

# 动态故障树的边值多值决策图分析<sup>①</sup>

李 莉, 刘翠杰, 王 政, 任逸飞

(北京电子科技学院 电子信息工程系, 北京 100070)

通讯作者: 李 莉, E-mail: [laury\\_li@126.com](mailto:laury_li@126.com)

**摘 要:** 动态故障树分析对于复杂系统来说是一种重要的可靠性分析技术, 但是二叉决策图等传统模块化方法存在严重的状态空间爆炸问题. 本文系统介绍了边值决策图的动态故障树分析方法, 其中边值多值决策图相对于其它现有的决策图具有更紧凑的表示函数, 通过状态数的缩减, 缩短了计算时间, 有效缓解状态空间爆炸问题. 实例证明了边值多值决策图在多状态系统和多功能系统中使用的方法和优势.

**关键词:** 边值多值决策图; 多值决策图; 故障树分析

引用格式: 李莉, 刘翠杰, 王政, 任逸飞. 动态故障树的边值多值决策图分析. 计算机系统应用, 2018, 27(12): 123-128. <http://www.c-s-a.org.cn/1003-3254/6632.html>

## Analysis of Edge-Value Multiple-Valued Decision Diagrams of Dynamic Fault Tree

LI Li, LIU Cui-Jie, WANG Zheng, REN Yi-Fei

(Department of Electronic and Information Engineering, Beijing Electronics Science and Technology Institute, Beijing 100070, China)

**Abstract:** Dynamic fault tree analysis is an important reliability analysis technique for complex systems. However, there are serious state space explosion problems in traditional modular methods such as binary decision diagrams. This paper systematically introduces a dynamic fault tree analysis method of edge-value decision diagram, in which the Edge-Value Multiple-valued Decision Diagram (EVMDD) has a more compact representation function than other existing decision diagrams. By reducing the number of states, the computation time is shortened and the state space explosion problem can be effectively alleviated. The example demonstrates the method and advantage of EVMDD for multi-state systems and multi-functional systems.

**Key words:** Edge-Value Multiple-valued Decision Diagram (EVMDD); multiple-valued decision diagrams; fault tree analysis

### 1 引言

随着信息时代的进步, 科学技术尤其是电子技术、计算机技术的飞速发展, 各种系统及设备的性能大大提高, 其结构也变得越来越复杂, 导致系统呈现出多种失效模式, 给系统的可靠性分析带来了新的问题.

故障树分析方法 (Fault Tree Analysis, FTA) 在六十年代初由美国贝尔研究所提出, 并用于民兵导弹的控制系统设计, 为预测导弹发射的随机失效概率做出

了贡献. 目前, FTA 已广泛应用于电子、电力、化工、机械、交通乃至土木建筑领域的关键系统定量或定性失效分析中. FTA 通过分析系统潜在的薄弱环节, 建立故障树模型, 为那些能够导致系统失效的事件组合提供了数学和图表的表达方法. 但随着容错系统的大量应用, 动态逻辑门的引入, 传统的基于最小割集 (Minimal Cut Set, MCS) 的故障树可靠性理论和方法必须加以修正才能全面描述和反映动态故障树的特

<sup>①</sup> 基金项目: 北京市自然科学基金 (4152048)

Foundation item: Natural science Foundation of Beijing Municipality (4152048)

收稿时间: 2018-04-03; 修改时间: 2018-04-24; 采用时间: 2018-05-08; csa 在线出版时间: 2018-12-03

性<sup>[1,2]</sup>. 越来越多的系统, 例如计算机服务器系统、电信系统、水、气以及配电系统等都要求有容错功能, 即在发生故障时, 这些系统仍保持在可接受的或性能下降一级开展工作. 近年来, 人们逐渐将决策图引入故障树分析和复杂系统容错功能的分析与设计中<sup>[3,4]</sup>.

本文通过对边值多值决策图和其相关决策图的介绍, 以及边值多值决策图在动态故障树分析中的应用, 对边值多值决策图进行了全面深入的分析阐述. 本文组织结构如下: 第2节介绍了二叉决策图、多比特函数二叉决策图和多比特边值二叉决策图的基本知识并列出了实例进行分析; 第3节通过具体实例对多值函数、多值决策图和边值多值决策图进行了介绍; 第4节以网络计算系统为例说明了边值多值决策图在动态故障树分析中的应用, 并分析了其性能; 第5节对边值多值决策图进行了总结.

## 2 边值二叉决策图

### 2.1 二叉决策图

二叉决策图(Binary Decision Diagram, BDD)采用有向无环图表示从 $\{0,1\}^n$ 到 $\{0,1\}$ 映射的布尔函数 $f(x_1, x_2, \dots, x_n)$ <sup>[5-9]</sup>.

二叉决策图可以根据香农展开定理, 对布尔函数 $f(x_1, x_2, \dots, x_n)$ 中的变量逐次进行香农展开获得: 根节点表示布尔函数 $f(x_1, x_2, \dots, x_n)$ 自身, 从根节点引出两个分支, 分别表示某个变量 $x_i$ 取0和1值时进行第一次香农展开后的布尔函数 $f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)$ 和 $f(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n)$ ; 布尔函数 $f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)$ 和 $f(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n)$ 可进一步进行香农展开, 并将它们和各自的0-分量和1-分量连接; 直至所有的变量均展开后得到最后的函数结果0或1, 获得布尔函数的二叉决策图表示<sup>[5]</sup>. 也可以直观的采用布尔函数的真值表获得二叉决策图.

例如: 对于布尔函数 $f = (x_1 + x_2) \times x_3$

二叉决策图(b)中0、1两个终节点分别代表 $f$ 的0和1两个取值;  $x_i$ 下方的两条分支分别表示 $x_i$ 取值为0的0-边和 $x_i$ 取值为1的1-边.

二叉决策图适用于具有两个对立状态的系统性能的判断<sup>[10]</sup>. 例如图1中的终点0和1分别表示系统无故障和有故障.

### 2.2 多比特函数二叉决策图

多比特函数二叉决策图是对二叉决策功能的扩展, 多比特函数的每个变量由多位二进制数表示, 而布尔

函数的每个变量都是用一位二进制数来表示. 下面对多比特函数的二叉决策图进行举例说明.

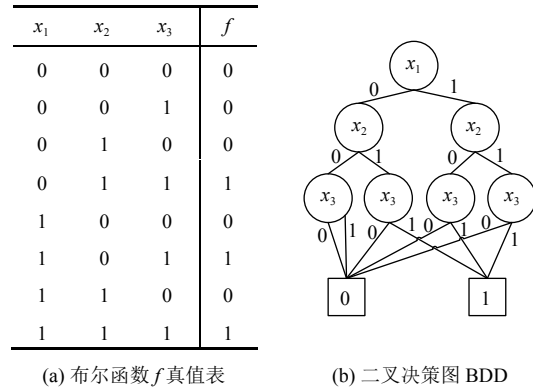


图1 布尔函数 $f$ 和 $f$ 的二叉决策图

表1(a)为 $\sin X$ 函数值表, 假设我们选择3 bit的二进制数来表示 $X$ 和 $\sin X$ , 则取递增单位为 $1/2^3=0.125$ , 采用就近取整原则, 可得二值化后的函数如表1(b)所示.

(a) $\sin X$ 函数		(b) $\sin X$ 二值化	
$X$	$\sin X$	$X$	$f(x)$
0.000	0.000	000	000
0.125	0.125	001	001
0.250	0.247	010	010
0.375	0.366	011	011
0.500	0.479	100	100
0.625	0.585	101	101
0.750	0.682	110	101
0.875	0.768	111	110

表1(b)的二叉决策图如图2所示. 节点 $X_0$ 、 $X_1$ 和 $X_2$ 分别表示变量 $X$ 的3个bit位,  $X_0$ 是最低位,  $X_2$ 是最高位. 虚线边表示 $X_i$ 的0-边, 即 $X_i$ 取值为0; 实线边表示 $X_i$ 的1-边, 即 $X_i$ 取值为1. 终节点表示函数的输出结果.

多比特函数的输出结果是由多位二进制数表示<sup>[11]</sup>, 即有多种输出结果. 多比特函数二叉决策图适用于对多状态且每个系统组件只有两个状态的系统进行表示. 例如图2中的7个终节点对应系统的7种不同运行状态, 而系统内各组件只有0和1两个状态, 对应组件的有故障和无故障状态.

### 2.3 多比特函数边值二叉决策图

边值二叉决策图(Edge-Value Binary Decision Diagram, EVBDD)是BDD的变体, 表示整数值函数. EVBDD仅由一个表示0的终节点和具有整数权重边

的内部节点组成. EVBDD 边值求解规则如下:

(1) 所有节点 0-边总是具有零权重, 即 0-边的边值为 0.

(2) 节点 1-边的边值为当其子节点取值为 0 且其它节点取值相同, 该节点取值为 1 时的函数值与取值为 0 时的函数值之差. 即节点  $x_i$  的 1-边的边值  $e$  为:

$$e = f(x_1, \dots, x_{i-1}, 1, 0, x_{n+2}, \dots, x_n) - f(x_1, \dots, x_{i-1}, 0, 0, x_{n+2}, \dots, x_n)$$

根据边值求解规则, 图 2 的边值二叉决策图如图 3.

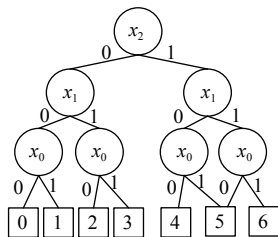


图 2 二叉决策图 BDD

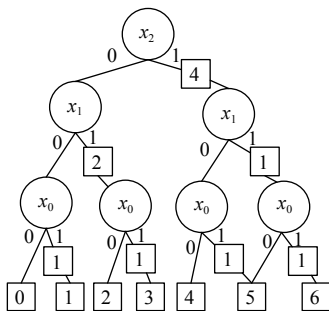


图 3 sinX 的边值二叉决策图 EVBDD

边值相加即可得到函数的最终输出结果. 例如  $x_2$  1-边的边值, 可以用  $x_2x_1x_0=100$  时的输出 100 减去  $x_2x_1x_0=000$  的输出 000, 结果等于 4, 即  $x_2$  的 1-边的边值为 4.

为便于系统状态的计算, 可以对边值二叉决策图进行缩减, 去掉冗余节点, 简化搜索路径. 冗余节点的定义如下: 若边值二叉决策图的两个或两个以上同名节点的 0-边或 1-边均指向相同的分支子节点, 或均指向终节点, 且 1-边的边值相同, 则此同名节点存在冗余. 缩减规则:

(1) 对边值二叉决策图由下至上进行递归判断, 判断是否存在冗余节点;

(2) 对存在冗余的同名节点, 保留一个节点即可, 直至边值二叉决策图中不再存有冗余节点.

缩减后的二叉决策图的函数输出结果由边值的和计算获得, 所以终节点由 0 来表示<sup>[1]</sup>. 图 3 的缩减边值二叉决策图如图 4 所示. 图 3 中四个  $x_0$  的 1-边的边值完全相同, 且均指向终节点, 所以可以删除其它三个  $x_0$  节点.

多比特函数边值二叉决策图的应用类似于多比特二叉决策图, 区别在于系统最终状态由边值的和来表示.

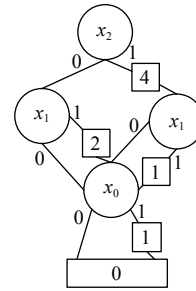


图 4 缩减后的边值二叉决策图 EVBDD

### 3 边值多值决策图

#### 3.1 多值决策图

如前所述, 当系统的状态多于 2 个时, 我们称系统为多态系统. 若系统中的各个组件也具有多个状态时, 我们称系统为具有多状态组件的多态系统, 简称为多态系统. 文献[3]指出多态系统的性能、容量或系统的状态可靠性级别都可以用系统的状态来表示.

多态系统的状态仅仅依赖系统组件的状态. 含有  $n$  个组件的系统可以被认为是一个多值函数  $f(x_1, x_2, \dots, x_n)$  的映射:  $R_1 \times R_2 \times \dots \times R_n \rightarrow M$ , 其中每一个  $x_i$  代表  $R_i$  状态的一个元组,  $R_i = \{0, 1, \dots, r_{i-1}\}$  是组件的状态集,  $M = \{0, 1, \dots, m-1\}$  表示系统的状态集. 此时多值函数被称为多态系统的结构函数. 在许多应用中, 一个系统的状态及其组件是完全有序的, 并且该系统组件的运行状态会影响整个系统的运行状态. 因此, 通过以升序的方式将值分配给每个状态, 结构函数通常会变成单调递增函数. 即多值函数  $f(x_1, x_2, \dots, x_n)$  当且仅当对于任意的  $x_i$  是单调递增函数, 即,

$$f(x_1, x_2, \dots, x_{i-1}, \alpha, x_{i+1}, \dots, x_n) \leq f(x_1, x_2, \dots, x_{i-1}, \beta, x_{i+1}, \dots, x_n) \\ \alpha, \beta \in R_i, \text{ 且 } \alpha \leq \beta.$$

可以定义当  $x_i$  取值为 0 时, 为组件的最坏状态即组件完全故障, 当  $x_i$  取值为  $r_{i-1}$  时, 为组件的最佳状态即组件完全无故障; 当  $f$  的值为 0 时, 为系统的最坏状态即系统完全故障, 当  $f$  的值为  $m-1$  时, 为系统的最佳

状态即系统完全无故障. 随着组件状态值的增加, 系统的状态值也增加, 即组件的故障越少, 系统的故障就越少, 运行状态就越好.

多值决策图 (Multiple-valued Decision Diagrams, MDD) 是反映部件状态与系统状态之间关系的有向无环图. MDD 的获得与 BDD 的获得类似, 通过香农展开定理, 重复应用于多值函数的各个组件获得. MDD 的内部节点表示通过向某些组件赋值从而获得的  $f$  的子函数, 每个内部节点具有对应于组件值的多个输出边<sup>[3]</sup>. 例如对于多值函数

$$f_0(x_1, x_2, x_3) = x_1 + x_2 + 2x_3, \\ x_1(0, 1, 2), x_2(0, 1, 2), x_3(0, 1).$$

$$f = \begin{cases} 0, f_0 = 0 \\ 1, f_0 \in [1, 2] \\ 2, f_0 \in [3, 4] \\ 3, f_0 \in [5, 6] \end{cases}$$

由以上的多值函数  $f$  得到的取值表如表 2 所示, 图 5 为其决策图, 图中的终节点 0, 1, 2, 3 分别表示多值函数  $f$  的取值.

表 2 多值函数  $f$  的取值表

$x_1$	$x_2$	$x_3$	$f$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	2
0	2	0	1
0	2	1	2
...	...	...	...
2	2	1	3

### 3.2 边值多值决策图

边值多值决策图 (Edge-Value Multiple-valued Decision Diagram, EVMDD) 是多值决策图的扩展, 它包括表示 0 的一个终节点和具有整数权重边值的内部节点; 0-边总是具有零权重. 在 EVMDD 中, 函数值被表示为从根节点遍历到终节点的边值的和<sup>[3,12,13]</sup>.

以图 5 为例, 使用与边值二叉决策图相同的边值求解和缩减规则得到的多值函数  $f$  的边值多值决策图如图 6 所示. 因为  $x_2$  的分支子节点  $x_3$  1-边的边值完全相同, 所以可以合并.  $x_1$  的 0-边的分支子节点  $x_2$  和 2-边的分支子节点  $x_2$  的边值相同, 所以进行合并.  $x_1$  的 1-边分支子节点  $x_2$  与其它边的分支子节点  $x_2$  的边值不相同, 所以不能缩减.

经过比较, 发现 MDD 有 7 个节点, 而 EVMDD 只

有 4 个节点, 减少了 3/7. 文献[3]中提到计算的时间复杂度与决策图中的节点数量成正比, 所以在计算的时间复杂度方面, EVMDD 比 MDD 更有优势.

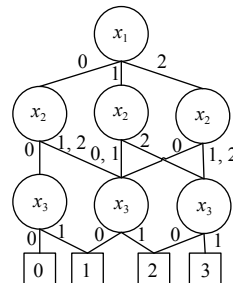


图 5 多值函数  $f$  的 MDD

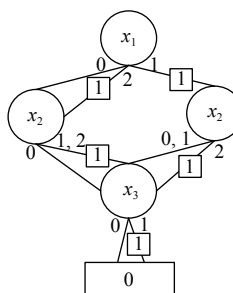


图 6 多值函数  $f$  的 EVMDD

## 4 案例研究

### 4.1 高度可靠的网络计算系统

以文献[14]中提到的高度可靠的网络计算系统为例, 系统架构如图 7 所示. 通过两个不同的数据进程提供网络计算服务. 系统分为两个部分, Complex A 和 Complex B. 每个子系统包含一个服务器 (SVR)、一个存储子系统 (STO) 及一个网络子系统 (NET). 存储子系统采用镜像存储方式, 包含一个存储控制器及两个存储空间. 当存储控制器故障时, 该存储控制器故障. 备用服务器 SVR\_C 作为失效备援, SVR\_C 和两个服务器 SVR\_A、SVR\_B 间采用心跳连接.

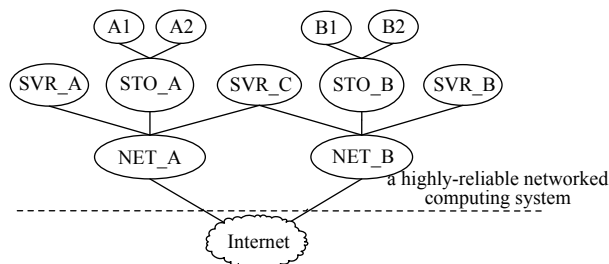


图 7 高可靠性网络计算系统



根据该系统的动态故障树 DFT 模型可以得到文献[10]中的系统性能初始 MDD, 如图 8 所示。

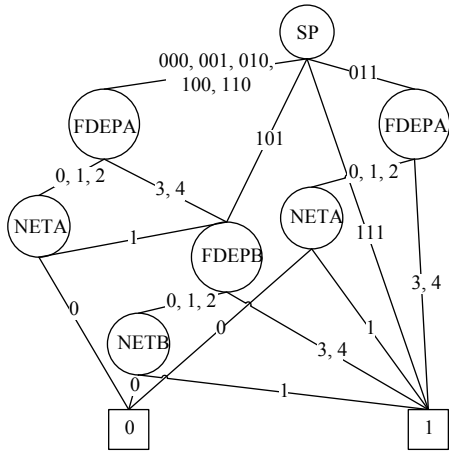


图 8 高可靠性网络计算系统的初始 MDD

下面用文中给出的边值多值决策图的构造方法来获得其 EVMDD. 将 SP 的 4 个分支分别用 0 到 3 的 4 个状态值代替. 即 000,001,010,100,110 用状态 0 代替; 101 用状态 1 代替; 111 用状态 2 代替;011 用状态 3 代替.

图 9 所示的系统动态门的 MDD, 按照本文所述的边值求解规则和缩减规则得到图 10 所示的 EVMDD.

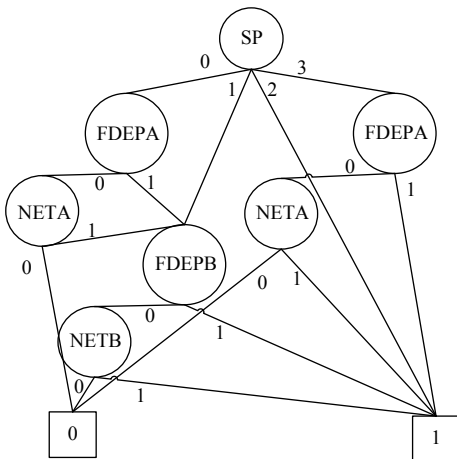


图 9 高可靠性网络计算系统动态门的 MDD

由于此系统比较简单, 所以 EVMDD 在节点和分支的数量上减少的优势没有显现. 但依据图 6 可见, 相对于 MDD 来说, EVMDD 在节点和分支的数量上都有所减少, 系统越复杂, 边值多值决策图在节点数量上的优势越明显.

### 4.2 环境检测物联网

我国空气污染形势严峻, 部分城市面临雾霾、沙尘暴等环境问题. 环保部门积极开展大气污染治理, 其核心是对污染源的精准监测和对污染数据的精准分析. 随着物联网技术的发展, 多功能、智能化、小型化的微观站监测设备得到广泛使用. 研究环境检测物联网故障树的边值多值决策图模型, 假设环境参数主要有温度、湿度和气体浓度, 分别用  $X_2$ 、 $X_1$ 、 $X_0$  来表示, 设备的最终检测状态用  $f$  来表示, 每一个参数的测量都有一个备份电路. 因此用状态 0 表示完全无故障, 状态 1 表示部分故障, 状态 2 表示完全故障. 得到多值函数  $f$  的取值表如表 3 所示, 环境监测物联网 MDD 如图 11 所示.

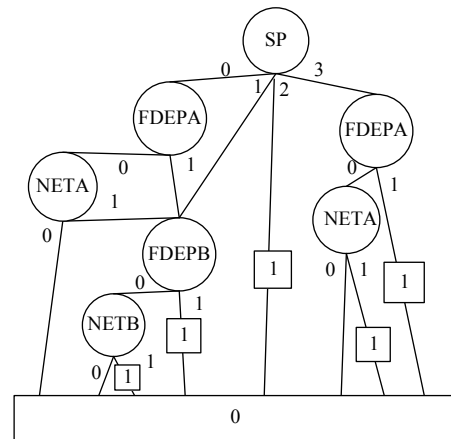


图 10 高可靠性网络计算系统动态门的 EVMDD

表 3 多值函数  $f$  的取值表

$X_2$	$X_1$	$X_0$	$f$
0	0	0	0
0	0	1	1
0	0	2	2
0	1	0	1
0	1	1	1
0	1	2	2
0	2	-	2
1	0	0	1
1	0	1	1
1	0	2	2
1	1	0	1
1	1	1	1
1	1	2	2
1	2	-	2
2	-	-	2

按照本文所述的边值求解规则和缩减规则得到如图 12 所示的环境检测物联网的 EVMDD.

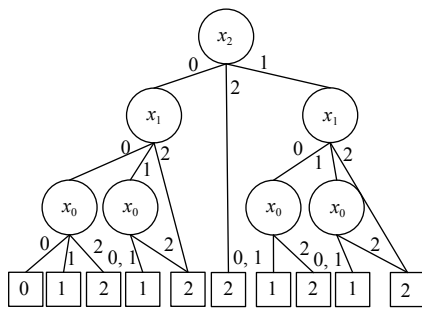


图 11 环境检测物联网的 MDD

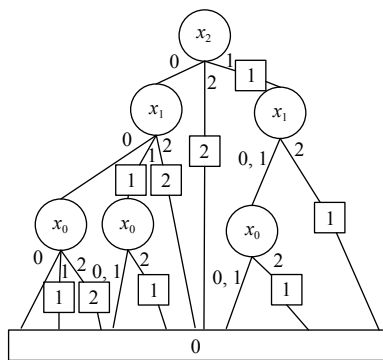


图 12 环境检测物联网的 EVMDD

通过对环境检测物联网的 MDD 和 EVMDD 的比较,用 EVMDD 用更少的节点来表示环境检测物联网.而计算的时间复杂度与决策图中的节点数量成正比,即节点数越少时间复杂度越低,因此 EVMDD 在系统的故障树分析方面更有优势.特别地,随着状态数的变大, EVMDD 的节点数远小于 MDD 的节点数.我们预计系统将在未来变得更加复杂,并且状态数将变得更大,因此, EVMDD 比 MDD 更有发展前景<sup>[15,16]</sup>.

## 5 结束语

本文对边值二叉决策图 EVBDD 和边值多值决策图 EVMDD 进行了系统的介绍和分析,特别提出了边值多值决策图在动态故障树方面的应用. EVMDD 可以更加紧凑的表示整个系统,综合运用组合方法和状态空间方法,这不仅使得状态空间爆炸问题得到缓解,也使得计算速度得到提升,可以广泛应用于现实生活中的多状态系统和多功能动态软件的性能分析等方面<sup>[17,18]</sup>.

## 参考文献

- 高顺川. 动态故障树分析方法及其实现[硕士学位论文]. 长沙: 国防科学技术大学, 2005.
- 段凌昊, 郭爱民, 潘勇. 动态故障树分析算法研究综述. 电子产品可靠性与环境试验, 2013, 31(4): 59–63. [doi: 10.3969/j.

issn.1672-5468.2013.04.014]

- Nagayama S, Sasao T, Butler JT. Analysis of multi-state systems with multi-state components using EVMDDs. Proceedings of the 42nd IEEE International Symposium on Multiple-Valued Logic. Victoria, BC, Canada. 2012. 122–127.
- 张红林, 付剑, 张春元, 等. 基于同构节点的动态故障树分析方法. 计算机工程与设计, 2011, 32(1): 1–4.
- 古天龙. 一类新型抽象数据类型: 有序二叉决策图. 桂林电子科技大学学报, 2010, 30(5): 374–388. [doi: 10.3969/j.issn.1673-808X.2010.05.002]
- 凌牧, 袁海文, 马钊, 等. 改进的动态故障树转化为二元决策图的成分组合算法与应用. 系统工程与电子技术, 2016, 38(7): 1600–1605.
- 高迎平, 李洋, 田楷. 基于有序二元决策图的动态故障树定性分析方法. 计算机与数字工程, 2016, 44(12): 2342–2347. [doi: 10.3969/j.issn.1672-9722.2016.12.012]
- 李佩昌, 袁宏杰, 兰杰, 等. 基于顺序二元决策图的动态故障树分析. 北京航空航天大学学报, 2017, 43(1): 167–175.
- 钟艳如, 黄美发, 古天龙. 装配序列生成的有序二叉决策图技术研究. 计算机集成制造系统, 2008, 14(10): 1996–2004.
- 张超. 基于 BDD 的动态故障树优化分析研究[硕士学位论文]. 西安: 西北工业大学, 2004.
- Nagayama S, Sasao T. Complexities of graph-based representations for elementary functions. IEEE Transactions on Computers, 2009, 58(1): 106–119. [doi: 10.1109/TC.2008.134]
- Doyle SA, Dugan JB. Dependability assessment using binary decision diagrams (BDDs). Proceedings of the 25th International Symposium on Fault-Tolerant Computing. Pasadena, CA, USA. 1995. 249–258.
- Nagayama S, Sasao T. On the optimization of heterogeneous MDDs. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2005, 24(11): 1645–1659. [doi: 10.1109/TCAD.2005.852290]
- 王斌, 吴丹丹, 莫毓昌, 等. 基于多值决策图的动态故障树分析方法. 计算机科学, 2016, 43(10): 70–73, 92. [doi: 10.11896/j.issn.1002-137X.2016.10.013]
- Nagayama S, Sasao T, Butler JT. A systematic design method for two-variable numeric function generators using multiple-valued decision diagrams. IEICE Transactions on Information and Systems, 2010, E93.D(8): 2059–2067. [doi: 10.1587/transinf.E93.D.2059]
- 王宁, 胡大伟. 基于多态多值决策图的多态故障树重要度计算方法. 计算机集成制造系统, 2015, 21(5): 1301–1308.
- 季会媛, 孟亚, 孙权, 等. 一种容错系统可靠性分析方法. 计算机工程与科学, 2001, 23(5): 36–38, 50. [doi: 10.3969/j.issn.1007-130X.2001.05.009]
- 冯雪, 王喜富. 基于动态故障树的计算机连锁系统可靠性及性能分析研究. 铁道学报, 2011, 33(12): 78–82. [doi: 10.3969/j.issn.1001-8360.2011.12.013]