Recent Progress in the Boolean Domain

Recent Progress in the Boolean Domain

Edited by

Bernd Steinbach

CAMBRIDGE SCHOLARS

PUBLISHING

Recent Progress in the Boolean Domain,
Edited by Bernd Steinbach

This book first published 2014

Cambridge Scholars Publishing

12 Back Chapman Street, Newcastle upon Tyne, NE6 2XX, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN (10): 1-4438-5638-X, ISBN (13): 978-1-4438-5638-6

Contents

List of Figures

List of Tables

Preface

Boolean logic and algebra are cornerstones of computing and other digital systems, and are thus fundamental to both theory and practice in Computer Science, Engineering, and many other disciplines. Understanding and developing Boolean concepts and techniques are critical in an increasingly digital world. This book presents recent progress through a variety of contributions by thirty-one authors from the international Boolean domain research community.

The first part of this book addresses exceptionally complex Boolean problems. The reader may well ask "What is an exceptionally complex Boolean problem?" The answer is that there are many and they are diverse. Some are theoretical–some are extremely practical. While every problem has its own defining features, they also have many aspects in common, most notably the huge computational challenges they can pose.

The first challenge considered is identified as the Boolean Rectangle Problem. Like many extremely complex Boolean problems, this problem is easy to state, easy to understand, and easy to tell when you have a solution. It is finding a solution that is the challenge.

The discussion of this problem takes the reader through the description of the problem, its analysis, its formulation in the Boolean domain and from there on to several solutions. While the discussion focuses on a particular problem, the reader will gain a very good general understanding of how problems of this nature can be addressed and how they can be cast into the Boolean domain in order to be solved subsequently by sophisticated and powerful tools such as the Boolean minimizer used in this instance. The discussion of the problem continues with a very insightful comparison of exact and heuristic approaches followed by a study of the role of permutation classes in solving such problems.

Building on the above, the discussion continues to show how the techniques developed in the Boolean domain can be extended to the multiple-valued domain. The presentation again focuses on a single problem, Rectangle-free Four-colored Grids, but as before, the presentation provides broad general insights. The reader is encouraged to consider which techniques transfer easily from the Boolean to the multiple-valued domain and where novel ideas must be injected. The discussion is interesting both in terms of how to approach solving the problem at hand and similar problems, and also as an illustration of the use of modern SAT-solvers. Satisfiability (SAT) is a central concept in the theoretical analysis of computation, and it is of great interest and value to see the application of a SAT-solver as a powerful tool for solving an extremely complex Boolean problem. The reader will benefit greatly from this demonstration of another powerful solution technique.

The contribution on Perception in Learning Boolean Concepts approaches the issue of complexity from a very different point of view. Rather than considering complexity in the mathematical or computational sense, the work examines complexity, complexity of Boolean concepts in particular, through consideration of a human concept of learning and understanding. This alternate view provides a very different insight into the understanding of the Boolean domain and will aid readers in broadening their conceptual understanding of the Boolean domain.

The use of logic in computation is a broad area with many diverse approaches and viewpoints. This is demonstrated in the presentation on Generalized Complexity of $\mathcal{ALC}$ Subsumption. The discussion considers a variety of concepts from a rather theoretical point of view but also points to the practical implications of those concepts. It also presents yet another view of an extremely complex Boolean problem in terms of algorithmic constructions for the subsumption problem.

The final presentation on exceptionally complex Boolean problems considers encryption and cryptanalysis. The discussion is of considerable interest due to the obvious practical importance of the problem. Readers, even those familiar with state-of-the-art encryption methods, will benefit from the presentation on the concept of algebraic immunity and its computation. The approach presented is also of considerable interest in its use of a reconfigurable computer. The reader should consider this approach as another tool in the computational toolbox for the Boolean domain.

The second part of this book begins with a discussion of low-power CMOS design. CMOS is currently the dominant technology for digital systems and this contribution is of particular significance given the ever-growing demand for low-power devices. After an overview of CMOS design, a number of techniques for power reduction are described. This discussion ends with the key question, "how low can power go?" – an interesting query on its own and also a perfect lead into the discussion of reversibility in the final part of the book.

Designing and testing of digital devices and systems have for a long time been a major motivation for research in the Boolean domain. The combinational logic design contributions in this book treat a variety of topics: the shape of binary decision diagrams; polynomial expansion of symmetric Boolean functions; and the issue of dealing with the don't-care assignment problem for incompletely specified Boolean functions. The final logic design contribution concerns state machine decomposition of Petri nets. Individually, these contributions provide insight and techniques specific to the particular problem at hand. Collectively they show the breadth of issues still open in this area as well as the connection of theoretical and practical concepts.

Testing is the subject of the next two contributions. The first concerns Boolean fault diagnosis with structurally synthesized BDDs. This contribution shows how binary decision diagrams, which are used in quite different contexts in earlier parts of the book, can be adapted to address a significantly different problem in a unique way. The second testing contribution considers techniques in a built-in self-test. After reviewing spectral techniques for testing, the discussion centers upon testing of polynomials by linear checks. The reader will gain an appreciation of the relationship between the spectral and the Boolean domains and how fairly formal techniques in the first domain are applied to a very practical application in the second.

The final part of this book addresses topics concerning the connection between two important emerging technologies: reversible and quantum logic circuits. A reversible logic circuit is one where there is a one-to-one correspondence between the input and output patterns, hence the function performed by the circuit is invertible. A major motivation for the study of reversible circuits is that they potentially lead to low power consumption. In addition, the study of reversible circuits has intensified because of the intrinsic connection of quantum computation to the gate model.

The transformations performed by quantum gates are defined by unitary matrices and are thus by definition reversible. Reversible Boolean functions are also central components of many quantum computation algorithms. This part of the book provides novel ideas and is also a very good basis for understanding the challenging problem of synthesizing and optimizing quantum gate realizations of reversible functions.

The part begins with a detailed study of the computational power of a gate referred to as the square root of NOT since two such gates in succession realize the conventional Boolean NOT gate. In addition to describing the computational power of such gates, this contribution provides a very good basis for understanding the connections and differences between reversible Boolean gates and quantum operations.

The Toffoli gate is a key building block in Boolean reversible circuits. The second contribution in this section considers the realization of Toffoli gates using controlled-`NOT` gates and the square root of `NOT` as well as the fourth root of `NOT` gates. The work extends beyond the conventional Toffoli gate to include multiple mixed positive and negative controls, and alternate control functions.

The final contribution in this part concerns the quantum realization of pairs of multi-control Toffoli gates. It builds nicely on the work in the two preceding contributions and provides the reader with valuable insight and techniques for the optimization of quantum gate realizations particularly for reversible logic.

I am confident that this book will provide novel ideas and concepts to researchers and students whether or not they are knowledgeable in modern approaches and recent progress in the Boolean domain. I am also confident that study of the work presented here will lead to further developments in Boolean problem solving and the application of such techniques in both theory and practice.

The contributions appearing in this book are extended versions of works presented at the International Workshop on Boolean Problems held at the Technische Universität Bergakademie Freiberg, Germany on September 19-21, 2012. The 2012 workshop was the tenth in a series of Boolean Problems Workshops held in Freiberg biennially since 1994. Prof. Bernd Steinbach has organized and hosted the workshop since its inception. The Boolean research community is indebted to him for this long-term contribution and for his efforts in organizing and editing this book.

D. Michael Miller

Department of Computer Science
University of Victoria
Victoria, British Columbia, Canada

Foreword

This book covers several fields in theory and practical applications where Boolean models support these solutions. Boolean variables are the simplest variables of all, because they have the smallest possible range of only two different values. In logic applications these values express the truth values *true* and *false*; in technical applications the values of signals *high* and *low* are described by Boolean variables. For simplification, the numbers 0 and 1 are most commonly used as values of Boolean variables.

The basic knowledge in the Boolean domain goes back to the English mathematician, philosopher and logician George Boole as well the American mathematician, electronic engineer, and cryptographer Claude Shannon. The initiator of the very strong increase of Boolean applications was Conrad Zuse. He recognized the benefit of Boolean values to avoid errors in large technical systems. In this way he was able to build the first computer.

The benefit of Boolean values is not restricted to computers, but can be utilized for all kinds of control systems in a wide range of applications. The invention of the transistor as a very small electronic switch and the integration of a growing number of transistors on a single chip, together with the strong decrease of the cost per transistor was the second important factor for both the substitution of existing systems by electronic ones and the extensive exploitation of new fields of applications. This development is forced by a growing community of scientists and engineers.

As part of this community, I built as an electrician control systems for machine tools, developed programs to solve Boolean equations during my studies, contributed to test software for computers as a graduate engineer, and taught students as an assistant professor for design automation. In 1992, I got a position as a full professor at the

Technische Universität Bergakademie Freiberg. Impressed by both the strong development and the challenges in the Boolean domain, I came to the conclusion that a workshop about *Boolean Problems* could be a valuable meeting point for people from all over the world which are working in different branches of the Boolean domain. Hence, I organized the first workshop in 1994 and, encouraged by the attendees, I continued the organization of the biennial series of such *International Workshops on Boolean Problems* (IWSBP).

The idea for this book goes back to Carol Koulikourdi, Commissioning Editor of Cambridge Scholars Publishing. She asked me one month before the 10th IWSBP whether I would agree to publish this book based on the proceedings of the workshop. I discussed this idea with the attendees of the 10th IWSBP and we commonly decided to prepare this book with extended versions of the best papers of the workshop. The selection of these papers was carried out based on the reviews and the evaluation of the attendees of the 10th International Workshop on Boolean Problems. Hence, there are many people which contributed directly or indirectly to this book.

I would like to thank all of them: starting with the scientists and engineers who have been working hard on Boolean problems and submitted papers about their results to the 10th IWSBP; continuing with the 23 reviewers from eleven countries; the invited speakers Prof. Raimund Ubar from the Tallinn University of Technology, Estonia, and Prof. Vincent Gaudet from the University of Waterloo, Canada; all presenters of the papers; and all attendees for their fruitful discussions the very interesting presentation on all three days of the workshop. Besides the technical program, such an international workshop requires a lot of work to organize all the necessary things. Without the support of Ms. Dr. Galina Rudolf, Ms. Karin Schüttauf, and Ms. Birgit Steffen, I would not have been able to organize this series of workshops. Hence, I would very much like to thank these three ladies for their valuable hard work very much.

Not only the authors of the sections but often larger groups contribute to the presented results. In many cases these peoples are financially supported by grants of many different organizations. Both the authors of the sections of this book and myself thank them for this significant support. The list of these organizations, the numbers of grants, and

the titles of the supported projects is so long that I must forward the interested reader to check this information to the proceedings of the 10th IWSBP [287].

I would like to emphasize that this book is a common work of many authors. Their names are directly associated to each section and additionally summarized in lexicographical order in the section *List of Authors* starting on page 413 and the *Index of Authors* on page 419. Many thanks to all of them for their excellent collaboration and high quality contributions. My special thanks goes to Prof. Michael Miller for his *Preface* which reflects the content of the whole book in a compact and clear manner, Prof. Christian Posthoff and Alison Rigg for corrections of the English text, and Matthias Werner for setting up the LaTeX-project for the book and improving the quality of the book using many LaTeX-tools.

Finally, I like to thank Ms. Carol Koulikourdi for her idea to prepare this book, the acceptance to prepare this scientific book using LaTeX, and for her very kind collaboration. I hope that all readers enjoy reading the book and find helpful suggestions for their own work in the future. It will be my pleasure to talk with many readers at one of the next International Workshops on Boolean Problems or at any other place.

Bernd Steinbach

Department of Computer Science
Technische Universität Bergakademie Freiberg
Freiberg, Saxony, Germany

Introduction

Applications of Boolean variables, Boolean operations, Boolean functions, and Boolean equations are not restricted to computers, but grow in nearly all fields of our daily life. It may be that the digitally controlled alarm-clock wakes us in the morning; we listen to the sounds of digital audio broadcasts during our breakfast; we buy the ticket for the train on a ticket vending machine controlled by Boolean values; we use our smart phones that transmit all information by Boolean values for business; look at the wrist watch which counts and shows the time based on Boolean data so that we do not miss the end of our work; we get the bill for shopping from a pay machine which calculates the sum of the prices and initiates a transmission between our bank account and the bank account of the shop; and in the evening we watch a movie on TV which is also transmitted by Boolean values. Hence, without thinking about the details, our daily life is surrounded with a growing number of devices which utilize Boolean values and operations.

Gordon E. Moore published in 1965 a paper about the trend of components in integrated circuits which double approximately every 12 to 24 months. This observation is known as Moore's Law. Of course, there are many physical limits which take effect against this law, but due to the creativity of scientists and engineers this law is valid in general even now. The exponential increase of the control elements is a strong challenge for all people working in different fields influenced by Boolean values.

The International Workshop on Boolean Problems (IWSBP) is a suitable event where people from all over the world meet each other to report new results, to discuss different Boolean problems, and to exchange new ideas. This book documents selected activities and results of the recent progress in the Boolean domain. All sections are written from authors who presented their new results at the 10th IWSBP in

September 2012 in Freiberg, Germany.

The most general challenge in the Boolean Domain originates from the exponential increase of the complexity of the Boolean systems as stated in Moore's Law. Chapter 1 of this book deals with this problem using a Boolean task of an unlimited complexity. Chapter 2 applies the found methods to a finite, but unbelievable complex multiple-valued problem of more than 10^{195} color patterns. The last open problem in this field was recently solved, too. For completeness, these results are added as Section 2.5 to this book. Basic versions of all other sections of this book are published in the proceedings of the 10th IWSBP [287].

Success in solving special tasks for applications requires a well developed theoretical basis. Chapter 3 of the book contains interesting new results which can be utilized in future applications. The design of digital circuits is the main field where solutions of Boolean problems result in real devices. Seven different topics of this field are presented in Chapter 4. Not all produced devices are free of errors, due to geometrical structures of a few nanometers on the chips. Hence, it is a big challenge to test such circuits which consist of millions of transistors as switching elements in logic gates. Chapter 5 deals with these Boolean problems. Following Moore's Law, in the near future single atoms must be used as logic gates. This very strong change of the basic paradigm from classical logic gates to reversible quantum gates requires comprehensive preparatory work of scientists and engineers. The final chapter, Chapter 6 of this book shows recent results in reversible and quantum computing.

A more detailed overview of the content of this book is given in the excellent preface by Prof. Miller. Hence, it remains to wish the readers in the name of all authors pleasure while reading this book and many new insights which are helpful to solve many future tasks.

Bernd Steinbach

Department of Computer Science
Technische Universität Bergakademie Freiberg
Freiberg, Saxony, Germany