# 概率安全评价软件 RiskA 中的非逻辑处理方法

李亚洲[1,2], 胡丽琴[1,2], 袁 润[1,2], 吴宜灿[1,2]
(1. 中国科学院 等离子体物理研究所, 安徽 合肥 230031; 2. 中国科学技术大学, 安徽 合肥 230026)

摘要: 非单调关联系统广泛存在于实际工程应用中, 传统针对单调系统的处理方法不适合于这类系统的处理。因此, 如何处理针对非单调关联系统所建立的模型成为概率安全评价软件研发面临的问题之一。本工作在调研一些国际流行概率安全评价软件非逻辑处理方法的基础上, 探讨了非逻辑求解难点, 基于 RiskA 的数据结构, 设计并实现了非逻辑处理模块, 并通过例题验证了 RiskA 软件非逻辑处理模块的正确性和可靠性。

关键词: 概率安全评价; 非逻辑; 非单调关联系统
中图分类号: TL364.1 文献标志码: A 文章编号: 1000-6931(2010)08-0969-05

# Development of Not-logic Module for Probabilistic Safety Assessment Program RiskA

LI Ya-zhou[1,2], HU Li-qin[1,2], YUAN Run[1,2], WU Yi-can[1,2]
(1. *Institute of Plasma Physics, Chinese Academy of Sciences, Hefei* 230031, *China*;
2. *University of Science and Technology of China, Hefei* 230026, *China*)

**Abstract:** With the rapid development of science and engineering, more and more non-coherent complex systems were emerged. How to evaluate probabilistic safety assessment (PSA) models of these non-coherent systems has attracted lots of the attention of the research community. Based on the survey of some commercial PSA software, the difficulty of dealing with the not-logic in the non-coherent models was brought forward in this study. Several key algorithms were proposed and had also been implemented based on the cross-linked list data structure in RiskA. The validity and reliability of RiskA's not-logic module were demonstrated by applications on many practical models.

**Key words:** probabilistic safety assessment; not-logic; non-coherent system

随着现代工业系统结构的日趋复杂, 非单 调关联系统越来越多地出现在实际工程应用

收稿日期: 2009-08-07; 修回日期: 2009-11-02
基金项目: 中国科学院知识创新重要方向项目资助(KJCX2-YW-N37, KJCX2-YW-N35); 核电项目风险监测器模型及软件系统研发资助项目(2008CCD064P)
作者简介: 李亚洲(1981—), 男, 安徽阜南人, 博士, 从事核电厂概率安全评价研究工作

中, 单调关联系统的大部分理论和方法已不适用于非单调关联系统的可靠性分析, 而且对于核能领域的概率安全评价应用, 如事件树分析、风险监测系统(RM)应用等, 非逻辑的处理有其特殊性。

FDS 团队[1-4] 自主研发的大型可靠性分析/概率安全评价软件系统 RiskA 提供了系统建模、故障树分析、事件树分析、不确定性分析、可靠性数据管理与分析、敏感性分析和重要度计算等概率安全评价所需基本功能。目前版本的 RiskA 已同时支持针对单调和非单调系统的建模和分析, 支持包括与非门、或非门、异或门、基本事件和房型事件非取值等在内的多种非逻辑的处理。

本工作首先介绍非单调关联系统处理涉及的基本概念、隐含集和质隐含集求解算法, 然后阐释 RiskA 非逻辑模块的设计思想、重要算法和实现流程, 最后通过例题验证 RiskA 软件非逻辑模块的正确性。

## 1 非单调关联系统

### 1.1 基本概念

与非单调系统相关的概念如下。

定义 1(结构函数) 设系统 $S$ 由 $n$ 个单元组成, 其状态向量为 $\boldsymbol{X}=(x_1, x_2, \cdots, x_n)\in\boldsymbol{B}^n$, 布尔函数 $\phi\in\boldsymbol{B}$ 表示系统 $S$ 状态, 若 $\boldsymbol{X}$ 与 $\phi$ 之间存在 $\boldsymbol{B}^n\rightarrow\boldsymbol{B}$ 的 1 个布尔函数 $\Phi=\Phi(\boldsymbol{X})$, 则称 $\Phi(\boldsymbol{X})$ 为系统 $S$ 的结构函数。

定义 2(单调性) 结构函数 $\Phi(\boldsymbol{X})(\boldsymbol{X}\in\boldsymbol{B}^n)$ 称为单调增加(单调减小)是指: $\forall\boldsymbol{X}_1, \boldsymbol{X}_2\in\boldsymbol{B}^n$, 若 $\boldsymbol{X}_1\leqslant\boldsymbol{X}_2$, 则有 $\Phi(\boldsymbol{X}_1)\leqslant(\Phi(\boldsymbol{X}_2)(\Phi(\boldsymbol{X}_1)\geqslant\Phi(\boldsymbol{X}_2))$。结构函数 $\Phi(\boldsymbol{X})(\boldsymbol{X}\in\boldsymbol{B}^n)$ 称为非单调是指: $\Phi(\boldsymbol{X})$ 既不是单调增加也不是单调减小的结构函数。

定义 3(关联性) 称结构函数 $\Phi(\boldsymbol{X})(\boldsymbol{X}\in\boldsymbol{B}^n)$ 与某个单元变量 $x_i$ 无关联是指: $\forall\boldsymbol{X}\in\boldsymbol{B}^n$, 有 $\Phi(\boldsymbol{X}_{x_i=0})=\Phi(\boldsymbol{X}_{x_i=1})$。

定义 4(非单调关联系统) 设 $\Phi(\boldsymbol{X})$ 为系统 $S$ 的结构函数, $S$ 为非单调关联系统是指: $\Phi(\boldsymbol{X})$ 既是非单调又是关联的结构函数。

定义 5(隐含及质隐含) 设 $\Phi(\boldsymbol{X})=\Phi(x_1, x_2, \cdots, x_n)$ 为一布尔函数, $P$ 称为 $\Phi(\boldsymbol{X})$ 的 1 个隐含(Implicant)是指: $\forall\boldsymbol{X}\in\{\boldsymbol{X}\mid P(\boldsymbol{X})=1, \boldsymbol{X}\in\boldsymbol{B}^n\}$, 有 $\Phi(\boldsymbol{X})=1$。$\Phi(\boldsymbol{X})$ 的最小隐含称为质隐含(Prime Implicant)。

### 1.2 求解算法

非单调系统故障树质隐含的求解算法主要有 Karnaugh 算法[5]、Quine 算法[6]、Nelson 算法[7]、Locks 算法[8] 和 Morreale 算法[9-10] 等。其中, Quine、Nelson、Locks 算法均为基于传统故障树求解数据结构提出的质隐含求解算法, 随着 BDD 或 ZBDD(Binary Decision Diagram 或 Zero-suppressed Binary Decision Diagram)数据结构的提出及在故障树求解中的应用[11], 1 种适合于 BDD 或 ZBDD 递归式结构的递归算法——Morreale 算法被提出。

尽管 Morreale 算法较其他算法在复杂度上有较大改进, 但对大规模模型质隐含的求解仍是 1 个难点问题。上述各种算法优缺点比较列于表 1。

表 1 常见质隐含算法优缺点

**Table 1 Comparison between different algorithms**

| 算法 | 优点 | 缺点 |
|---|---|---|
| Karnaugh | 简单直观 | 处理规模有限 |
| Quine | | 进行比较操作、对合操作和吸收操作, 效率低 |
| Nelson | | 取补之后需进行展开、吸收等运算, 效率低 |
| Locks | | 需求解 1 棵规模相当的对偶树, 计算开销大 |
| Morreale | 递归式结构, 适合 BDD 或 ZBDD | 求解的规模仍受限, 大规模故障树求解费时 |

因此, 目前多数概率安全评价软件采用的方法是不直接求解质隐含集, 而是采用 DTP(Delete Term Procedure)近似求解的方法。表 2 列出目前常用的概率安全评价软件对于非单

调系统求解方法的支持情况。从表 2 可看出, 目前一些流行的商用软件, 如 CAFTA、Risk Spectrum 和 FORTE 等, 针对非单调关联系统的求解均采取DTP 方法。由于 DTP 方法求解效率高且精度能够满足实际工程应用需求, 因此, 在RiskA设计中选用的也是 DTP 近似方法。

表 2　常用软件 DTP 和质隐含集求解支持情况

Table 2　Comparison between different software for not logic handlings

| 软件名称 | DTP 求解 | 质隐含集求解 | 质隐含求解算法 |
|---|---|---|---|
| CAFTA[12] | ✓ | | |
| Risk Spectrum[13] | ✓ | | |
| FORTE[14] | ✓ | | |
| SETS[7] | ✓ | ✓ | Nelson 算法 |
| FTAP[7] | ✓ | ✓ | Wille 算法 |
| MetaPrime[9] | ✓ | ✓ | Morreale 算法 |

## 2　设计思想

DTP 的基本思想为: 将复杂门按照特定规则进行展开, 并将非逻辑依据德摩根定律展开为基本事件非取值的情形, 再将基本事件的非取值作为 1 个新的独立基本事件参与运算, 最后对于获得结果进行后处理, 将同时包含某基本事件和该基本事件非取值的无效割集删除[8]。

概率安全评价软件中对于非逻辑的引入主要有以下 5 种基本类型: 或非门(NOR)、与非门(NAND)、异或门(XOR)、房型事件非取值和基本事件非取值。因此, 依据上述基本思想需对或非门、与非门和异或门依据一定规则进行展开。

异或门的展开规则如下。

异或门: $A \oplus B = A\overline{B} + \overline{A}B$。

或非门和与非门按照德摩根定律展开规则如下。

或非门: $\overline{A + B} = \overline{A}\,\overline{B}$;

与非门: $\overline{AB} = \overline{A} + \overline{B}$。

由于异或门展开过程中可能会出现或非门、与非门, 因此其应放在德摩根定律展开之前完成。

## 3　主要步骤

### 3.1　数据结构

RiskA 中故障树求解采用 ZBDD/MCS 算法, 为该算法设计了十字链表的存储结构[15], 定义 CNode 类来存储节点信息。图 1 示出十字链表存储示意图。

### 3.2　算法设计

基于上述 RiskA 的数据结构, 设计其计算流程如图 2 所示。

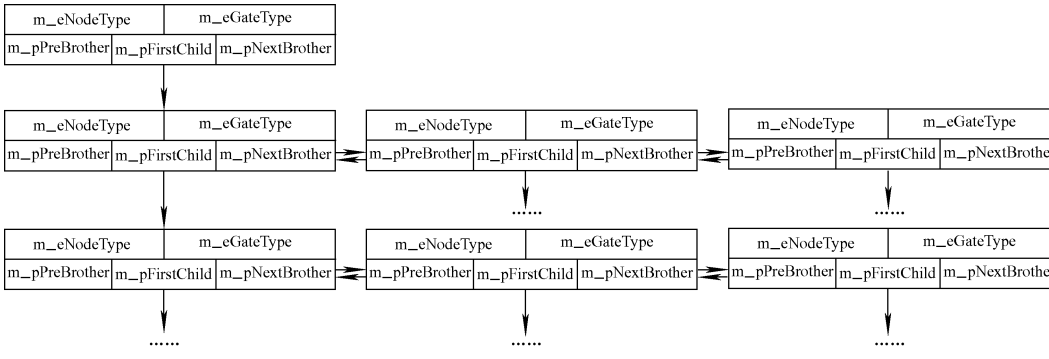


图 1　RiskA 数据结构

Fig. 1　Data structure for RiskA

图 2 中虚线所示为添加非逻辑前处理流程,实线所示为添加非逻辑后处理流程。从中可看出,较之于添加非逻辑前,添加非逻辑后的主要修改体现在复杂门移除、德摩根定律展开和最小割集后处理。其中,复杂门移除重新修改了原来的替换部分,而德摩根定律展开和最小割集后处理则为新添加的计算步序。复杂门移除的修改如图 3 所示,对于新生成的节点信息应使用哈希表进行存储,以方便计算时的调用。

德摩根定律展开和最小割集后处理两步思路清晰、步序明确,在此不再详述。

## 4 测试

针对上述流程分别从转换页展开、复杂门展开、割集计算、割集后处理等方面设计例题,对 RiskA 非逻辑处理模块正确性进行验证,同时也设计例题对事件树分析、敏感性分析、不确定性分析、重要度分析和共因分析中涉及的非逻辑进行验证。通过与商用软件计算结果的比较验证其计算的正确性。

依据计算规模选择所做测试例题中 3 棵较具有代表意义例题,测试结果列于表 3。

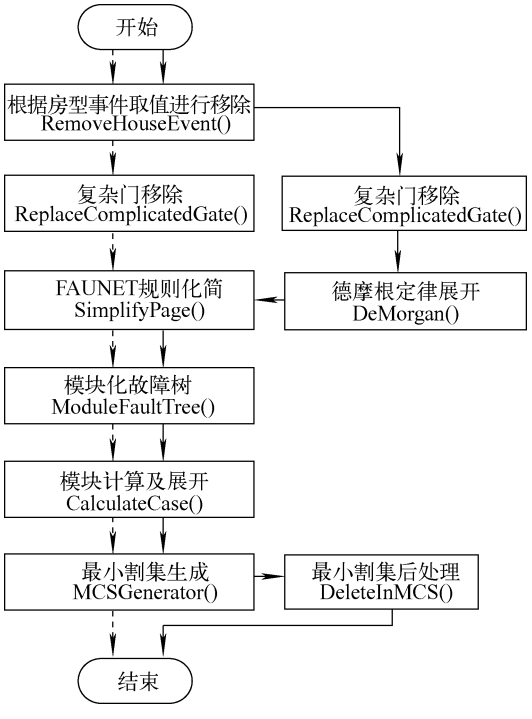


图 2 非逻辑处理流程

Fig. 2 Flow chart in RiskA's calculation

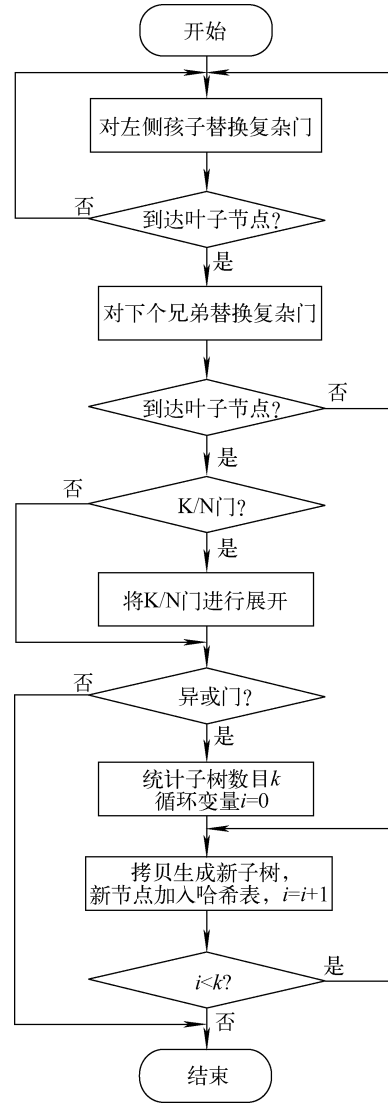


图 3 复杂门展开算法

Fig. 3 Algorithm for handling complicated gates

表 3 测试结果

**Table 3 Testing result**

| 例题名称 | 割集数目 | | 失效概率 | |
|---|---|---|---|---|
| | RiskA | 商用软件 | RiskA | 商用软件 |
| ASGP0000 | 7 373 | 7 373 | $4.11\times10^{-2}$ | $2.01\times10^{-2}$ |
| LKPP0000 | 169 | 169 | $4.95\times10^{-5}$ | $4.95\times10^{-5}$ |
| DVHP0000 | 10 026 | 10 026 | $4.71\times10^{-5}$ | $4.67\times10^{-5}$ |

从表 3 可看出,定性分析最小割集数目完全一致,经进一步对最小割集所含基本事件进行比对,两套软件定性分析结果完全吻合;定量计算结果在失效概率较大时误差较大,经进一步分析误差产生原因,认为误差主要产生于两

个方面。

1) 概率截断误差: 无论商用软件或 RiskA 在计算过程中均使用了概率截断, 但截断策略不同, 一般而言概率截断包含上近似、下近似、独立近似等, 然而对于商用软件每种近似方法究竟采用何种近似策略并不清晰。

2) 系统截尾误差: 在使用计算机中离散点表示连续数字时产生的误差。

然而, 上述误差会随所计算的失效概率的降低而减少。在核电厂概率安全评价中, 系统失效概率通常低于 $10^{-4}$ 量级, 甚至更小, 故 DTP 方法产生的误差不会影响核电厂的实际工程应用。

因此, 测试表明, RiskA 非处理模块是正确和可靠的, DTP 方法作为一种近似方法能够满足核电厂概率安全评价应用需求。

## 5 总结

传统的可靠性分析主要以单调关联系统为对象, 此类系统不含回路和反馈, 但现代科学技术的发展出现了许多非单调关联的系统结构。因此, 作为可靠性分析软件应能够处理非单调关联系统的模型。

利用 RiskA 针对 ZBDD/MCS 算法设计的十字链表存储结构的递归式特点, 设计并实现了高效的非逻辑处理算法, 使得 RiskA 能够处理的系统扩展到了非单调系统, 可处理或非门(NOR)、与非门(NAND)、异或门(XOR)、房型事件非取值和基本事件非取值等。例题测试验证了 RiskA 非逻辑处理模块的正确性和可靠性。

参考文献:


[1] 吴宜灿, 刘萍, 胡丽琴, 等. 大型集成概率安全分析软件系统的研究与发展[J]. 核科学与工程, 2007, 27(3): 270-276.
WU Yican, LIU Ping, HU Liqin, et al. Development of an integrated probabilistic safety assessment program[J]. Chinese Journal of Nuclear Science and Engineering, 2007, 27(3): 270-276(in Chinese).

[2] 刘萍, 吴宜灿. 适用于 Living PSA 的故障树求解方法[J]. 核动力工程, 2003, 24(6): 568-572.
LIU Ping, WU Yican. Fault tree analysis strategy for living PSA[J]. Nuclear Power Engineering, 2003, 24(6): 568-572(in Chinese).

[3] 李亚洲, 吴宜灿, 刘萍, 等. PSA 中不确定性分析实现方法研究[J]. 核科学与工程, 2006, 26(4): 353-357.
LI Yazhou, WU Yican, LIU Ping, et al. A low complexity method for the distributions' simulation in PSA's uncertainty analysis[J]. Chinese Journal of Nuclear Science and Engineering, 2006, 26(4): 353-357(in Chinese).

[4] 王海涛, 吴宜灿, 刘萍, 等. 概率截断对 PSA 中 RAW 重要度的影响研究[J]. 核科学与工程, 2006, 26(4): 363-367.
WANG Haitao, WU Yican, LIU Ping, et al. Study on the effect of probability truncation limit on probabilistic safety assessment RAW for importance measures[J]. Chinese Journal of Nuclear Science and Engineering, 2006, 26(4): 363-367(in Chinese).

[5] 鲍家元. 数字逻辑[M]. 北京: 高等教育出版社, 1997.

[6] QUINE W. The problem of simplifying truth functions[J]. American Mathematics Monthly, 1952, 59(8): 521-531.

[7] 周经纶. 非单调关联系统可靠性分析技术研究[D]. 北京: 国防科学技术大学可靠性研究中心, 1999.

[8] 周法清. 核电厂概率安全分析[M]. 上海: 上海交通大学出版社, 1996.

[9] COUDERT O. MetaPrime: An interactive fault-tree analyzer[J]. IEEE Transactions on Reliability, 1994, 43(1): 121-127.

[10] RAUZY A. Exact and truncated computations of prime implicants of coherent and non-coherent fault trees within Aralia[J]. Reliability Engineering and System Safety, 1997, 58(2): 127-144.

[11] RAUZY A. A brief introduction to binary decision diagrams[J]. RAIRO-APII-JESA, 1996, 30(8): 1 033-1 051.

[12] CAFTA user manual version 5.2[M]. America: EPRI and DSS, 2005.

[13] Risk Spectrum theory manual version 1.10.00[M]. Sweden: Relcon AB, 1999.

[14] FORTE user's manual version 3.0a[M]. Korea: KOPEC, 2004.

[15] 刘萍. 大型故障树分析算法研究与系统设计[D]. 北京: 中国科学院研究生院, 2007.