Boolean Models and Methods in Mathematics, Computer Science, and Engineering

This collection of papers presents a series of in-depth examinations of a variety of advanced topics related to Boolean functions and expressions. The chapters are written by some of the most prominent experts in their respective fields and cover topics ranging from algebra and propositional logic to learning theory, cryptography, computational complexity, electrical engineering, and reliability theory. Beyond the diversity of the questions raised and investigated in different chapters, a remarkable feature of the collection is the common thread created by the fundamental language, concepts, models, and tools provided by Boolean theory. Many readers will be surprised to discover the countless links between seemingly remote topics discussed in various chapters of the book. This text will help them draw on such connections to further their understanding of their own scientific discipline and to explore new avenues for research.

Dr. Yves Crama is Professor of Operations Research and Production Management and former Dean of the HEC Management School of the University of Liège, Belgium. He is widely recognized as a prominent expert in the field of Boolean functions, combinatorial optimization, and operations research, and he has coauthored more than 70 papers and 3 books on these subjects. Dr. Crama is a member of the editorial board of *Discrete Optimization, Journal of Scheduling*, and *4OR – The Quarterly Journal of the Belgian, French and Italian Operations Research Societies*.

The late Peter L. Hammer (1936–2006) was a Professor of Operations Research, Mathematics, Computer Science, Management Science, and Information Systems at Rutgers University and the Director of the Rutgers University Center for Operations Research (RUTCOR). He was the founder and editor-in-chief of the journals *Annals of Operations Research, Discrete Mathematics, Discrete Applied Mathematics, Discrete Optimization*, and *Electronic Notes in Discrete Mathematics*. Dr. Hammer was the initiator of numerous pioneering investigations of the use of Boolean functions in operations research and related areas, of the theory of pseudo-Boolean functions, and of the logical analysis of data. He published more than 240 papers and 19 books on these topics.

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

The titles below, and earlier volumes in the series, are available from booksellers or from Cambridge University Press at www.cambridge.org.

100 E. Olivieri and M. Eulália Vares *Large Deviations and Metastability*
101 A. Kushner, V. Lychagin and V. Rubtsov *Contact Geometry and Nonlinear Differential Equations*
102 L. W. Beineke and R. J. Wilson (eds.) with P. J. Cameron *Topics in Algebraic Graph Theory*
103 O. J. Staffans *Well-Posed Linear Systems*
104 J. M. Lewis, S. Lakshmivarahan and S. K. Dhall *Dynamic Data Assimilation*
105 M. Lothaire *Applied Combinatorics on Words*
106 A. Markoe *Analytic Tomography*
107 P. A. Martin *Multiple Scattering*
108 R. A. Brualdi *Combinatorial Matrix Classes*
109 J. M. Borwein and J. D. Vanderwerff *Convex Functions*
110 M.-J. Lai and L. L. Schumaker *Spline Functions on Triangulations*
111 R. T. Curtis *Symmetric Generation of Groups*
112 H. Salzmann et al. *The Classical Fields*
113 S. Peszat and J. Zabczyk *Stochastic Partial Differential Equations with Lévy Noise*
114 J. Beck *Combinatorial Games*
115 L. Barreira and Y. Pesin *Nonuniform Hyperbolicity*
116 D. Z. Arov and H. Dym *J-Contractive Matrix Valued Functions and Related Topics*
117 R. Glowinski, J.-L. Lions and J. He *Exact and Approximate Controllability for Distributed Parameter Systems*
118 A. A. Borovkov and K. A. Borovkov *Asymptotic Analysis of Random Walks*
119 M. Deza and M. Dutour Sikirić *Geometry of Chemical Graphs*
120 T. Nishiura *Absolute Measurable Spaces*
121 M. Prest Purity *Spectra and Localisation*
122 S. Khrushchev *Orthogonal Polynomials and Continued Fractions*
123 H. Nagamochi and T. Ibaraki *Algorithmic Aspects of Graph Connectivity*
124 F. W. King Hilbert *Transforms I*
125 F. W. King Hilbert *Transforms II*
126 O. Calin and D.-C. Chang *Sub-Riemannian Geometry*
127 M. Grabisch et al. *Aggregation Functions*
128 L. W. Beineke and R. J. Wilson (eds.) with J. L. Gross and T. W. Tucker *Topics in Topological Graph Theory*
129 J. Berstel, D. Perrin and C. Reutenauer *Codes and Automata*
130 T. G. Faticoni *Modules over Endomorphism Rings*
131 H. Morimoto *Stochastic Control and Mathematical Modeling*
132 G. Schmidt *Relational Mathematics*
133 P. Kornerup and D. W. Matula *Finite Precision Numbers Systems and Arithmetic*

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Boolean Models and Methods in Mathematics, Computer Science, and Engineering

Edited by

YVES CRAMA
Université de Liège

PETER L. HAMMER

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town,
Singapore, São Paulo, Delhi, Mexico City

Cambridge University Press
32 Avenue of the Americas, New York, NY 10013-2473, USA

www.cambridge.org
Information on this title: www.cambridge.org/9780521847520

First published 2010
Reprinted 2012 (twice)

A catalog record for this publication is available from the British Library.

Library of Congress Cataloging in Publication Data

Boolean models and methods in mathematics, computer science, and engineering /
edited by Yves Crama, Peter L. Hammer.
p. cm. – (Encyclopedia of mathematics and its applications ; 134)
Includes bibliographical references and index.
ISBN 978-0-521-84752-0
1. Algebra, Boolean. 2. Probabilities. I. Crama, Yves, 1958–
II. Hammer, P. L., 1936– III. Title. IV. Series.
QA10.3.B658 2010
511.3´24–dc22 2010017816

ISBN 978-0-521-84752-0 Hardback

Contents

Preface

Boolean models and methods play a fundamental role in the analysis of a broad diversity of situations encountered in various branches of science.

The objective of this collection of papers is to highlight the role of Boolean theory in a number of such areas, ranging from algebra and propositional logic to learning theory, cryptography, computational complexity, electrical engineering, and reliability theory.

The chapters are written by some of the most prominent experts in their fields and are intended for advanced undergraduate or graduate students, as well as for researchers or engineers. Each chapter provides an introduction to the main questions investigated in a particular field of science, as well as an in-depth discussion of selected issues and a survey of numerous important or representative results. As such, the collection can be used in a variety of ways: some readers may simply skim some of the chapters in order to get the flavor of unfamiliar areas, whereas others may rely on them as authoritative references or as extensive surveys of fundamental results.

Beyond the diversity of the questions raised and investigated in different chapters, a remarkable feature of the collection is the presence of an "Ariane's thread" created by the common language, concepts, models, and tools of Boolean theory. Many readers will certainly be surprised to discover countless links between seemingly remote topics discussed in various chapters of the book. It is hoped that they will be able to draw on such connections to further their understanding of their own scientific disciplines and to explore new avenues for research.

The collection intends to be a useful companion and complement to the monograph by Yves Crama and Peter L. Hammer, *Boolean Functions: Theory, Algorithms, and Applications.* Cambridge University Press, Cambridge, U.K., 2010, which provides the basic concepts and theoretical background for much of the material handled here.

Cambridge University Press
978-0-521-84752-0 - Encyclopedia of Mathematics and its Applications: Boolean Models and Methods in Mathematics, Computer Science, and Engineering
Edited by Yves Crama and Peter L. Hammer
Frontmatter
More information

Introduction

The first part of the book, "Algebraic Structures," deals with compositions and decompositions of Boolean functions.

A set F of Boolean functions is called *complete* if every Boolean function is a composition of functions from F; it is a *clone* if it is composition-closed and contains all projections. In 1921, E. L. Post found a completeness criterion, that is, a necessary and sufficient condition for a set F of Boolean functions to be complete. Twenty years later, he gave a full description of the lattice of Boolean clones. Chapter 1, by Reinhard Pöschel and Ivo Rosenberg, provides an accessible and self-contained discussion of "Compositions and Clones of Boolean Functions" and of the classical results of Post.

Functional decomposition of Boolean functions was introduced in switching theory in the late 1950s. In Chapter 2, "Decomposition of Boolean Functions," Jan C. Bioch proposes a unified treatment of this topic. The chapter contains both a presentation of the main structural properties of modular decompositions and a discussion of the algorithmic aspects of decomposition.

Part II of the collection covers topics in logic, where Boolean models find their historical roots.

In Chapter 3, "Proof Theory," Alasdair Urquhart briefly describes the more important proof systems for propositional logic, including a discussion of equational calculus, of axiomatic proof systems, and of sequent calculus and resolution proofs. The author compares the relative computational efficiency of these different systems and concludes with a presentation of Haken's classical result that resolution proofs have exponential length for certain families of formulas.

The issue of the complexity of proof systems is further investigated by John Franco in Chapter 4, "Probabilistic Analysis of Satisfiability Algorithms." Central questions addressed in this chapter are: How efficient is a particular algorithm when applied to a random satisfiability instance? And what distinguishes "hard" from "easy" instances? Franco provides a thorough analysis of these questions, starting with a presentation of the basic probabilistic tools and models and covering advanced results based on a broad range of approaches.

In Chapter 5, "Optimization Methods in Logic," John Hooker shows how mathematical programming methods can be applied to the solution of Boolean inference and satisfiability problems. This line of research relies on the interpretation of the logical symbols 0 and 1 as numbers, rather than meaningless symbols. It leads both to fruitful algorithmic approaches and to the identification of tractable classes of problems.

The remainder of the book is devoted to applications of Boolean models in various fields of computer science and engineering, starting with "Learning Theory and Cryptography" in Part III.

In Chapter 6, "Probabilistic Learning and Boolean Functions," Martin Anthony explains how an unknown Boolean function can be "correctly approximated," in a probabilistic sense, when the only available information is the value of the function on a random sample of points. Questions investigated here relate to the quality of the approximation that can be attained as a function of the sample size, and to the algorithmic complexity of computing the approximating function.

A different learning model is presented by Robert H. Sloan, Balázs Szörényi, and György Turán in Chapter 7, "Learning Boolean Functions with Queries." Here, the objective is to identify the unknown function *exactly* by asking questions about it. The efficiency of learning algorithms, in this context, depends on prior information available about the properties of the target function, about the type of representation that should be computed, about the nature of the queries that can be formulated, and so forth. Also, the notion of "efficiency" can be measured either by the number of queries required by the learning algorithm (*information complexity*) or by the total of amount of computational steps required by the algorithm (*computational complexity*). The chapter provides an introduction and surveys a large variety of results along these lines.

In Chapter 8, Claude Carlet provides a very complete overview of the use of "Boolean Functions for Cryptography and Error-Correcting Codes." Both cryptography and coding theory are fundamentally concerned with the transformation of binary strings into binary strings. It is only natural, therefore, that Boolean functions constitute a basic tool and object of study in these fields. Carlet discusses quality criteria that must be satisfied by error-correcting codes and by cryptographic functions (high algebraic degree, nonlinearity, balancedness, resiliency, immunity, etc.) and explains how these criteria relate to characteristics of Boolean functions and of their representations. He introduces several remarkable classes of functions such as bent functions, resilient functions, algebraically immune functions, and symmetric functions, and he explores the properties of these classes of functions with respect to the aforementioned criteria.

In Chapter 9, "Vectorial Boolean Functions for Cryptography," Carlet extends the discussion to functions with multiple outputs. Many of the notions introduced in Chapter 8 can be naturally generalized in this extended framework: families of representations, quality criteria, and special classes of functions are introduced and analyzed in a similar fashion.

Part IV concentrates on "Graph Representations and Efficient Computation Models" for Boolean functions.

Beate Bollig, Martin Sauerhoff, Detlef Sieling, and the late Ingo Wegener discuss "Binary Decision Diagrams" (BDDs) in Chapter 10. A BDD for function f is a directed acyclic graph representation of f that allows efficient computation of the value of $f(x)$ at any point x. Different types of BDDs can be defined by placing restrictions on the underlying digraph, by allowing probabilistic choices, and so forth. Questions surveyed in Chapter 10 are, among others: What is the size of a smallest BDD representation of a given function? How can a BDD be efficiently generated? How difficult is it to solve certain problems on Boolean functions (satisfiability, minimization, etc.) when the input is represented as a BDD?

Matthias Krause and Ingo Wegener discuss a different type of graph representations in Chapter 11, "Circuit Complexity." Boolean circuits provide a convenient model for the hardware realization of Boolean functions. Krause and Wegener describe efficient circuits for simple arithmetic operations, such as addition and multiplication. Further, they investigate the possibility of realizing arbitrary functions by circuits with small size or small depth. Although lower bounds or upper bounds on these complexity measures can be derived under various assumptions on the structure of the circuit or on the properties of the function to be represented, the authors also underline the existence of many fundamental open questions on this challenging topic.

Fourier transforms are a powerful tool of classical analysis. More recently, they have also proved useful for the investigation of complex problems in discrete mathematics. In Chapter 12, "Fourier Transforms and Threshold Circuit Complexity," Jehoshua Bruck provides an introduction to the basic techniques of Fourier analysis as they apply to the investigation of Boolean functions and neural networks. He explains, in particular, how they can be used to derive bounds on the size of the weights and on the depth of Boolean circuits consisting of threshold units.

The topic of "Neural Networks and Boolean Functions" is taken up again by Martin Anthony in Chapter 13. The author focuses first on the number and on the properties of individual threshold units, which can be viewed as linear, as nonlinear, or as "delayed" (*spiking*) threshold Boolean functions. He next discusses the expressive power of feed-forward artificial neural networks made up of threshold units.

Martin Anthony considers yet another class of graph representations in Chapter 14, "Decision Lists and Related Classes of Boolean Functions." A decision list for function f can be seen as a sequence of Boolean tests, the outcome of which determines the value of the function on a given point x. Every Boolean function can be represented as a decision list. However, when the type or the number of tests involved in the list is restricted, interesting subclasses of Boolean functions arise. Anthony investigates several such restrictions. He also considers the algorithmic complexity of problems on decision lists (recognition, learning, equivalence), and he discusses various connections between threshold functions and decision lists.

The last part of the book focuses on "Applications in Engineering."

Since the 1950s, electrical engineering has provided a main impetus for the development of Boolean logic. In Chapter 15, J.-H. Roland Jiang and Tiziano Villa survey the use of Boolean methods for "Hardware Equivalence and Property Verification." A main objective, in this area of system design, is to verify that a synthesized digital circuit conforms to its intended design. The chapter introduces the reader to the problem of formal verification, examines the complexity of different versions of equivalence checking ("given two Boolean circuits, decide whether they are equivalent"), and describes approaches to this problem. For the solution of these engineering problems, the authors frequently refer to models and methods covered in earlier chapters of the book, such as satisfiability problems or binary decision diagrams.

In Chapter 16, Tiziano Villa, Robert K. Brayton, and Alberto L. Sangiovanni-Vincentelli discuss the "Synthesis of Multilevel Boolean Networks." A multilevel representation of a Boolean function is a circuit representation, similar to those considered in Chapter 11 or in Chapter 13. From the engineering viewpoint, the objective of multilevel implementations is to minimize the physical area occupied by the circuit, to reduce its depth, to improve its testability, and so on. Villa, Brayton, and Sangiovanni-Vincentelli survey efficient heuristic approaches for the solution of these hard computational problems. They describe, in particular, factoring and division procedures that can be implemented in "divide-and-conquer" algorithms for multilevel synthesis.

The combinatorial structure of operating or failed states of a complex system can be reflected through a Boolean function, called the *structure function* of the system. The probability that the system operates is then simply the probability that the structure function takes value 1. In Chapter 17, Charles J. Colbourn explores in great detail the "Boolean Aspects of Network Reliability." He reviews several exact methods for reliability computations, based either on "orthogonalization" or decomposition, or on inclusion-exclusion and domination. He also explains the intimate, though insufficiently explored, connections between Boolean models and combinatorial simplicial complexes, as they arise in deriving bounds on system reliability.

Acknowledgments

The making of this book has been a long process, and it has benefited over the years from the help and advice provided by several individuals. The editors gratefully acknowledge the contribution of these colleagues to the success of the endeavor.

First and foremost, all chapter contributors are to be thanked for the quality of the material that they have delivered, as well as for their patience and understanding during the editorial process.

Several authors have contributed to the reviewing process by cross-reading each other's work. Additional reviews, suggestions, and comments on early versions of the chapters have been kindly provided by Endre Boros, Nadia Creignou, Tibor Hegedűs, Lisa Hellerstein, Toshi Ibaraki, Jörg Keller, Michel Minoux, Rolf Möhring, Vera Pless, Gabor Rudolf, Mike Saks, Winfrid Schneeweiss, and Ewald Speckenmeyer.

Special thanks are due to Endre Boros, who provided constant encouragement and tireless advice to the editors over the gestation period of the volume. Marty Golumbic gave a decisive push to the process by bringing most contributors together in Haifa, in January 2008, on the occasion of the first meeting on "Boolean Functions: Theory, Algorithms, and Applications." Terry Hart provided the efficient administrative assistance that allowed the editors to keep track of countless mail exchanges.

Finally, I must thank my mentor, colleague, and friend, Peter L. Hammer, for helping me launch this ambitious editorial project, many years ago. Unfortunately, Peter did not live to see the outcome of our joint efforts. I am sure that he would have loved it, and that he would have been very proud of this contribution to the dissemination of Boolean models and methods.

Yves Crama
Liège, Belgium, January 2010

Contributors

Martin Anthony
Department of Mathematics
London School of Economics and Political Science, UK

Jan C. Bioch
Department of Econometrics
Erasmus University Rotterdam, The Netherlands

Beate Bollig
Department of Computer Science
Technische Universität Dortmund, Germany

Robert K. Brayton
Department of Electrical Engineering & Computer Sciences
University of California at Berkeley, USA

Jehoshua Bruck
Computation and Neural Systems and Electrical Engineering
California Institute of Technology, USA

Claude Carlet
Department of Mathematics
University of Paris 8, France

Charles J. Colbourn
Computer Science and Engineering
Arizona State University, USA

John Franco
Department of Computer Science
University of Cincinnati, USA

John Hooker
Tepper School of Business
Carnegie Mellon University, USA

J.-H. Roland Jiang
Department of Electrical Engineering
National Taiwan University, Taiwan

Matthias Krause
Theoretical Computer Science
Mannheim University, Germany

Reinhard Pöschel
Institut für Algebra
Technische Universität Dresden, Germany

Ivo Rosenberg
Département de Mathématiques et de Statistique
Université de Montréal, Canada

Alberto L. Sangiovanni-Vincentelli
Department of Electrical Engineering & Computer Sciences
University of California at Berkeley, USA

Martin Sauerhoff
Department of Computer Science
Technische Universität Dortmund, Germany

Detlef Sieling
Department of Computer Science
Technische Universität Dortmund, Germany

Robert H. Sloan
Department of Computer Science
University of Illinois at Chicago, USA

Balázs Szörényi
Hungarian Academy of Sciences
University of Szeged, Hungary

György Turán
Department of Mathematics, Statistics, and Computer Science
University of Illinois at Chicago, USA

Alasdair Urquhart
Department of Philosophy
University of Toronto, Canada

Tiziano Villa
Dipartimento d'Informatica
University of Verona, Italy

Ingo Wegener[†]
Department of Computer Science
Technische Universität Dortmund, Germany

[†]Professor Wegener passed away in November 2008.

Acronyms and Abbreviations

AB	almost bent
AIG	AND-Inverter graph
ANF	algebraic normal form
APN	almost perfect nonlinear
ATPG	Automatic Test Pattern Generation (p. 698)
BDD	binary decision diagram
BED	Boolean Expression Diagram
BMC	bounded model checking
BP	branching program
C-1-D	complete-1-distinguishability
CDMA	code division multiple access
CEC	combinational equivalence checking
CNF	conjunctive normal form
CQ	complete quadratic
CTL	computation tree logic
DD	decision diagram
DNF	disjunctive normal form
DPLL	Davis-Putnam-Logemann-Loveland
EDA	electronic design automation
FBDD	free binary decision diagram
FCSR	feedback with carry shift register
FFT	fast Fourier transform
FRAIG	Functionally Reduced AIG
FSM	finite-state machine
FSR	feedback shift register
GPS	generalized partial spread
HDL	hardware description language
HFSM	hardware finite-state machine
HSTG	hardware state transition graph
IBQ	incomplete boundary query

LFSR	linear feedback shift register
LP	linear programming
LTL	linear temporal logic
MTBDD	multiterminal binary decision diagram
NNF	numerical normal form
OBDD	ordered binary decision diagram
PAC	probably approximately correct
PBDD	partitioned binary decision diagram
PC	propagation criterion
QBF	quantified Boolean formula
ROBDD	reduced ordered binary decision diagram
RTL	register-transfer level
SAC	strict avalanche criterion
SAT	satisfiability [not an acronym]
SBS	stochastic binary system
SCC	strongly connected component
SEC	sequential equivalence checking
SEM	sample error minimization
SOP	sum-of-product
SQ	statistical query
STG	state transition graph
UBQ	unreliable boundary query
UMC	unbounded model checking
VC	Vapnik-Chervonenkis
XBDD	extended binary decision diagram

Boolean Models and Methods in Mathematics, Computer Science, and Engineering