3 - G_9$ (onde "-" implica em exceto), $G_j = G_9$, $G_k = C$ e $G_l = D$ [ver Figura 9(a)]. A expansão dos termos pode ser visualizada pela Figura 9(b). É possível constatar que a expansão tornou *G9* passível da contração C1, que após contraído leva *Y* a assumir a estrutura exibida na Figura 9(c), permitindo a remoção da redundância de geração I elaborada. A remoção da redundância de geração III leva *Y* à estrutura mostrada na Figura 9(d).

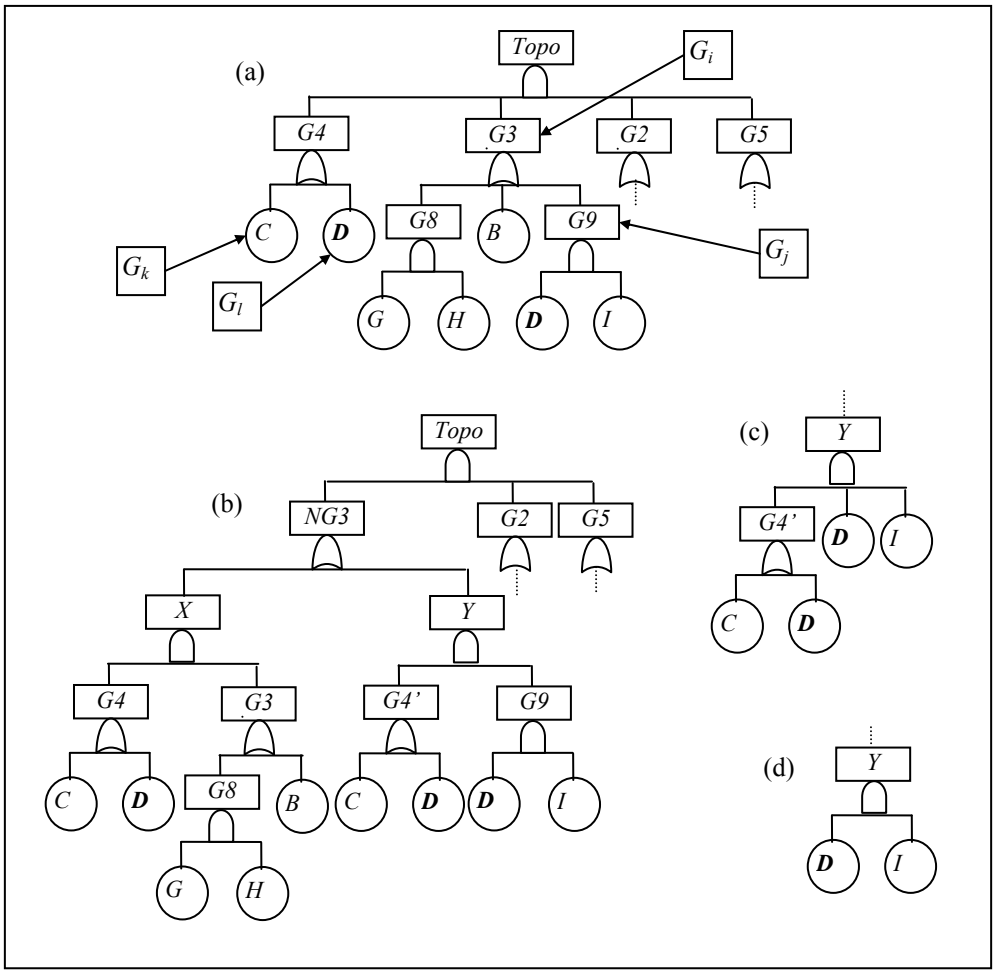

Figura 9 – Remoção de redundâncias de geração III do exemplo exibido na Figura 6.

Ao final da remoção de redundâncias, a árvore assume a estrutura esboçada pela Figura 10. Deve-se destacar que houve uma redução significativa do tamanho da árvore. Enquanto que a estrutura original possuía 17 portas lógicas e 22 eventos básicos, a árvore exibida pela Figura 10 possui 13 portas lógicas e 17 eventos básicos. Contudo, esta característica não é uma regra. É possível que após a remoção de redundâncias haja um aumento em ao menos um dos componentes da árvore de falhas, a depender do gênero e da quantidade de redundâncias de geração III e elevada.

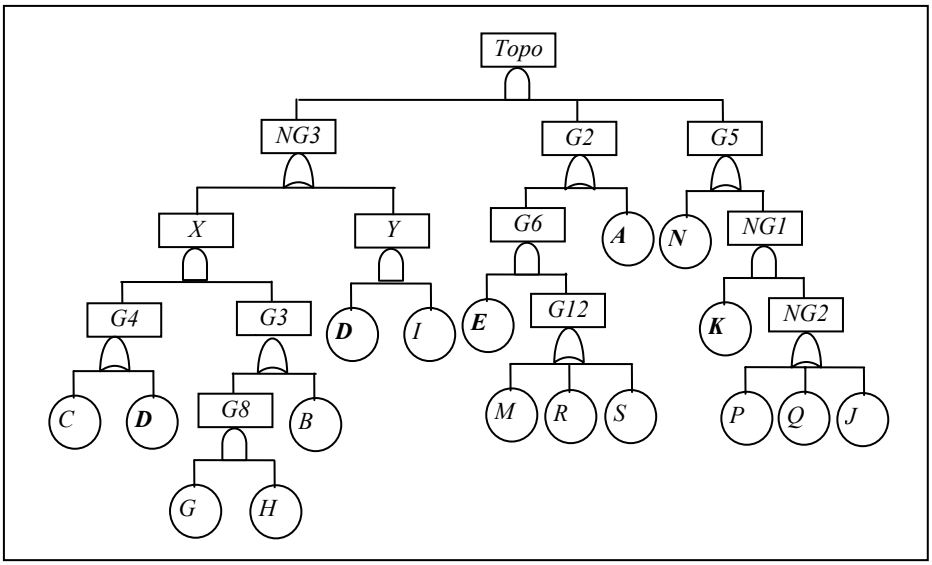

Figura 10 – Árvore resultante da remoção de redundâncias da estrutura exibida na Figura 6.

Ao final, tem-se 80 cortes mínimos, com probabilidades variando de 1,35E-09 (corte $D \cap I \cap A \cap N$) a 8,47E-16 (corte $C \cap G \cap H \cap E \cap S \cap K \cap J$), o que indica a adequação do uso do método do evento raro, já que é recomendado que todos os cortes tenham no máximo a probabilidade 2,5E-04 para a possibilidade de sua aplicação (ver Modarre *et al.*, 1999). A Tabela 3 exibe as probabilidades dos eventos básicos tal como propõem Reay & Andrews (2002), enquanto que a Tabela 4 compara os métodos do evento raro, o proposto pelo artigo e o exato (a partir de BDDs).

Tabela 3 – Probabilidades associadas aos eventos básicos da árvore exibida pela Figura 6.

Ev. Bás.	*Probab.*	*Ev. Bás.*	*Probab.*
A	*0,003*	*J*	*0,004*
B	*0,0045*	*K*	*0,007*
C	*0,008*	*M*	*0,015*
D	*0,01*	*N*	*0,005*
E	*0,0035*	*P*	*0,008*
F	*0,0025*	*Q*	*0,0065*
G	*0,015*	*R*	*0,012*
H	*0,012*	*S*	*0,006*
I	*0,009*		

Da Tabela 4, vê-se que embora existam probabilidades muito baixas associadas aos eventos básicos (Tabela 3), o que leva a uma baixa probabilidade de ocorrência de falha do sistema modelado, o erro percentual do método do evento raro é 2,5 vezes maior que o do método proposto pelo trabalho.

Tabela 4 – Erro percentual dos métodos de aproximação apresentados diante da árvore exibida pela Figura 6.

Método	*Probabilidade*	*Erro % não-absoluto*
Evento Raro	*2,785E-09*	*-0,5*
Proposto	*2,776E-09*	*-0,2*
Exato	*2,769E-09*	*-*

Note-se que a discrepância entre o método proposto e o do evento raro em relação à inferência exata aumenta sensivelmente à medida que as probabilidades dos eventos básicos crescem. Na Tabela 5, exibe-se os erros percentuais da avaliação da árvore exibida na Figura **10** sob incrementos nas probabilidades de ocorrência dos eventos básicos envolvidos. Foram avaliados os resultados com as probabilidades exibidas na Tabela 3 multiplicadas por 10 e 20. Em ambos os casos pode-se aplicar o método de aproximação do evento raro, já que tem-se como corte mínimo mais provável $D \cap I \cap A \cap N$, com probabilidades 1,35E-05 e 2,16E-04, para o primeiro e o segundo casos respectivamente.

Tabela 5 – Erro percentual dos métodos de aproximação apresentados diante da árvore exibida pela Figura 6 com probabilidades dos eventos básicos incrementadas.

	10•valores da Tabela 3		*20•valores da Tabela 3*	
Método	*Probabilidade*	*Erro % não-absoluto*	*Probabilidade*	*Erro % não-absoluto*
Evento Raro	*5,320E-05*	*-12,6*	*1,521E-03*	*-39,2*
Proposto	*4,838E-05*	*-2,4*	*1,143E-03*	*-4,6*
Exato	*4,724E-05*	*-*	*1,093E-03*	*-*

8. Conclusões

Neste artigo propôs-se uma maneira alternativa de se realizar inferências sobre a confiabilidade de sistemas através da análise de árvores de falhas. Pôde-se ver que, mesmo dedutivamente, o desafio de sua aplicação consiste na retirada de redundâncias, o qual pode ser considerado superável, embora seja ainda alvo de estudos (seção 4).

O procedimento recursivo para o cálculo da probabilidade de ocorrência de cada evento postulado (seção 6) mostra-se simples e pode ser aplicado durante a obtenção dos cortes mínimos da árvore, gerando um esforço computacional próximo ao desprezível. Deve-se enfatizar também que caso a estrutura analisada não possua redundâncias de geração III e elevada, o método proposto permite inferências exatas.

Buscou-se demonstrar analiticamente (seção 6) e através de exemplos (seções 6 e 7) que o método proposto oferece melhores inferências quando comparado a técnicas convencionais e não requer qualquer condição para as probabilidades de ocorrência dos cortes mínimos, limitação de métodos de aproximação tais como o do evento raro e o de exclusão de cortes

pouco prováveis. Demonstrou-se (seção 6), também, que apenas após a remoção de redundâncias garante-se uma cota inferior para a confiabilidade, o que evidencia sua necessidade.

Quanto às deficiências da técnica proposta ressalte-se a necessidade de aprimoramento dos métodos de remoção de redundâncias e o não tratamento de árvores de falhas incoerentes, sendo estes fontes de pesquisa atualmente.

Referências Bibliográficas

(1) Barlett, L.M. & Andrews, J.D. (1999). Efficient Basic Event Ordering Schemes for Fault Tree Analysis. *Quality and Reliability Engineering International*, **15**, 95-101.

(2) Bedford, T. & Cooke, R. (2001). *Probabilistic Risk Analysis: Foundations and Methods.* Cambridge University Press, Cambridge.

(3) Bryant, R.E. (1992). Symbolic Boolean Manipulation with Ordered Binary-Decision Diagrams. *ACM Computing Surveys*, **24**(3), 293-318.

(4) Dutuit, Y. & Rauzy, A. (2001). Efficient algorithms to assess component and gate importance in fault tree analysis. *Reliability Engineering and System Safety*, **72**, 213-222.

(5) Firmino, P.R. & Droguett, E.L. (2004). *Redes bayesianas para a parametrização da confiabilidade em sistemas complexos.* Engenharia de Produção, Universidade Federal de Pernambuco, Centro de Tecnologia e Geociências.

(6) Firmino, P.R.; Moreira, P.I.; Chikushi, R.T. & Droguett, E.L. (2004). Métodos para a remoção de redundâncias de árvores de falhas. *Revista Produção Online*, **04**, 1782-1787.

(7) Hauptmanns, U. (2002). Analytical propagation of uncertainties through fault trees. *Reliability Engineering & System Safety*, **76**, 327-329.

(8) Heger, A.S.; Bhat, J.K.; Stack, Q.W. & Talbott, D.V. (1995). Calculating exact top-event probabilities using $\sum\prod$-Patrec. *Reliability Engineering & System Safety*, **50**, 253-259.

(9) Jung, W.S.; Han, S.H. & Há, J. (2004). A fast BDD algorithm for large coherent fault trees analysis. *Reliability Engineering and System Safety*, **83**, 369-374.

(10) Mazumdar, M. (1982). An approximate method for computation of probability intervals for the top-event probability of fault trees. *Nuclear Engineering and Design*, **71**, 45-50.

(11) Modarres, M.; Kaminskiy, M. & Krivtsov, V. (1999). *Reliability engineering and risk analyses*. Marel Dekker, New York.

(12) Rauzy, A. (1993)-New algorithms for fault trees analysis. *Reliability Engineering & System Safety*, **40**, 203-211.

(13) Reay, K.A. & Andrews, J.D. (2002). A fault tree analysis strategy using binary decision diagrams. *Reliability Engineering and System Safety*, **78**, 45-56.

(14) Swaminathan, S. & Smidts, C. (1999). The mathematical formulation for the event sequence diagram framework. *Reliability Engineering and System Safety*, **65**, 103-118.

(15) Wegner, I. (2004). BDDs-design, analysis, complexity, and applications. *Discrete Applied Mathematics*, **138**, 229-251.