

Further Improvements in the Boolean Domain

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

Copyright © 2018 by Bernd Steinbach and contributors

All rights for this book reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the copyright owner.

ISBN (10): 1-5275-0371-2

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

Contents

LIST OF FIGURES	xi
LIST OF TABLES	xv
FOREWORD	xix
PREFACE	xxiii
ACKNOWLEDGMENTS	xxxiii
LIST OF ABBREVIATIONS	xxxvii

I Extensions in Theory and Computations 1

1 MODELS, METHODS, AND TECHNIQUES	3
1.1 NP-Problems and Boolean Equations	3
1.1.1 Classes of Hard Problems	3
1.1.2 Boolean Functions and Equations	4
1.1.3 Boolean Equations and Ternary Vectors	5
1.1.4 NP-Complete Problems	9
1.1.5 Boolean Equations - a Unifying Instrument ..	24
1.2 Number of Variables of Index Generation Functions ..	25
1.2.1 Background	25
1.2.2 An Index Generation Unit	26
1.2.3 Notation	27
1.2.4 Expected Number of Variables	29
1.2.5 Distribution of the Expected Number	31
1.2.6 Expected Number of Balanced Columns	38
1.2.7 Found Results	42

1.3	Computational Complexity of Error Metrics	43
1.3.1	Approximate Computing	43
1.3.2	Preliminaries	44
1.3.3	Error Metrics	46
1.3.4	Complexity of Computing Error Metrics	49
1.4	Spectral Techniques - Origins and Applications	54
1.4.1	Origins and Evolution of Spectral Techniques	54
1.4.2	Digital System Design	55
1.4.3	Signal processing	57
1.4.4	Towards FFT	59
1.4.5	Towards Alternative Spectral Techniques	60
1.4.6	Applications of Spectral Techniques	63
1.5	A Relational Approach to Finite Topologies	69
1.5.1	Experimentation as Motivation	69
1.5.2	Relation Algebra	70
1.5.3	Modeling Sets and Finite Topologies	71
1.5.4	Closures, Interiors and Boundaries	74
1.5.5	Topological Relations and Random Topologies	79
1.5.6	Implementation and Related Work	84
1.6	A Real-World Model of Partially Defined Logic	87
1.6.1	Real-World Asynchronous Feedback	87
1.6.2	Related Topics	88
1.6.3	Use Case: Low-Active RS-Latch	89
1.6.4	Stabilized Dual-Rail Implementation	93
1.6.5	Results	96
2	ACCELERATED COMPUTATIONS	99
2.1	Bent Function Enumeration Using an FPGA	99
2.1.1	Background	99
2.1.2	Properties of Bent Functions	100
2.1.3	Architecture for Bent Function Discovery	101
2.1.4	Circular Pipeline Architecture	106
2.1.5	Circuit of the Circular Pipeline	110
2.1.6	Experimental Results	111
2.1.7	Analytical Results	115
2.1.8	Practical Aspects	117
2.2	Efficient Generation of Bent Functions Using a GPU	120
2.2.1	Discovery of Bent Functions	120
2.2.2	Bent Functions in Two Domains	122
2.2.3	Random Generation of Bent Functions	128

2.2.4	Implementation on a GPU Platform	130
2.2.5	Comparison Between CPU and GPU Platforms	134
2.3	Multi-GPU Approximation Methods	136
2.3.1	Error Detection and Correction	136
2.3.2	Computing Distance Distribution of AN Codes	140
2.3.3	Results	147
2.3.4	Summary	154
2.4	Orthogonalization of a TVL in Disjunctive or Conjunctive Form	156
2.4.1	Orthogonality	156
2.4.2	Ternary Vector List (TVL)	159
2.4.3	Orthogonal Operations for Ternary Vectors . .	162
2.4.4	Orthogonalization of a TVL in DF or CF . . .	166
2.4.5	Experimental Results	171

II Digital Circuits 173

3	SYNTHESIS, VISUALIZATION, AND BENCHMARKS	175
3.1	Vectorial Bi-Decompositions for Lattices	175
3.1.1	Synthesis of Combinational Circuits	175
3.1.2	Vectorial and Single Derivative Operations . .	180
3.1.3	Generalized Lattices of Boolean Functions . . .	182
3.1.4	Vectorial Bi-Decompositions	189
3.1.5	Application of the Vectorial Bi-Decomposition	194
3.1.6	Comparison with Other Synthesis Approaches .	196
3.2	Hardware/Software Co-Visualization: The Lost World	199
3.2.1	The Lost World	199
3.2.2	Visualization Techniques	200
3.2.3	Core Issues	208
3.2.4	Enabling the Fiddlers and Tinkerers	210
3.2.5	A Brave New World	212
3.3	Synthesis of Complemented Circuits	214
3.3.1	Decomposition with Two-Input Operators . . .	214
3.3.2	Previous Work	217
3.3.3	Boolean Relations	218
3.3.4	Complemented Circuits	220
3.3.5	Minimization of Complemented Circuits	224
3.3.6	Structure of Complemented Circuits	225
3.3.7	Experimental Results	228

3.4	Design of Multipliers Using Fourier Transformations	240
3.4.1	Approaches for Multiplication on Hardware	240
3.4.2	Design of Monolithic Multipliers	241
3.4.3	The Adder Tree in Multiplication	246
3.4.4	Discussion of the Results	249
3.5	Low Power Race-Free State Assignment	253
3.5.1	Synthesis for Low Power Consumption	253
3.5.2	A Behavioral Model	253
3.5.3	The Condition for Absence of Critical Races	255
3.5.4	Minimizing the Length of State Codes	257
3.5.5	Minimizing the Switching Activity	258
3.5.6	A Heuristic Method	263
3.6	Boolean Discrete Event Modeling of Circuit Structures	268
3.6.1	Different Abstraction Levels for Modeling	268
3.6.2	Theoretical Foundation	270
3.6.3	Syntax for Discrete Event Modeling	272
3.6.4	Use Case: CMOS Inverter	274
3.6.5	Results	279
3.7	Collection of Logic Synthesis Examples	281
3.7.1	The Reasons to be Prudent	281
3.7.2	Benchmarks to Compare Design Tools	288
3.7.3	Origins of Benchmarks	290
3.7.4	Improvements of the Usability of Benchmarks	294
3.7.5	A Provided Collection of Benchmarks	297
3.7.6	Examples and Statistical Properties	300
4	RELIABILITY AND LINEARITY OF CIRCUITS	303
4.1	Low Complexity High Rate Robust Codes	303
4.1.1	The Hardware Security Problem	303
4.1.2	Security Versus Reliability	304
4.1.3	Robust Codes	306
4.1.4	The Shortened QS Code	312
4.1.5	The Triple QS and Triple Sum Codes	313
4.2	Synthesis for Reliability Using Bi-Decompositions	319
4.2.1	Methods to Improve the Reliability of Circuits	319
4.2.2	Synthesis for Reliability	321
4.2.3	Experimental Results	327
4.2.4	Reliability: Challenges and Approaches	333
4.3	Linearization of Partially Defined Boolean Functions	334
4.3.1	Partially Defined Boolean Functions	334

4.3.2	The Linearization Method	336
4.3.3	Efficient Finding of a Linear Transform	337
4.3.4	Existence of an Injective Linear Transformation	344
4.3.5	Connections to Linear Error-Correcting Codes	347

III Towards Future Technologies 353

5	REVERSIBLE AND QUANTUM LOGIC	355
5.1	FDD-Based Reversible Synthesis by Levels	355
5.1.1	Methods to Synthesize Reversible Circuits	355
5.1.2	Post-Order FDD-Based Reversible Synthesis	357
5.1.3	FDD-Based Reversible Synthesis by Levels	363
5.1.4	Experimental Results	369
5.2	Distributed Evolutionary Design of Reversible Circuits	372
5.2.1	Extending RIMEP2 to DRIMEP2	372
5.2.2	Background	372
5.2.3	The Hierarchical Model Based on RIMEP2	374
5.2.4	The Islands Model Based on RIMEP2	375
5.2.5	Hybrid Models	376
5.2.6	Experiments and Interpretation of the Results	377
5.2.7	Relevant Features	382
5.3	Towards Classification of Reversible Functions	384
5.3.1	Reversible Boolean Functions	384
5.3.2	Preliminaries	388
5.3.3	Homogeneous Component Functions	391
5.3.4	Motivation for Future Work	403
5.4	The C^nF Logic Functions Derived from C^nNOT Gates	405
5.4.1	Reconfigurable Reversible Processors	405
5.4.2	Background	406
5.4.3	C^3NOT Gate and C^3F Functions	408
5.4.4	Analysis of C^4NOT and C^4F	412
5.4.5	Generalizations and Remarks	413
	BIBLIOGRAPHY	419
	LIST OF AUTHORS	465
	INDEX OF AUTHORS	473
	INDEX	475

List of Figures

1.1	Ten queens and two pawns located at $c3$ and $e5$	10
1.2	Example of a vertex cover	13
1.3	Birkhoff's Diamond: uncolored and colored	16
1.4	Graph with a clique of three vertices	17
1.5	The adjacency matrix of a graph	18
1.6	Graph with a red colored clique	19
1.7	The incidence matrix of the graph of Figure 1.6	19
1.8	Edge cover of a graph	21
1.9	Hamiltonian path	22
1.10	Graph for exploring Eulerian paths	23
1.11	Index generation unit	26
1.12	Fraction of functions realized using 4 to 32 vectors . .	35
1.13	Adder circuit approximated from a ripple carry adder	48
1.14	A relation and two vector-models of sets of sets	75
1.15	Models of a topology and the set of closed sets	75
1.16	Sets and their closures, interiors and boundaries	78
1.17	Graphical visualization of a closure operation	78
1.18	Specialization, distinction and separation relation . . .	83
1.19	RELVIEW-programs: closures, interiors, boundaries . .	84
1.20	Low-active RS-latch and metastability	90
1.21	Race condition resulting in non-determined signals . .	90
1.22	Behavior of the programmable JK-/RS-buffer	94
1.23	Structure of the programmable JK-/RS-buffer	94
1.24	RS-buffer	95
1.25	Parallel composed partial low-active RS-latch	96
2.1	Original bent function enumeration circuit	102
2.2	Distribution of functions to the number of bent weights for $n = 4$	108

2.3	Distribution of functions to persistence in a circular pipeline for $n = 4$	109
2.4	Architecture of a single circular pipeline	110
2.5	Speed-Up and number of LUTs versus the number of circular pipelines	112
2.6	The Xilinx ZedBoard system	117
2.7	The complete system	118
2.8	Butterfly operations for the Reed-Muller and Walsh transform matrices	127
2.9	Example of a data-flow graph of the fast Reed-Muller transform algorithm of the Cooley-Tukey class	128
2.10	High-level architecture diagram of the GPU	132
2.11	Host program to launch a GPU program	133
2.12	Encoding of data words and decoding of code words.	137
2.13	CUDA implementation using local memory	143
2.14	CUDA implementation using shared memory	145
2.15	Shared memory access pattern	147
2.16	p_2^A and p_3^A for odd A 's for $k \in \{8, \dots, 16\}$	150
2.17	Convergence of the maximum relative error Δ	151
2.18	Influence of the number of iterations M	152
2.19	How value A controls the probability for $k = \{8, 16\}$	152
2.20	How value A controls the probability for $k = 24$	153
2.21	Structure of a Ternary Vector List (TVL).	160
2.22	Preprocessing steps to speed-up the orthogonalization	170
2.23	Comparison of computation time for $N=20$	171
2.24	Average number of Ternary Vectors (TVs) in the solution TVL for $N=20$	172
3.1	General structure of the bi-decomposition	177
3.2	Adding several directions of change to the independence matrix $IDM(f)$	188
3.3	Vectorial bi-decompositions: structure and conditions	190
3.4	Karnaugh-maps of (a) the given lattice and (b) the realized Boolean function.	195
3.5	Circuit structure with two vectorial OR-bi-decompositions	196
3.6	Circuit structure synthesized by weak and strong bi-decompositions	197
3.7	The Voronoi treemap of a software system	201
3.8	Software visualization through metaballs	201

3.9	The Pharo system visualizes software evolution	202
3.10	The code_swarm system animates software evolution	202
3.11	The state of current hardware visualizations	203
3.12	Waveform viewer illustrating signal assignments over time	204
3.13	Multi view hardware visualization	206
3.14	SystemC visualization of an adder module	207
3.15	SystemC visualization of a RISC CPU	207
3.16	Alternative realizations of a function $f(\mathbf{x})$ with complemented circuits	216
3.17	Maximal frequencies of monolithic multipliers and multipliers synthesized by Synopsys	243
3.18	Adder tree for a multiplication in regular arithmetic	247
3.19	Adder tree for a multiplication in saturation arithmetic: version 1	249
3.20	Adder tree for a multiplication in saturation arithmetic: version 2	250
3.21	Maximal frequencies of multipliers with adder trees	251
3.22	Module M^i with input vector ${}^i\mathbf{x}$ and output vector ${}^i\mathbf{y}$	273
3.23	Pull-up transistor circuit of a CMOS inverter	275
3.24	Pull-down transistor circuit of a CMOS inverter	276
3.25	Parallely composed CMOS inverter	278
3.26	Impact of transforming circuit examples into SOPs	284
3.27	Impact of transforming circuit examples into SOPs for 20 iterations	285
3.28	Comparison of IWLS'91 and IWLS'93	286
3.29	Comparison of IWLS'91 and IWLS'93 after synthesis	287
3.30	Development of the most popular benchmark sets	292
3.31	Structure of the circuit collection	299
3.32	Circuit sizes by literals in the original description	301
3.33	Circuit sizes by LUTs after synthesis	302
4.1	Schematic illustration of a communication model	305
4.2	Schematic of a hardware system	307
4.3	Mathematical model of a protected hardware system	310
4.4	Architecture for circuits with a high reliability	321
4.5	Separation of a variable using XOR gates	323
4.6	Structure of strong and vectorial bi-decompositions	326
4.7	Vectorial and strong XOR bi-decomposition of the carry function	328

4.8	Gate equivalents for the decomposed adder	330
4.9	Power for the decomposed adder	330
4.10	FPGA synthesis results	332
5.1	Types of Toffoli gates	357
5.2	Realization of the $4\text{mod}5$ benchmark	363
5.3	Optimal realization of the $4\text{mod}5$ benchmark	364
5.4	Utilization of a shared successor	364
5.5	Zero-polarity FDD for rd53	367
5.6	Circuit rd53 synthesized by the post-order algorithm	367
5.7	Circuit rd53 synthesized by mapping of levels	368
5.8	Topologies used to design reversible circuits	377
5.9	$C^2\text{NOT}$ gate implemented in the $\text{CNOT}/\text{CV}/\text{CV}^\dagger$	406
5.10	$C^3\text{NOT}$ using the Barenco model	408
5.11	Karnaugh-map of the function C^4F	412
5.12	Function $f_g(5) \cdot f_s(5)$	417

List of Tables

1.1	Negation	4
1.2	Boolean functions of two arguments	5
1.3	Binary code of ternary values	7
1.4	Two pawns and $n + 2$ queens on an $n \times n$ chessboard .	11
1.5	Set cover: all characteristic functions and all minimal covers	12
1.6	Exact set cover	13
1.7	All solutions to color Birkhoff's Diamond using 3, 4 or 5 colors	17
1.8	Ramsey numbers $R(r, s)$	20
1.9	Example of a registered vector table of weight 8	28
1.10	Fraction of $k \times k$ binary matrices versus the number of columns needed to distinguish all rows for $2 \leq k \leq 7$.	30
1.11	Fraction of $k \times k$ binary matrices versus the number of columns needed to distinguish all rows for $8 \leq k \leq 64$	31
1.12	Fraction of binary matrices $\mathcal{T}(n, k)$ with $k \leq 32$ rows and n columns (all rows are distinguished)	33
1.13	Average number of columns to distinguish rows in random binary matrices	36
1.14	Fraction of binary matrices such that all rows are distinguished	41
1.15	Truth table and bitflips for the exact adder $+$ and the approximated adder $\hat{+}$	49
1.16	Low-active RS-latch—logical vs. digital	91
2.1	Speed and resources used in a circular pipeline compared to the resources available in a Xilinx FPGA . .	113
2.2	Simultaneous bent functions found per clock period for $n = 4$	114

2.3	Functions with persistence 8 and their contributions	115
2.4	Functions with persistence 7 and their contributions	116
2.5	Clocks used by functions of various persistence values	117
2.6	Limitation of the number of non-zero PPRM coefficients of bent functions	129
2.7	Comparison of random generation of one bent function on a CPU and two GPUs	135
2.8	Calculation of the distance distribution of AN codes	148
2.9	Solution time for 1D grid point sampling with $A=61$	148
2.10	Profiler results	149
2.11	Super A 's and minimum Hamming distances	154
2.12	Orthogonal conjunctions	158
2.13	Orthogonal disjunctions	158
2.14	Relationship between a ternary element and a Boolean Variable	160
2.15	Complement of ternary elements	161
2.16	Intersection of two ternary elements	161
3.1	Alternative circuits for the same function of a lattice	198
3.2	Example of a Boolean relation	219
3.3	A three-output function specified by a relation	219
3.4	Binary operations depending on both x and y	221
3.5	Relations corresponding to the operation AND	222
3.6	Relations corresponding to the operation OR	223
3.7	Relations corresponding to the operation XOR	224
3.8	Boolean relations for functions with two outputs	228
3.9	Comparison of SOP vs. complemented circuits using the method EXACT	230
3.10	Comparison of SOP vs. complemented circuits using the method HEURISTIC	231
3.11	Minimization results using the method EXACT	232
3.12	Minimization results using the method HEURISTIC	233
3.13	Gain of complemented circuits w.r.t. corresponding SOP forms	234
3.14	Average gain of complemented circuits w.r.t. corresponding SOP forms	234
3.15	Comparison of time, area and delay between ESPRESSO and complemented circuits - EXACT case	235
3.16	Comparison of time, area and delay between ESPRESSO and complemented circuits - HEURISTIC case	236

3.17	Number of conjunctions of the DNF and the minimized DF	242
3.18	Number of adders needed for FTM multiplications	248
3.19	Transition function	255
3.20	Conditional probabilities of the explored transitions	260
3.21	Absolute probabilities of the explored transitions	261
3.22	Compatible sets	261
3.23	Definition of the implication and equivalence	270
3.24	Partial and total specification of proposition C	271
3.25	Pin specification of the pull-up transistor	275
3.26	Pin specification of the pull-down transistor	277
3.27	Circuit origins and filename prefixes	298
3.28	Basic statistical properties	301
4.1	Comparison of binary high rate robust separable codes	317
4.2	Comparison of non-binary high rate robust separable codes	318
4.3	Degree of linearity of adder functions s_0, \dots, s_8	325
4.4	Areas and delay for different decomposed adders	331
5.1	Realization of BDD and FDD nodes by Toffoli gates	359
5.2	Realization of positive Davio nodes by Toffoli gates	360
5.3	Realization of negative Davio nodes by Toffoli gates	361
5.4	Reversible networks using zero-polarity FDDs	370
5.5	Reversible networks using optimal PPFDDs	371
5.6	Benchmark specifications from [357, 394]	379
5.7	Average quantum cost within 100 runs	380
5.8	The total execution time for 100 independent runs	381
5.9	Successful runs over 100 runs	382
5.10	Performance of DRIMEP2 versus [357, 394]	383
5.11	Establishing values of the 3-variable function f_1	399
5.12	Truth table for the function NPC3×3	400
5.13	Construction of a 3×3 reversible function	403
5.14	Two components of the C^2 NOT gate	406
5.15	Truth table of the C^3 NOT function	409
5.16	Truth table of the Majority controlled NOT gate	411
5.17	Significant control functions of the $f_g(\cdot)$ components	413

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 C^nF gate as derived from the C^nNOT gate.

Mitchell A. Thornton

Southern Methodist University, Dallas, Texas, USA
June 2017

Preface

Digital systems significantly contribute to the progress in almost all areas of our life. Boolean variables and functions are used to describe such systems. These variables can only carry two different values: 0 and 1. This is the smallest possible number and contributes to both a high reliability and a simpler production in comparison to systems with a higher number of different basic values. This book presents further improvements regarding a large number of problems by 36 authors from the international Boolean domain research community. Basic versions of the contributions of this book have been published in the proceedings of the 12th International Workshop on Boolean Problems [320].

Improvements in the Boolean domain require both progress in theory and powerful tools which utilize the new theory. The first part of this book deals with methods, algorithms, and programs for these aims.

Solutions of many Boolean problems exponentially depend on the number of variables. Hence, we are faced in the Boolean domain with the most complex problems. In addition to the well-known CD-SAT-formulas which are restricted to conjunctions of disjunctions (clauses), the more compact CDC-SAT-formulas are introduced where the variables of the disjunctions are replaced by the conjunction of Boolean variables. Due to the improved power of SAT-solvers and the high performance of ternary vectors and further concepts implemented in the XBOOLE system, Boolean problems can be solved that have a complexity far beyond any human possibilities. Hence, it remains to find a proper description of the problem using Boolean variables, Boolean functions, and Boolean equations. Using many examples reaching from combinatorics on the chessboard, over several covering problems, to different graph coloring problems, the creation of models represented by Boolean equations as a unifying instrument have been demonstrated.

An index generation function is a function which maps a binary input pattern to a unique non-zero integer index value. Such a pattern may represent a virus to be detected or a packet to be routed. The number of Boolean variables needed to distinguish between all patterns determines the size and cost of the hardware needed to realize such a function. Assuming that the k patterns must be detected then m variables are needed, where $\lceil \log_2 k \rceil \leq m \leq k - 1$. Using an experimental approach it has been found that the minimum number of variables needed in the realization of an index generation function can be expected to be closer to the lower bound than to the upper bound, especially when k is large. Hence, most index generation functions can be realized using inexpensive conventional memory. Furthermore, it has been found that balanced columns are of benefit to the search for minimum distinguishing sets, especially when k is small.

Significant improvements in terms of performance and energy efficiency can be achieved when instead of an exact implementation an approximate one is realized. Approximate computing is a technique that relaxes the requirement for an exact equivalence between the specification and the implementation of circuits. This approach can be used, e.g., when the limited perceptual capabilities of humans do not require an exact numerical computation. The quality of an approximation is measured using an error metric that compares the approximated function with the original one. Several error metrics are explored with the result that the synthesis for approximate computing with precise error bounds is a difficult task. The derived challenges have a need for strong methods in computing precise errors as well as heuristics methods.

Spectral techniques based on various spectral transforms in different algebraic structures provide the foundations for the approaches for classifying Boolean functions, detecting their hidden properties, or reducing the computation effort. A comprehensive review of the origins and evolution of spectral techniques provide the readers with a very useful basis for research in the areas of design of digital systems and signal processing. Many references to books or articles in journals support this research. This review indicates that both serious tasks and restricted resources are incitements for scientific progress and practical applications. It can be expected that spectral techniques furthermore contribute to improvements in the Boolean domain.

Topology is a fundamental branch of mathematics that explores the properties of mathematical structures. Basics of topology are geometry and set theory. The descriptive set theory that explores operator algebras, computability, mathematical logic, as well as harmonic analysis belong to the wide field of applications of topologies. Due to the focus on computational problems finite topologies are explored. It is shown how objects and concepts from finite topologies can be modeled using relations, how related tasks can be expressed using the language of relation algebra and how the RELVIEW system can be used to compute and visualize solutions. The efficient implementation of this tool allows for experiments with very large topologies.

The clocked synchronization of digital systems ensures their deterministic behavior to the price of a certain inefficiency. Analog systems work efficiently but suffer under an ambiguous behavior. It is a challenge to couple the advantages of these types of systems to create efficient deterministic circuits. Key issues in this field of research are partially defined functions, their models, and utilization within the design process. A new formal methodology is suggested that warrants the match between the partially specified functions and real world asynchronous feedback structures. This dual-rail approach combines the benefits of both traditional types of systems and can even be used for safety critical systems.

Due to the exponentiation complexity of almost all Boolean problems efficient tools for their solution are needed. As an example of a very hard Boolean problem the computation of the number of bent functions has been selected. Bent functions are the most non-linear functions that can be used in cryptography to resist linear attacks. In a previous work an expensive reconfigurable computer was used to speed-up this calculation by about 60,000 times. The utilization of both a deeper knowledge about bent functions and the application of a circular pipeline on a much cheaper Field Programmable Gate Array (FPGA) result in an additional speed-up of more than two orders of magnitude.

The computation of bent functions is also the topic of other research. The key idea of this approach consists of the random generation of a function of a certain even number of variables and the check to see whether it is a bent function. Due to the very small fraction of

bent functions the generation is executed in the Reed-Muller domain, where the search spaces for bent functions can be restricted by means of several theorems. The fast Reed-Muller transform has been used to compute the truth vector of a Boolean function. Utilizing the GPU an additional speedup of up to three orders of magnitude has been reached for bent functions of up to ten variables.

An important practical problem is the detection and correction of one or more bit flips (errors) in data words, for which data coding is typically exploited. There is always the risk that bit flips change valid code words into other valid code words, which prohibits both error detection and correction. In order to minimize this risk non-systematic, non-linear AN-codes are used. The letter A indicates an integer constant used to encode the data word N , which is usually also an integer number. Here, the error detection capability is influenced by both the parameter A and the data type of N . To estimate the risk of undetectable bit flips, we need to compute the distance distribution between the codewords for each possible value of A depending on the width k of the data words. This computation is a big challenge which has time complexity in the order of 4^k . Efficient multi-GPU implementations have been developed to solve this problem and determine preferable values of A .

The representation of a Boolean function as an orthogonal list of ternary vectors allows us to use such a TVL for both a disjunctive form and an antivalence form. The knowledge that each binary vector cannot be covered by more than one ternary vector of such an orthogonal TVL is an additional advantage. A special order in which the ternary vectors are selected from a TVL in disjunctive form to compute the needed orthogonal difference leads to a shorter number of ternary vectors in the resulting TVL. The preprocessing steps of absorption and sorting of the ternary vectors by increasing numbers of dashes additionally contribute to both a shorter time needed to compute an orthogonal TVL and the smaller number of ternary vectors in the result.

Improvements in the Boolean domain considerably affect the development and application of digital circuits. Due to the extensive use of such circuits in almost all areas of our daily life we immediately notice this progress. Digital circuits have been developed and applied over

several decades. Hence, one could think all problems about them have already been solved. The second part of this book explores new insights in this field and confirms the continuous progress in appropriate research and applications.

Bi-decomposition is a powerful synthesis method for combinational circuits. This method splits a given function into two simpler functions which control the inputs of an AND-, an OR, or an XOR-gate such that the given function appears on the output of this gate. The simplification of the decomposition functions is reached in the case of the strong bi-decomposition by a smaller number of variables that the decomposition functions are depending on. Strong and weak bi-decompositions are sufficient for a complete synthesis approach. The decomposition functions of recently suggested vectorial bi-decompositions are simpler than the given function because of the independence of the simultaneous change of several variables. The generalized theory of derivative operations for lattices of the second level has been utilized for vectorial bi-decompositions of such lattices and furthermore reduces the needed chip-area, power, and delay of the synthesized circuits.

An interesting analysis about the visualization in both the hardware and software domains come to astounding and alarming results. While software visualization is an active field of research that supports the software designer with many helpful visualization techniques, the hardware visualization is in a state of a “lost world”. Almost unchanged over several decades are graph views that are used to show how parts of the hardware are interconnected and waveform views visualize the signal changes over time. In the context of growing system designs, where both hardware and software contribute to the solution, innovative tools are needed for Hardware/Software Co-Visualization. The answer to the question “why” there is such a discrepancy between hardware and software visualization approaches can help to remove obstacles and encourage engineers and scientist to fill the recent gap in this field.

Traditional aims in circuit design consist of the synthesis of smaller and faster circuits for a given function. A new contribution to improve the reached limits of these aims is the synthesis of complemented circuits. This approach utilizes the differences in the space and delay

needed that can exist between a circuit that realizes the given function and a circuit of the complement of this function. The benefits of the new complemented circuits result from the common use of both the function and its complement as well as the utilization of given and created don't cares. The theoretical basis of this approach is the utilization of Boolean relations which are explored for all ten operations depending on two-inputs. Comprehensive experimental results for both the exact and heuristic synthesis of more than 100 benchmark functions show that this new approach improves the known results of three-level circuits in many cases.

Next to addition, multiplication is a frequently used arithmetic operation in digital circuits. While several approaches of optimized adders are known, the possibilities to optimize multipliers are not as yet completely utilized. There are two types of multipliers. Assuming n bits for each of the two input values, in regular arithmetic the output of the multiplier contains $2n$ bits, but in saturation arithmetic the output is restricted to n bits. A comprehensive exploration of circuit structures of multipliers in both regular and saturation arithmetic leads to up to 33% faster circuits in comparison to the multipliers synthesized by the commercial tool Synopsys. The sources for this improvement are the use of a monolithic multiplier block of a size of around 4×4 , the concatenation of fitted intermediate results, and a restricted tree of adders. Unfortunately, the reached speed up of monolithic multiplier blocks of a size of 4×4 or 5×5 requires about two to five times more area.

The power consumption becomes a more and more important limitation factor for very large scale integrated circuits. The thermal leakage power causes a temperature rise that constrains the circuit behavior and requires additional equipment for heat transmission away from the device. Low power consumption is also welcome for a long period of use of a mobile device until the next charge of the rechargeable battery. The power consumption is caused by the switching elements. One contribution to reduce the power consumption consists of the state assignment of an automaton such that a minimal number of switching elements must be changed for the needed transitions. A basic model and an heuristic algorithm for this task will be explained. This approach can be used for asynchronous finite state machines and leads to race-free circuits of low power consumption.

Digital systems are realized by logic gates and flip-flops. Many synthesis approaches are known to find a circuit structure of these building blocks for a given behavior. Transistors are the real switching elements used within the logic gates and flip-flops. A more fine granular modeling technique has been suggested that directly allows us to use transistors as basic building blocks of digital systems. The theoretical foundation is constituted on the definition of both partial and total operations of the implication and equivalence. This approach can be uniformly used on several levels of abstraction: the global behavior represented by a directed graph, the more concrete signal flow graph which can be seen as the most abstract structural view of a arbitrary circuit, the even more concrete signal flow plan that consists of modules of partially defined behaviors, down to the transaction level modeling.

The complexity of digital circuits requires the use of design automation tools. Consequently, new synthesis procedures are implemented in such tools to improve the structure of the designed circuits. The only way to compare the properties of several synthesis tools is the synthesis of a set of circuits based on the same descriptions of these benchmark circuits. This general approach has been used over several decades and different benchmark sets were published and used for this purpose. However, the circuit implementations have been changed over the years and influenced the creation of new benchmark sets. A prudent approach led to a comprehensive collection of benchmark circuits for logic synthesis and optimization. The benefit of this collection is a unique description of benchmarks of many sources presented in a cleaned, flattened form and split into connected components.

Secret information stored within a hardware system is the target of side-channel attacks such as the differential fault analysis. Such attacks try to inject faults into the system that alter the output. Knowing the injected faults and the associated output signals the wanted secret keys can be calculated. The faults can be injected within the communication channel. Security oriented codes for the transmitted data can be used to detect injected faults and prevent such side-channel attacks. The few known codes have drawbacks regarding the error masking probability as well as the cost of their implementation. New suggested low complexity, high rate robust codes are the shortened quadratic-sum, triple sum, and triple-quadratic-sum codes.

These codes close the mentioned gaps and are able to detect any error in the transmitted data with non-zero probability.

The decrease of circuit structures to a few nanometers has the benefit of both a reduced area and a reduced power consumption but unfortunately increases the appearance of faults caused by outer influences like cosmic radiations. Hence, fault tolerant techniques must be used to improve the reliability of digital circuitry. One of these techniques is the extension of the circuit by redundancy such that an error correction becomes realizable. Low density parity check codes can be used for this purpose and were successfully applied to improve the reliability of XOR-only logic network. This requires a split of the circuit into a linear and a non-linear part. Methods to synthesize circuits where the linear part is separated from the non-linear part are explored for adders of different sizes. Both the strong and the vectorial bi-decompositions contribute to this aim of synthesis.

Another application of a linear circuit is the transformation of incompletely specified Boolean functions of n variables into a Boolean space of m variables where $m < n$. Such a transformation is possible when the function values are specified only for k input patterns and the value of k is much smaller than 2^n . Applications of this task are, e.g., the design of on-line real-time control systems or built-in self-test equipment. The number of variables m of the target space should be as small as possible. An efficient method of finding a linear transform that is injective for the k specified input patterns will be explained. Using the knowledge of the coding theory and the theory of finite fields a lower bound has been found which strongly reduces the search space for such a transformation. This lower bound depends on both the number of variables n and the number of specified input patterns k . The provided results have interesting connections to linear error-correcting codes.

The third part of this book deals with problems that the Boolean domain will be faced with in the future. The continued reduction of the size of the switching elements brings us closer (and close) to the level of single atoms and quantum logic. Completely different physical laws must be considered in this field. The exploration of reversible circuits can be seen as a bridge between traditional circuit structures and circuits realized using future quantum technologies.