Problems and New Solutions in the Boolean Domain

Problems and New Solutions in the Boolean Domain

Edited by

Bernd Steinbach

Cambridge
Scholars
Publishing

Problems and New Solutions in the Boolean Domain

Edited by Bernd Steinbach

This book first published 2016

Cambridge Scholars Publishing

Lady Stephenson Library, Newcastle upon Tyne, NE6 2PA, UK

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

ISBN (10): 1-4438-8947-4
ISBN (13): 978-1-4438-8947-6

Contents

List of Figures

List of Tables

Foreword

Boolean Algebra was introduced by George Boole in 1847. Originally, it was used to study the law of thought. After the invention of digital computers, Boolean Algebra has been used to design digital circuits.

Logic functions are represented by Boolean expressions or decision diagrams, and the circuits are directly represented by expressions or decision diagrams. Thus, the simplification of expressions or decision diagrams reduces the size of the circuits. In the early days, the cost of logical elements was rather high, so research on the minimization of logical representations was very important.

A Boolean expression is satisfiable (SAT) if it is possible to find an assignment that makes the expression true. Recently, efficient SAT engines have been developed, and they are used for the verification of digital systems. Since various digital systems are used in the infrastructure of our daily life such as power, communication, transportation, and bank systems, verifications of digital systems are essential. Also, SAT engines are used to solve complex combinatorial optimization problems.

Now, many engineers are working on semiconductor devices. The pace of evolution of semiconductor technology is very fast, and the cost of basic logic elements has become rather low. Thus, the reduction in circuit size is not so important as before. More important problems are to reduce power dissipation, or to increase the reliability or dependability of digital systems. Furthermore, programmability and regularity are desired.

Since fewer researchers are working in the area of Boolean logic, the speed of the research is slower than that in the device area.

I would like to mention that the editor of the book, Prof. Dr. Bernd

Steinbach has been regularly organizing the **International Workshops on Boolean Problems** since 1994. This is a unique and important workshop to exchange the ideas of Eastern and Western people in Boolean problems. His long-term service to the society should be appreciated.

Similar meetings are the International Symposium on Multiple-Valued Logic, the International Workshop on Logic and Synthesis, and the Reed-Muller Workshop.

I hope the readers can participate in these meetings and present their new research work to enhance the research in the field of Boolean logic.

Tsutomu Sasao

Meiji University, Japan
April 2016

Preface

Progress in the Boolean domain requires both an improved theory and powerful tools which utilize the new theory for practical applications. The first part of this book deals with methods, algorithms, and programs for these aims.

Technological progress extends the conventional information processing by switching circuits with alternative information processing systems that use multiple-valued, quantum, reversible, and fuzzy methods. A suggested vector space model can uniquely be applied to all these different areas. A system with n primary inputs and m primary outputs is described by a $2^n \times 2^m$ transfer matrix. A benefit of the transfer matrix is that it allows both the simulation from known inputs to unknown outputs and the justification from known outputs to unknown inputs. At first glance, the size of the transfer matrix seems to restrict the vector space model to very small systems. However, when the transfer matrix is mapped into a fitting decision diagram, experimental results confirm that the vector space model provides a practical alternative to switching algebraic solutions.

Boolean equations play a major role in the Boolean domain. They can be used to solve problems of Discrete Mathematics, not only for digital systems, but for many other problems as well. A Boolean equation is an instrument to map a Boolean function into a set of Boolean vectors and vice versa. A Boolean inequality and a system of Boolean equations can be mapped to a single Boolean equation having the same solution. The field of application is additionally extended by the possibility of solving a Boolean equation with regard to variables. It is sufficient to create correct models, as the appropriate software is available. Both the domain-specific software XBOOLE and the more specialized SAT-solvers can be used. The complexity of the problems solved by Boolean equations is already extremely high. The simple hint that a problem has exponential complexity is no longer sufficient

to leave the problem behind, without the intention of solving it.

The evaluation of expressions with millions of terms could take several months. Such expressions occur both in High Energy Physics and in the specification of Boolean problems. The simplification of such expressions can drastically reduce the time for their evaluation. Simple methods for this simplification are the utilization of Horner's rule and the common subexpression elimination. Drawbacks of these methods are eliminated by variants of the Monte Carlo Tree Search (MCTS) using Upper Confidence bounds applied to Trees (UCT). Justifications of control parameters needed in these methods can be soften by the approach of Simulated Annealing. Both the benefits and restrictions of these methods are explored by very large benchmarks of High Energy Physics. The significant improvements reached should be a reason to adjust these methods to the simplification of large Boolean expressions.

The 2^{n+1} symmetric Boolean functions of n variables are only a small part of all 2^{2^n} Boolean functions. However, due to the independence regarding the exchange of arbitrary pairs of variables, symmetric Boolean functions are preferably used in many applications, e.g., for testing or cryptography. Symmetric Boolean functions can be uniquely specified either by a set of symmetry levels or by the set of numbers that indicate how many variables occur in the conjunction of complete polynomials. The transeunt triangle method is, so far, the best method of calculating one of these sets based on the given other set and has a complexity of $O(n^2)$. A new combinatorial method will be presented that utilizes the Lucas Theorem to solve the same task. The complexity of the new method could be reduced for elementary symmetric Boolean functions to the linear complexity $O(n)$.

The exponential complexity of Boolean functions requires efficient methods for their calculation. An important approach to reach this aim is the utilization of parallel computation. Besides other concepts, XBOOLE realizes the parallel computation of 2^d binary vectors which are represented by a single ternary vector containing d dashes as well as the parallel computation of all Boolean variables which are assigned to the bits of the machine word of the computer used. Modern computers provide, in addition to the CPU, a much larger number of computing cores in the available GPUs. The new library XBOOLE-

CUDA utilizes these additional resources to increase the computation power again by approximately two orders of magnitude. Based on a practical application, that can be scaled in a very wide range, the welcome properties are explored. Programmers who want to solve Boolean problems benefit from all efforts of optimizing the special requirements of the GPU and the strongly increased computation power by the simple exchange of the XBOOLE library with the XBOOLE-CUDA library.

Due to a renewed interest in Walsh and dyadic analysis, alternative approaches for the efficient computation of Gibbs dyadic derivatives were explored. The FFT-like approach leads to a strong speedup on a GPU but is restricted to Boolean functions of not more than 25 variables. This limit can be exceeded by an adapted version of this algorithm utilizing SMTBDDs. An alternative approach based on the first row of the Gibbs matrix outperforms the calculation of the Gibbs dyadic derivatives for Boolean functions of less than 15 variables.

Basically, it can be expected that Electronic Design Automation tools generate the same results for semantically identical inputs. Experimental explorations have shown that large differences in the size of the designed circuits are caused by irrelevant changes in the input descriptions. Similar behaviors are also noticed for a tool to compress test patterns or a tool for two level minimization of a disjunctive form. Due to the complexity of the used algorithms, it is difficult to find the behavior from these tools. Using the stochastic model of the Gaussian Mixtures and the Expectation and Maximization algorithm it was possible to approximate the parameter probability density function of the evaluated tools.

Both the progress in the theory of Boolean functions and their very cost-efficient realizations as microelectronic circuits contribute to a growing number of applications. The second part of this book explores some of these practical applications of Boolean functions.

The rapid development of the internet influences both our daily life and particularly the successful cooperation in the area of scientific projects. Unfortunately the risk regarding network attacks such as computer viruses or worms increases also. Network Intrusion Detection Systems contribute to network security by checking the transmit-

ted data on network nodes. Due to the increasing number of signatures to test and the high speed of data transmission reached, the check to prevent attacks becomes the bottleneck on the internet. New, very fast hardware for regular expression matching based on systolic arrays and dual position automaton avoids this bottleneck. More than one gigabit per second can be checked at high speed using a compact hardware in which the comparison pattern can be quickly updated. For low-end Network Intrusion Detection Systems an efficient software approach based on Zero-Suppressed Binary Decision Diagrams and one-hot encoding of the relations needed will be presented.

A huge amount of data is transferred each second through the internet and this amount of data grows continuously. Cipher systems enable the encryption of a given plaintext so that the transmitted ciphertext can only be decrypted by a cipher system with the right key. Due to successful attacks against practically used cipher systems, it is a challenge to increase their security. Boolean functions with special properties become very important in the development of new cipher systems with much higher security. Different types of cipher systems as well as the necessary properties of Boolean functions for such systems are explored within a section about cryptography. The structure, behavior and possible attacks are explained. A list of topics for further research guides the scientists to the development of cipher systems of possibly even higher security.

A special problem in cryptography is the computation of a function based on information of two parties such that both parties share the result but maintain the privacy of their secret input data used by the function. Secure two-party computation protocols are the theoretical basis for such computations. The cost of this protocol is determined by the exchange of keys needed. A new type of Exclusive-OR Sums Of Products (ESOP) is suggested, called Secure Computation (SC) - ESOP. An adapted minimization algorithm may increase the total number of gates, but decreases the cost which is caused by the number of EXOR gates that are controlled by the information of both parties. The best gain for the benchmark circuits explored was about 22 percent.

Several external reasons can cause errors of one or more bits of a digital system. It is well known that additional check bits in codewords allow

the detection or even the correction of an error. This method increases the security of safety critical systems, but can also be used to increase the rate of yield of the circuits produced. A new heuristic is suggested that finds almost optimal check bits for an arbitrary error model. This heuristic was successfully applied to an error graph of 2^{19} vertices and almost 100 million edges to improve the double-bit error protection.

The probabilities of Boolean functions have a strong influence on the efforts of their implementation. Some of these properties are well indicated by the coefficients of several spectra of Boolean functions. However, due to the exponential complexity of Boolean functions, the direct computation of all spectral coefficients needed can be very time-consuming based on the truth table of the Boolean function. The exploration of the relationship between Boolean function spectra and associated circuit output probabilities opens a new way for such computations. Besides the application to the well known Shannon decomposition, operations of the Boolean Differential Calculus, and several spectral transformations are explained.

There are hard problems which require the computation of the minimal and maximal sets of given very large sets of sets. Problems in Social Choice Theory such as, e.g., finding the set of maximal transitive sets as subject to a given tournament relation, or game-theoretic problems such as, e.g., the minimal winning coalitions, belong to this class of problems. Using Reduced Ordered Binary Decision Diagrams and Quasi-Reduced Ordered Binary Decision Diagrams new algorithms were implemented in the Computer Algebra System RelView which solve such tasks significantly faster.

The properties of Boolean functions have a strong influence on their application. For instance, the most nonlinear functions, called bent functions, are used in cryptographic applications. It is a very difficult problem to compute all bent functions for a large number of variables. Additional knowledge about these functions is valuable for future research and applications. New results for multiple-valued functions having a bent Reed-Muller spectrum are presented and provide such valuable new insights.

Gordon E. Moore published in 1965 a paper about the trend that the components in integrated circuits double approximately every 12 to 24

months. This observation is known as Moore's Law. The predicted exponential increase of the performance requires permanently new ideas and contributions from scientists and engineers. The third part of this book enumerates several problems about future technologies and also presents important new results in this research area.

Reversibility is a necessary condition for quantum circuits. Therefore, this class of circuits has been intensively explored over the last two decades. Despite the substantial knowledge about reversible functions and their implementation as reversible circuits, important open problems remain. Using the repeated basic knowledge about reversible circuits, both upper and lower bounds for several classes of gates in the circuit are given. A suggested framework guides scientists to open questions in the complexity analysis of reversible circuits.

The evaluation of algorithms using available benchmark functions is a general approach in circuit design. Using the same cost function different algorithms can be compared. However, this method does not give an answer about the distance between the found solution and an optimal one. One step to close this gap is the presentation of a reversible circuit with a minimal number of multiple-control Toffoli gates and the proof of the minimality for the generalized Miller function of an arbitrary number of variables.

The Boolean values true and false of logic circuits, short bits, are replaced in quantum circuits by qubits. The values of these qubits are complex numbers and the gates to change these values are quantum gates which are described by unitary matrices. Using controlled `NEGATOR`s and controlled `PHASOR`s as quantum gates, the relationships between reversible computing and quantum computing are explained. Utilizing the properties of the unitary matrices, synthesis algorithms for quantum circuits are proposed. These algorithms decompose the given unitary matrix such that additionally to classical gates and `FOURIER` circuits either only `PHASOR` gates or only `NEGATOR` gates are necessary.

Different approaches to synthesize quantum circuits utilize several type of elementary quantum gates and transformations from reversible circuits to quantum circuits. Already the gates `NOT`, controlled-`NOT`, controlled-`V`, and controlled-$\texttt{V}^\dagger$ of the NCV library are required to

distinguish between the separable and entangled circuits. A semi-classical two-qubit gate library allows the merger of neighbored two-qubit gates in order to reduce the two-qubit cost. A restricted gate library extends the potential for improvements. The results found are applied to Linear Nearest Neighbor circuits to realize Toffoli gates.

Bernd Steinbach

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

Acknowledgments

This is the second book that summarizes the best scientific results of contributions to the International Workshop on Boolean Problems (IWSBP). In this sense it establishes a new series of books. The idea for the first 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 a book based on the proceedings of the workshop. This initial book [313] was entitled *Recent Progress in the Boolean Domain*. The interest of many people working in the Boolean domain or faced with such problems encouraged me also to prepare a book about the best results from the 11th IWSBP. Cambridge Scholars Publishing accepted my proposal for this second book within a series about problems and solutions in the Boolean domain.

Many people contributed to the origination of 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 11th IWSBP. My next thanks goes to the 28 members of the program committee from eleven countries. Based on their reviews the best papers submitted could be selected for presentation at the 11th IWSBP. Furthermore, their hints helped the authors to improve the final versions of their papers.

My special thanks goes to the invited speakers: Prof. Mitchell A. Thornton from the Southern Methodist University, Dallas, Texas, USA; Prof. Jaap van den Herik, from Leiden University, The Netherlands; and Prof. Shinobu Nagayama, Hiroshima City University, Hiroshima, Japan, as well as all presenters of the papers and all attendees for their fruitful discussions and very interesting presentations 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 parts. Without the support of Dr. Galina Rudolf, Karin Schüttauf, and Birgit Steffen, I would not have been able to organize this series of workshops. Hence, I would very much like to thank them for their valuable hard work.

Not only the authors of the sections but often larger groups contribute to the presented results. In many cases these people are financially supported by grants from 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 for this information to the proceedings of the 11th IWSBP [311]. Exemplary, we acknowledge some of these supporters here.

The research of Section 2.3 about Electronic Design Automation tools regarding their behaviors in case of similar input descriptions were supported by computational resources provided by the MetaCentrum under the program LM2010005 and the CERIT-SC under the program Centre CERIT Scientific Cloud, part of the Operational Program Research and Development for Innovations, registration number CZ.1.05/3.2.00/08.0144. We thank them for this valuable support.

The research of Section 3.1 for fast network intrusion detection systems with high maintainability is partly supported by the Ministry of Education, Culture, Sports, Science, and Technology (MEXT) of Japan as Grant-in-Aid for Scientific Research (C), (No. 25330071), and the Satake Foundation, 2014. We would like to thank Prof. Shinichi Minato, Ryutaro Kurai, Dr. Masato Inagi, Yosuke Kawanaka, Dr. Yoichi Wakaba, and Takumi Makizaki for their support of this work.

The work about functions with Bent Reed-Muller Spectra was supported by the Ministry of Education and Science of Serbia, through the project No. ON174026, and by the Foundation for the Advance of Soft Computing, Mieres, Spain.

The development of the presented results has been also supported by further scientists. We thank, e.g., Eugenia Rosu for her help to complete the proof of Theorem 5.17.

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 423 and the *Index of Authors* on page 431. Many thanks to all of them for their excellent collaboration and high quality contributions. My special thanks go to Prof. Tsutomu Sasao for his *Foreword*, Alison Rigg for corrections to the English text, and Dr. Galina Rudolf as well as M.Sc. Matthias Werner for their support improving the quality of the book using many LaTeX-tools.

Finally, I would like to thank Samuel Baker, Commissioning Editor, Victoria Carruthers, Author Liaison, and Amanda Millar, Typesetting Manager, for the fruitful collaboration in preparing this scientific book. 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