Further Improvements in the Boolean Domain

Edited by

Bernd Steinbach

Cambridge
Scholars
Publishing

Further Improvements in the Boolean Domain

Edited by Bernd Steinbach

This book first published 2018

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): 1-5275-0371-2
ISBN (13): 978-1-5275-0371-7

Foreword

Further Improvements in the Boolean Domain contains some of the latest innovations with regard to the theory and application of algebraic methods over the Boolean domain. Algebras involving the Boolean domain have been studied and used by philosophers, scientists, mathematicians, and engineers since at least the time of Aristotle's development of the syllogism. In the past century, electrical and electronic artifacts that utilize switching elements have been extensively modeled with switching algebras or binary-valued algebras due to the advent of digital computation and communication. Although many theorists and practitioners have studied and used methods in the Boolean domain, new and useful results continue to emerge as the information age continues to evolve. This useful compilation of further improvements continues this tradition.

The book is organized into three parts titled: "Extensions in Theory and Computations", "Digital Circuits", and "Towards Future Technologies". These three parts are further divided into five separate chapters that provide results in areas ranging from theoretical concerns to those that are applicable to modern design and implementation challenges such as automated synthesis and reliability. Emerging computational paradigms based upon reversible functions and quantum mechanical phenomena continue to utilize frameworks in the Boolean domain, further underscoring the need for continued improvements in this area of discrete mathematics.

The first part of the book is devoted to theory and computation. Chapter One contains several new theoretical results including the relationship of Boolean equations to problems in the class NP. A recent area of interest is the study of the class of functions known as index generation functions. New theoretical characteristics are provided for these functions that have many useful applications in data networks and memory. Approximate computing encompasses the use of func-

tions that are not precisely equivalent to those they approximate. The use of approximate functions can lead to significant efficiencies although a corresponding loss in precision accompanies their use and this topic is considered. Spectral methods have been the subject of both practical and theoretical concern for many years although new results continue to emerge and some of the latest results are provided in a survey of applications. Next, the topic of finite topologies is considered with the interesting approach of using a relational algebraic framework provided by the RelView computer algebra system. Chapter One concludes with a subsection devoted to the application of partially defined logic to the important and timely area of asynchronous circuit design.

The second Chapter of the book is concerned with accelerated computations. Performance continues to be a major concern and new results in the Boolean domain are applied to achieve performance enhancement. Bent functions are those that exhibit maximal nonlinearity and are known to have desirable characteristics when employed in certain classes of cryptographic algorithms. While bent functions are desirable to use in these circumstances, their enumeration and discovery remains a hard problem that motivates the development of new architectures for that purpose. An approach based upon FPGAs for the purpose of finding such functions is described and its effectiveness is analyzed. A second approach for generating bent functions combines a random method with GPU computational cores. Next, the subject of an arithmetic code known as the AN code is considered. AN codes are nonlinear and find their application in error detection at the hardware level. Once again, a GPU-based analysis and experimentation environment is described that allows for the computation of AN code distance distributions and SDC probabilities. The final contribution in Chapter Two considers the situation wherein associated forms of Boolean functions are often preferable to normal forms in terms of the literal count; however, the associated forms are not necessarily orthogonal. Ternary vector lists (TVLs) are presented and a means for using them to find orthogonal associated forms is provided and validated with experimental results.

The next part of the book is devoted to digital circuits and is comprised of Chapter Three which is concerned with synthesis, visualization, and benchmarks, and, Chapter Four which is concerned with

reliability and linearity.

A fundamental operation in digital circuit synthesis is that of decomposition. A particular form of decomposition, namely vectorial bi-decomposition for lattices is described in detail in the first contribution of Chapter Three. The next contribution takes a somewhat philosophical view and considers the use of visualization as a tool in hardware/software design with both a survey of present methods and predictions about the future of this area and its corresponding potential impact. The subject of complemented circuits and their role in logic synthesis is described with emphasis placed upon the minimization problem and experimental results provided to validate the approach. A large percentage of digital circuit data-paths include arithmetic circuitry with the multiplier being a common element. An approach for the design of such multipliers based upon the use of the Fourier transform is described and example multiplier designs using both regular and saturated arithmetic are provided. The state assignment problem is considered next with respect to the criterion of minimizing power dissipation. A heuristic approach to the state assignment problem for low power is provided with an accompanying example to illustrate the method. Simulation is a basic need in digital circuit design and analysis and is often used in a stand-alone manner, or in support of other digital circuit engineering tasks. Discrete event modeling is considered and a syntax is provided based on both partially and totally specified propositions. The final contribution of Chapter Three is concerned with the use of benchmark circuits for the purpose of evaluating new approaches in digital circuit engineering tasks. A history and analysis of many common benchmark circuit collections is provided as well as an analysis of their performance characteristics when used in a variety of different digital circuit engineering tasks.

Chapter Four is also included in the digital circuits section of the book and is comprised of three contributions. The first contribution is concerned with security oriented codes that are referred to as low complexity high rate robust codes. The motivation for the use of these types of codes is to overcome the effects of adversaries that may be employing side channel or other types of attacks. The next section is aimed toward increasing reliability through decomposing a circuit into linear and non-linear portions. A degree of linearity is introduced

whereby the measure can be used to guide a bi-decomposition of a candidate circuit. The final contribution of Chapter Four is concerned with partially specified functions and describes how such functions can be linearized.

The third and final part of the book is concerned with future technologies and is comprised of four contributions. The first contribution is concerned with reversible circuit synthesis via the use of functional decision diagrams (FDDs). Reversible circuit design is also considered in the second contribution; however this time a probabilistic approach in the form of an evolutionary algorithm is used. Although irreversible function classification has a rich history, the classification of reversible functions has not been studied to a similar depth. The next contribution is concerned with the classification of reversible circuits and provides several definitions and theorems. The final contribution moves from reversible logic into the more general realm of quantum operators and considers various decompositions for the $\texttt{C}^n\texttt{F}$ gate as derived from the $\texttt{C}^n\texttt{NOT}$ gate.

Mitchell A. Thornton

Southern Methodist University, Dallas, Texas, USA
June 2017