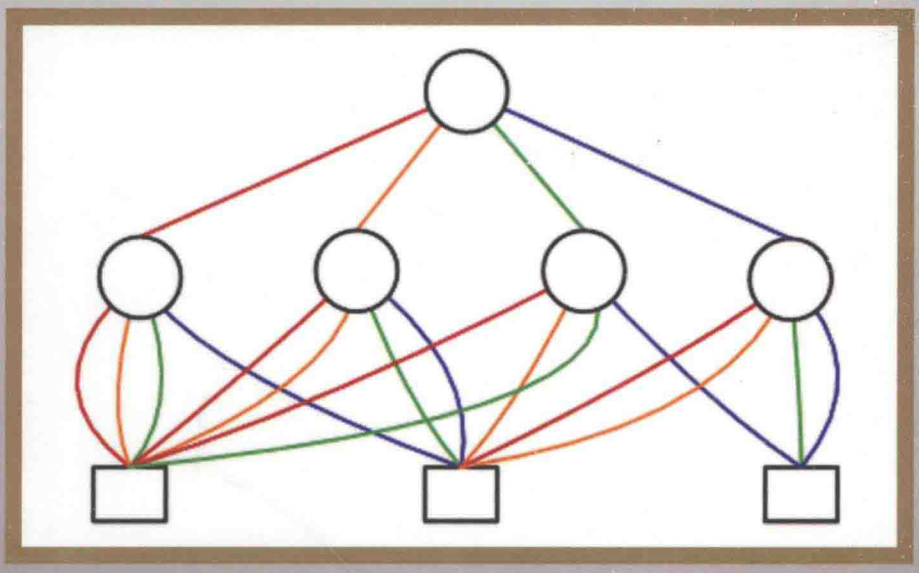
PERFORMABILITY ENGINEERING SERIES

Series Editors: Krishna B Misra and John Andrews

Binary Decision Diagrams and Extensions for System Reliability Analysis



Liudong Xing and Suprasad V. Amari

Scrivener Publishing

WILEY

Binary Decision Diagrams and Extensions for System Reliability Analysis

Liudong Xing and Suprasad V. Amari

WILEY

Co-published by John Wiley & Sons, Inc. Hoboken, New Jersey, and Scrivener Publishing LLC, Salem, Massachusetts.
Published simultaneously in Canada.

Cover design by Russell Richardson

Library of Congress Cataloging-in-Publication Data:

ISBN 978-1-118-54937-7

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Binary Decision Diagrams and Extensions for System Reliability Analysis

Scrivener Publishing
100 Cummings Center, Suite 541J
Beverly, MA 01915-6106

Performability Engineering Series

Series Editors: Krishna B. Misra (kbmisra@gmail.com)
and John Andrews (John.Andrews@nottingham.ac.uk)

Scope: A true performance of a product, or system, or service must be judged over the entire life cycle activities connected with design, manufacture, use and disposal in relation to the economics of maximization of dependability, and minimizing its impact on the environment. The concept of performability allows us to take a holistic assessment of performance and provides an aggregate attribute that reflects an entire engineering effort of a product, system, or service designer in achieving dependability and sustainability. Performance should not just be indicative of achieving quality, reliability, maintainability and safety for a product, system, or service, but achieving sustainability as well. The conventional perspective of dependability ignores the environmental impact considerations that accompany the development of products, systems, and services. However, any industrial activity in creating a product, system, or service is always associated with certain environmental impacts that follow at each phase of development. These considerations have become all the more necessary in the 21st century as the world resources continue to become scarce and the cost of materials and energy keep rising. It is not difficult to visualize that by employing the strategy of dematerialization, minimum energy and minimum waste, while maximizing the yield and developing economically viable and safe processes (clean production and clean technologies), we will create minimal adverse effect on the environment during production and disposal at the end of the life. This is basically the goal of performability engineering.

It may be observed that the above-mentioned performance attributes are interrelated and should not be considered in isolation for optimization of performance. Each book in the series should endeavor to include most, if not all, of the attributes of this web of interrelationship and have the objective to help create optimal and sustainable products, systems, and services.

Publishers at Scrivener
Martin Scrivener(martin@scrivenerpublishing.com)
Phillip Carmical (pcarmical@scrivenerpublishing.com)

To Kevin X. Zhang
and
Joseph Amari

Preface

Recent advances in science and technology have made modern engineering systems more powerful and sophisticated than ever. This decade particularly has witnessed several disruptive technological innovations in distributed and cloud computing, wireless sensor networks, internet of things, big data analytics, autonomous vehicles, space exploration that has pushed the limits of internet and mobile computing technologies beyond our imagination. The increasing level of sophistication and automation in engineering systems not only increases the complexity of these systems, but also increases the dependencies among components within these systems, and as a result, reliability analysis of these systems becomes more challenging than ever. At the same time, an accurate reliability modeling and analysis is crucial to verify whether a system has met desired reliability and availability requirements, as well as to determine optimal cost-effective design policies that maximize system reliability and/or performance.

Reliability of a system depends on reliabilities of its components and the system design configuration that includes the assembly of its components. In general, both the system and its components can have multiple failure modes and performance levels, and they can operate at different environments, stress and demand levels at different phases during their entire mission or life time. As a result, the component failure behavior and system configuration can vary with phases. In most applications, the relationship between a system and its components can be represented using combinatorial models where the system state can be represented using a logic function of its components states. This function that maps the set of component states to the system state is known as a system structure function, which is dependent on the system configuration. Once the system structure function and reliabilities of the system components are determined, traditionally the system reliability was determined using truth-tables, path-sets/cut-sets based on inclusion-exclusion expansion or sum-of-disjoint

products representation of the structure function. However, all these traditional reliability evaluation methods are computationally inefficient and are limited to small scale models or problems. To solve large models, bounding and approximating methods have been used. However, finding good bounds and approximations were still considered as a challenging problem for several decades. This situation has changed after the seminal work by Bryant on binary decision diagrams (BDD) in 1986.

BDD is the state-of-the-art data structure, which is primarily based on Shannon's decomposition theorem, used to encode and manipulate Boolean functions. The full potential for efficient algorithms based on the data structure of BDD is realized by Bryant's seminal work in 1986. Since then, BDD and its extended formats have been extensively applied in several fields including formal circuit verification and symbolic model checking. The success of BDD in these areas and the important applications of Boolean functions in system reliability analysis have stimulated considerable efforts to adapt BDD and its extended formats to reliability analysis of complex systems since 1993. These efforts have been firstly expended in reliability analysis of binary-state single-phase systems in which both the system and components exhibit only two states: operational or failed and their behaviors do not change throughout the mission. Many studies showed that in most cases, the BDD-based method requires less memory and computational time than other reliability analysis methods. Subsequently, various forms of decision diagrams have become the state-of-the-art combinatorial models for efficient reliability analysis of a wide range of complex systems, such as phased-mission systems, multi-state systems, fault-tolerant systems with imperfect fault coverage, systems with common-cause failures, and systems with functional dependent failures. These types of systems abound in safety-critical or mission-critical applications such as aerospace, circuits, power systems, medical systems, telecommunication systems, transmission systems, traffic light systems, data storage systems, and etc.

The topic of the book "Binary Decision Diagrams and Extensions for System Reliability Analysis" has gained much attention in the reliability and safety community. Several commercial reliability software vendors and research groups have started implementing these methods. Several tutorials on this topic have been presented at various international reliability and system safety conferences. The importance of this topic is also mentioned in the latest handbooks on fault tree analysis, safety and reliability analysis, and performability analysis. Research articles on this subject are continuously being published in peer-reviewed scholarly journals and conference proceedings. With the increased and sustained interest in this subject, it is a right time to bring the first book on this topic.

The purpose of this book is to provide a comprehensive coverage of binary decision diagrams and their extensions in solving complex reliability problems. In the Introduction, the book briefly describes the historical developments of BDD and its extended formats and discusses how they are related to reliability and safety applications. Chapter 2 introduces basic probability concepts that are relevant to the study of reliability, various reliability measures, and fault tree analysis. Chapter 3 discusses fundamentals of BDD including preliminaries, basic concepts, BDD construction, BDD evaluation, and existing software packages. Different strategies for variable orderings and their impact on BDD sizes are also discussed. Chapter 4 discusses the BDD-based binary-state reliability models and analysis with an emphasis on network reliability analysis, event tree analysis, failure frequency analysis, and important measures and analysis. The chapter also presents methods for modularization, non-coherent systems, and systems consisting of disjoint or dependent failures.

Chapter 5 introduces the application of BDD to the reliability analysis of phased-mission systems (PMS), in which multiple non-overlapping phases must be accomplished in sequence. During each phase, a PMS has to accomplish a specified task and may be subject to different stresses and environmental conditions as well as different reliability requirements. Thus, system structure function and component failure behavior may change from phase to phase. This dynamic behavior usually requires a distinct model for each phase of the mission in the reliability analysis. Further complicating the analysis are *s*-dependencies across the phases for a given component. For example, the state of a component at the beginning of a new phase is identical to its state at the end of the previous phase in a non-repairable PMS. This chapter explains a phase algebra-based BDD method to consider all these dynamics and dependencies in the reliability analysis of PMS.

As another application of decision diagrams in system reliability analysis, Chapter 6 explains multi-state systems (MSS), and their analysis using decision diagrams. MSSs are systems in which both the system and its components may exhibit multiple performance levels (or states) varying from perfect operation to complete failure. As compared to the analysis of binary-state systems, the unique challenge of analyzing MSSs arises from dependencies among different states of the same component, i.e., intra-component state dependencies. This chapter explains three different forms of decision diagrams to address the state dependencies in the MSS analysis: multi-state BDD (MBDD), logarithmically-encoded BDD (LBDD), and multi-state multi-valued decision diagrams (MMDD). Performances of these three methods are also discussed and compared in this chapter.

Chapter 7 presents basic concepts and types of imperfect fault coverage models and fault tolerant systems. Decision diagrams based methods are discussed for considering imperfect fault coverage in reliability analysis of binary-state systems, multi-state systems, and phased-mission systems.

Chapter 8 discusses shared decision diagrams and their advantages in storage requirement, model construction, and model evaluation. Both multi-rooted decision diagrams and multi-terminal decision diagrams are discussed. Applications of these models in solving multi-state systems, phased-mission systems and multi-state k-out-of-n systems with non-identical components are presented. This chapter also presents methods for evaluating multi-state component importance measures as well as failure frequency-based measures of multi-state systems.

Finally, Chapter 9 provides summary and conclusions on binary decision diagrams and their extensions for system reliability analysis.

The book has the following distinct features:

- It is the first book on the topic of reliability analysis using binary decision diagrams and their extensions.
- It provides basic concepts as well as detailed algorithms for reliability analysis of different types of systems using binary decision diagrams and their extended formats.
- It provides a comprehensive treatment on phased-mission systems, multi-state systems, and imperfect fault coverage models.
- It covers several system performance measures including system reliability, failure frequency, and component importance measures.
- It includes both small-scale illustrative examples and large-scale benchmark examples to demonstrate broad applications and advantages of different decision diagrams based methods for complex system reliability analysis.
- It covers recent advances in binary decision diagrams and their extensions for system reliability analysis, which lays a solid theoretical foundation for researchers to make new and further developments.
- It has more than 250 references, providing helpful and rich resources for readers to pursue further research and study of the topics.

This book provides several variable ordering schemes, variables encoding schemes, and BDD extensions for reliability and system performance

evaluation. Based on the comparisons of storage requirement, model construction, and model evaluation presented in this book, users can determine the type of decision diagrams and algorithms that can be most efficiently applied to their own problems.

The target audience of the book is reliability and safety engineers or researchers. The book can serve as a textbook on system reliability analysis. It can also serve as a tutorial and reference book on decision diagrams, multi-state systems, phased-mission systems, and imperfect fault coverage models. The book can also cover some parts of graduate level courses on data structures and algorithms.

We would like to express our sincere appreciation to Professor Krishna B. Misra and Professor John D. Andrews, editors of the Book Series on Performability Engineering, for providing us with the opportunity to include this book in the series. We are also indebted to many researchers who have developed some underlying concepts and methods of this book, or have coauthored with us on some topics of the book and provided their insights, to name a few, Professor Joanne Bechta Dugan from the University of Virginia, Professor Kishor S. Trivedi from Duke University, Dr. Gregory Levitin from The Israel Electric Corporation, Israel, Dr. Akhilesh Shrestha from ARCON Corporation, USA, Professor Yuchang Mo from Zhejiang Normal University, China, Professor Antoine Rauzy from Centrale-Supélec, France, Professor Sy-Yen Kuo from National Taiwan University, and Dr. Albert Myers from Northrop Grumman Corporation, USA. Although there are numerous other researchers to mention, we have tried to recognize their contributions in the bibliographical references of the book.

Finally it was our great pleasure to work with Martin D. Scrivener, President of Scrivener Publishing LLC, and his team who has assisted in the publication of this book. We appreciate their efforts and support.

Liudong Xing
Suprasad V. Amari
May 3, 2015

Nomenclature

AGREE	Advisory Group on Reliability of Electronic Equipment
BDD	Binary Decision Diagram
BFS	Breadth First Search
CC	Common Cause
CCE	Common Cause Event
CCF	Common Cause Failure
CCG	Common Cause Group
cdf	cumulative distribution function
CIF	Criticality Importance Factor
CIM	Composite Importance Measure
CMTBF	Cumulative Mean Time Between Failures
CPR	Combinatorial Phase Requirement
CSP	Cold SPare
CSS	Critical System State
DAG	Directed Acyclic Graph
DFLM	Depth-First-Left-Most
DFT	Dynamic Fault Tree
DFS	Depth-First Search
EDA	Efficient Decomposition and Aggregation
EDT	Expected Down Time
ELC	Element Level Coverage
ENF	Expected Number of Failures
ENS	Expected Number of Successes

ETA	Event Tree Analysis
EUT	Expected Up Time
FDEP	Functional DEPendence
FLC	Fault Level Coverage
FT	Fault Tree
FTA	Fault Tree Analysis
FTS	Fault Tolerant System
FV	Fussell-Vesely
HSP	Hot SPare
I-E	Inclusion-Exclusion
IMTBF	Instantaneous Mean Time Between Failures
IPC	ImPerfect Coverage
IPCM	ImPerfect Coverage Model
ite	if-then-else
LBDD	Logarithmically-encoded BDD
MAD	Mean Absolute Deviation
MBDD	Multistate BDD
MC	Minimal Cutset
MCNC	Microelectronics Center of North Carolina
MCS	Monte Carlo Simulation
MDD	Multiple-valued Decision Diagram
MDO	Multi-state Dependent Operation
MDT	Mean Down-Time
MFT	Multi-state Fault Tree
MFV	Multi-state Fussell-Vesely
MIPCM	Modular IPCM
MMAW	Mean Multi-state risk Achievement Worth
MMDD	Multi-state Multi-valued Decision Diagram
MMCV	Multi-state Minimal Cut Vector
MMFV	Mean MFV
MMPV	Multi-state Minimal Path Vector
MP	Minimal Pathset

MRAW	Multi-state Risk Achievement Worth
MRBD	Multi-state Reliability Block Diagram
MR-DD	Multi-Rooted Decision Diagram
MR-LBDD	Multi-Rooted LBDD
MR-MBDD	Multi-Rooted MBDD
MR-MMDD	Multi-Rooted MMDD
MRL	Mean Residual Life
MRRW	Multi-state Risk Reduction Worth
MSS	Multi-State System
MTBF	Mean Time Between Failures
MT-DD	Multi-Terminal Decision Diagram
MT-LBDD	Multi-Terminal LBDD
MT-MBDD	Multi-Terminal MBDD
MT-MMDD	Multi-Terminal MMDD
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
MUT	Mean Up Time
NDS	Network Driven Search
OBDD	Ordered BDD
PAND	Priority AND
PCCF	Probabilistic CCF
PDC	Performance Dependent Coverage
pdf	probability density function
pmf	probability mass function
PMS	Phased-Mission System
RBD	Reliability Block Diagram
ROBDD	Reduced OBDD
r.v.	random variable
SAD	Sum of Absolute Deviation
SDP	Sum of Disjoint Products
SEA	Simple and Efficient Algorithm
SEQ	SEQuence enforcing