

Intelligent Systems Reference Library

Volume 201

Series Editors

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland

Lakhmi C. Jain, KES International, Shoreham-by-Sea, UK

The aim of this series is to publish a Reference Library, including novel advances and developments in all aspects of Intelligent Systems in an easily accessible and well structured form. The series includes reference works, handbooks, compendia, textbooks, well-structured monographs, dictionaries, and encyclopedias. It contains well integrated knowledge and current information in the field of Intelligent Systems. The series covers the theory, applications, and design methods of Intelligent Systems. Virtually all disciplines such as engineering, computer science, avionics, business, e-commerce, environment, healthcare, physics and life science are included. The list of topics spans all the areas of modern intelligent systems such as: Ambient intelligence, Computational intelligence, Social intelligence, Computational neuroscience, Artificial life, Virtual society, Cognitive systems, DNA and immunity-based systems, e-Learning and teaching, Human-centred computing and Machine ethics, Intelligent control, Intelligent data analysis, Knowledge-based paradigms, Knowledge management, Intelligent agents, Intelligent decision making, Intelligent network security, Interactive entertainment, Learning paradigms, Recommender systems, Robotics and Mechatronics including human-machine teaming, Self-organizing and adaptive systems, Soft computing including Neural systems, Fuzzy systems, Evolutionary computing and the Fusion of these paradigms, Perception and Vision, Web intelligence and Multimedia.

Indexed by SCOPUS, DBLP, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

More information about this subseries at <http://www.springer.com/series/8578>

Antonio Lloris Ruiz ·
Encarnación Castillo Morales · Luis Parrilla Roure ·
Antonio García Ríos · María José Lloris Meseguer

Arithmetic and Algebraic Circuits

Antonio Lloris Ruiz
Departamento de Electrónica y
Tecnología de Computadores
Campus Universitario Fuentenueva
Universidad de Granada
Granada, Spain

Encarnación Castillo Morales
Departamento de Electrónica y
Tecnología de Computadores
Campus Universitario Fuentenueva
Universidad de Granada
Granada, Spain

Luis Parrilla Roure
Departamento de Electrónica y
Tecnología de Computadores
Campus Universitario Fuentenueva
Universidad de Granada
Granada, Spain

Antonio García Ríos
Departamento de Electrónica y
Tecnología de Computadores
Campus Universitario Fuentenueva
Universidad de Granada
Granada, Spain

María José Lloris Meseguer
Oficina Española de Patentes y Marcas
O.A. (OEPM), Madrid, Spain

ISSN 1868-4394

ISSN 1868-4408 (electronic)

Intelligent Systems Reference Library

ISBN 978-3-030-67265-2

ISBN 978-3-030-67266-9 (eBook)

<https://doi.org/10.1007/978-3-030-67266-9>

© Springer Nature Switzerland AG 2021

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To our children and grandchildren

Julio

Lucía, Adriana and Pablo

José Luis and Sofía

Marina

Ana, Carmen and Jaime

who are the future

Prologue

Arithmetic Circuits are those digital circuits with inputs interpreted as numbers and whose outputs provide the results of some arithmetic operation over the inputs (addition, subtraction, multiplication, or division). These initial objectives (the elemental arithmetic operations) have been expanded so any mathematical function (trigonometrics, exponentials, logarithmics, etc.) is included as the purpose of the arithmetic circuits.

As a first definition, *Algebraic Circuits* are those digital circuits whose behaviour can be associated with any algebraic structure. Specifically, a polynomial is associated to each circuit, so that the evolution of the circuit will correspond to the algebraic properties of the polynomial. **LFSRs** (**L**inear **F**eedback **S**hift **R**egisters) and **CAs** (**C**ellular **A**utomata), included in this first denomination of algebraic circuits, are grouped under the name of *basic algebraic circuits*.

As a second definition, *Algebraic Circuits* are those digital circuits implementing the different operations within some algebraic structure. Specifically, in this book, this definition references to finite or Galois fields. The implementation of this *algebraic circuits* requires **LFSRs** and some basic arithmetic circuits.

This book is an expansion of our previous book *Algebraic Circuits*, including now arithmetic circuits, as both, arithmetic and algebraic, have many in common. Besides the addition of new material, each chapter includes a collection of exercises for didactic purposes.

The reader mainly interested in algebraic circuits will find the corresponding materials in Chaps. 1, 2, 3, 9, 10, 11, and 12; those interested only in arithmetic circuits may obviate Chaps. 3, 9, 10, 11, and 12.

Each chapter has been written as autonomous as possible from the rest of the book, thus avoiding back-consultation; this has the drawback of some redundancy, particularly of Chaps. 1 and 2 with those devoted to arithmetic circuits.

Chapter 1 is devoted to number systems, and a complete revision of the different representations of integer numbers is made, including redundant systems. The main procedures for the implementation of the fundamental arithmetic operations (addition, subtraction, multiplication, division, and square root) are also presented.

The implementation of those arithmetic circuits used for the construction of algebraic circuits is the purpose of Chap. 2. Addition, subtraction, multiplication,

division (with special attention to modular reduction), and square root are implemented. Also, comparators and shifters, which can be considered to actually perform arithmetic operations but usually not considered as such, are described.

Chapter 3 deals with residue number systems, which are systems for numerical representation with interesting applications under the appropriate circumstances. Also, the Galois fields $\text{GF}(p)$ are introduced in this chapter, since modular operations for prime values of p have to be implemented in $\text{GF}(p)$.

Chapter 4 is mainly dedicated to the floating-point representation of real numbers, used profusely in arithmetic circuits. Rounding schemes and the IEEE 754 standard are presented, as well as circuit design to implement the main floating-point arithmetic operations. Also, the logarithmic system for real number representation is described.

Chapters 5–8 expand the basic arithmetic circuits presented in Chap. 2. As mentioned above, and in order to make each chapter autonomous, some redundancy is allowed in these chapters.

Addition and subtraction are explored in detail in Chap. 5, specially all the questions associated to carry propagation for the construction of fast adders. Multioperand adders are described, to be used in the design of multipliers.

Multiplication is approached in Chap. 6, studying both combinational and sequential multipliers, as well as some special multipliers.

Division, the most complex of the basic arithmetic operations, is the object of Chap. 7. Division algorithms and their hardware implementations are sufficiently covered.

The computation of the most commonly used mathematical functions (logarithms, exponentials, trigonometrics, etc.) is the purpose of Chap. 8. The **CORDIC** algorithm is used as a general introduction to the procedures described in this chapter.

The basic algebraic circuits are the objective of Chap. 9. Regarding **LFSRs**, classic circuits, those storing a single bit in each cell, are introduced first. Then, they are generalized defining circuits with cells storing more than one bit each. The **CAs** studied in this chapter are mainly one-dimensional and linear, although two-dimensional **CAs** are also defined.

Chapter 10 is devoted to the Galois fields $\text{GF}(2^n)$, presenting circuits to implement sums, products, divisions, squares, square roots, exponentiations, and inversions using power representation and the standard, normal, and dual basis. Also, the operations in the composite Galois fields $\text{GF}((2^n)^m)$ are detailed.

Chapter 11 is parallel to Chap. 10, but refers to Galois fields $\text{GF}(p^n)$ and $\text{GF}((p^n)^m)$.

Chapter 12 presents two very simple cryptographic applications of Galois fields: the first is based on the use of discrete logarithms, and as a real example, the Galois field $\text{GF}(2^{233})$ is used. The second is devoted to elliptic curves, and as a real example, the Galois field $\text{GF}(2^{192} - 2^{64} - 1)$ is used.

All related mathematical fundamentals concerning Galois fields are divided into three appendices structuring everything that is used in the corresponding chapters, without any demonstration of most of the theorems and algorithms. The objective of these appendices is to provide an immediate source and to unify the nomenclature. Readers interested in in-depth details may use the indicated

references. In Appendix A, the postulates and theorems about Galois fields are provided. Appendix B is devoted to the algebra of polynomials, paying particular attention to the different forms of representation. Appendix C includes all matters relating to elliptic curves used in the application examples developed in Chap. 12. Appendix D elaborates on errors, an important question when dealing with arithmetic circuits. Finally, Appendix E describes some important algorithms for function implementation, while Chebyshev and Legendre sequences of orthogonal polynomials are also presented.

Written as a self-contained text, this book is mainly intended as a practical reference for designers of hardware applications, but also may be used as textbook for courses on arithmetic and/or algebraic circuits. The exercises at the end of each chapter facilitate the practice of the corresponding concepts.

Contents

1	Number Systems	1
1.1	Introduction	1
1.1.1	Additional Notation	2
1.1.2	Positional Notation	3
1.2	Positional Notation Using One Base	3
1.2.1	Most Efficient Radix	4
1.2.2	Base Conversion	5
1.2.3	Bases Power of Two	8
1.2.4	Modular Arithmetic	11
1.2.5	Fractional Numbers: Fixed Point Representation	14
1.3	Multiple Radix Representations	15
1.3.1	Double Radix	15
1.3.2	Mixed Radix	16
1.4	Negative Integer Numbers	18
1.4.1	SM Representation	19
1.4.2	Complement Representations	21
1.4.3	Biased Representation	35
1.4.4	Advantages and Disadvantages of the Different Representations	37
1.5	Binary Numbers Multiplication	37
1.5.1	SM Representation	38
1.5.2	Complement Representations	38
1.6	Division and Square Root of Binary Integer Numbers	41
1.6.1	Division	42
1.6.2	Square Root	43
1.7	Decimal Numbers	45
1.7.1	BCD Sum	46
1.7.2	Negative Decimal Numbers	48
1.7.3	Packed BCD Codification (CHC)	51
1.8	Signed Digits	55
1.8.1	Negative Digits	55
1.8.2	Conversion Between Representations	57

1.8.3	Binary Signed Digits (BSD)	58
1.9	Redundant Number Systems	67
1.9.1	Carry Propagation	68
1.9.2	Binary Case	71
1.10	Conclusion	72
1.11	Exercises	72
	References	75
2	Basic Arithmetic Circuits	77
2.1	Introduction	77
2.1.1	Serial and Parallel Information	77
2.1.2	Circuit Multiplicity and Pipelining	78
2.2	Binary Adders	80
2.2.1	Parallel Adders	80
2.2.2	Pipelined Adders	83
2.2.3	Serial Adders	84
2.3	Binary Subtractors	85
2.4	Multipliers	87
2.4.1	Combinational Multipliers	87
2.4.2	Sequential Multipliers	91
2.4.3	Multiplying by a Constant	95
2.5	Exponentiation	98
2.5.1	Binary Methods	100
2.5.2	Additive Chains	103
2.6	Division and Square Root	106
2.6.1	Combinational Divisors	106
2.6.2	Sequential Divisors	108
2.6.3	Dividing by a Constant	109
2.6.4	Modular Reduction	109
2.6.5	Calculating the Quotient by Undoing the Multiplication	112
2.6.6	Calculating the Quotient by Multiplying by the Inverse of the Divisor	114
2.6.7	Modular Reduction (Again)	119
2.6.8	Square Root	120
2.7	BCD Adder/Subtractor	120
2.8	Comparators	124
2.9	Shifters	126
2.9.1	Shifters Built with Shift Registers	128
2.9.2	Combinational Shifters	128
2.10	Conclusion	130
2.11	Exercises	130
	References	131

3	Residue Number Systems	133
3.1	Introduction	133
3.2	Residue Algebra	134
3.3	Integer Representation Using Residues	142
3.4	Arithmetic Operations Using Residues	144
3.5	Mixed Radix System Associated to Each RNS	145
3.6	Moduli Selection	147
3.7	Conversions	148
3.7.1	From Positional Notation to RNS	148
3.7.2	From RNS to Positional Notation	152
3.8	Modular Circuits	153
3.8.1	Addition and Subtraction	153
3.8.2	Multiplication and Division	158
3.8.3	Montgomery Multiplier	163
3.8.4	Exponentiation	165
3.8.5	Two Implementation Examples: 3 and 7	166
3.9	Conclusion	171
3.10	Exercises	171
	References	172
4	Floating Point	173
4.1	Introduction	173
4.2	Precision and Dynamic Range	176
4.3	Rounding	181
4.3.1	Rounding Without Halfway Point	182
4.3.2	Rounding with Halfway Point	186
4.3.3	ROM Rounding	194
4.4	Decimal Rounding	195
4.5	Basic Arithmetic Operations and Rounding Schemes	196
4.5.1	Comparison	196
4.5.2	Addition and Subtraction	198
4.5.3	Multiplication and Division	199
4.5.4	Rounding Bits	201
4.5.5	Leading Zeros Detection	202
4.6	The IEEE 754 Standard	203
4.6.1	Binary Interchange Formats	204
4.6.2	Decimal Interchange Formats	206
4.6.3	Zero, Infinite and NaNs	208
4.6.4	Arithmetic Formats	208
4.6.5	Formats and Roundings	209
4.6.6	Operations	209
4.7	Circuits	210
4.7.1	Adder/Subtractor	210
4.7.2	Multiplier and Divider	211
4.7.3	Binary Square-Root	212

4.7.4	Comment	213
4.8	The Logarithmic System	213
4.8.1	Conversions	215
4.8.2	Arithmetic Operations	216
4.9	Conclusion	218
4.10	Exercises	218
	References	220
5	Addition and Subtraction	221
5.1	Introduction	221
5.2	Basic Concepts	222
5.3	Carry Propagation: Basic Structures	225
5.3.1	Considerations on Carry Propagation	227
5.3.2	Basic Carry Look-Ahead	227
5.3.3	Carry Look-Ahead Adders	230
5.3.4	Carry Skip Adders	235
5.3.5	Prefix Adders	238
5.4	Carry-Selection Addition: Conditional Adders	241
5.5	Multioperand Adders	244
5.5.1	Carry-Save Adders	246
5.5.2	Adder Trees	248
5.5.3	Signed Operands	254
5.6	Conclusion	254
5.7	Exercises	254
	References	255
6	Multiplication	257
6.1	Introduction	257
6.2	Basic Concepts	258
6.3	Combinational Multipliers	259
6.4	Combinational Multiplication of Signed Numbers	265
6.5	Basic Sequential Multipliers	268
6.5.1	Shift and Add Multipliers	268
6.5.2	Shift and Add Multiplication of Signed Numbers	271
6.6	Sequential Multipliers with Recoding	274
6.6.1	Multiplication Using Booth Codification	275
6.6.2	Multiplication Using (−1, 0, 1, 2) Coding	277
6.7	Special Multipliers	280
6.7.1	Multipliers with Saturation	280
6.7.2	Multiply-and-Accumulate (MAC)	281
6.7.3	Multipliers with Truncation	282
6.8	Conclusion	283
6.9	Exercises	284
	References	284

7	Division	287
7.1	Introduction	287
7.2	Basic Concepts	287
7.3	Non-restoring Division	290
7.4	Signed Non-restoring Division	295
7.5	SRT Division	298
7.5.1	Radix-2 SRT	301
7.5.2	Radix-4 SRT	305
7.5.3	Radix-4 SRT with Codification $[-2, 2]$	312
7.6	Conclusion	314
7.7	Exercises	314
	References	315
8	Special Functions	317
8.1	Introduction	317
8.2	A Case Study: The CORDIC	320
8.2.1	Circular Case	320
8.2.2	Hyperbolic Case	329
8.2.3	Linear Case	339
8.2.4	Unification and Modifications	342
8.2.5	Implementation	342
8.3	Shift-and-Add Algorithms	343
8.3.1	Algorithm for the Function e^t	345
8.3.2	Algorithm for the Function $\ln(x)$	346
8.4	Newton-Raphson Method	348
8.4.1	Square Root	349
8.4.2	Reciprocal	351
8.5	Polynomial Approximation	353
8.5.1	Least Squares Methods	355
8.5.2	Least Maximum Methods	356
8.6	Table-Based Methods	357
8.6.1	Mainly Look-Up Table Based Methods	358
8.6.2	Small Look-Up Tables Based Methods	362
8.6.3	Table-Based Balanced Methods	367
8.7	Conclusion	374
8.8	Exercises	375
	References	376
9	Basic Algebraic Circuits	379
9.1	LFSR	379
9.1.1	Type 1 LFSR	380
9.1.2	M Sequences	385
9.1.3	Polynomials Associated to LFSR1s	388
9.1.4	Type 2 LFSR	392
9.1.5	LFSRmod 2^m	396
9.2	LFSRmodp	400

9.2.1	Type 1 LFSRmodp	400
9.2.2	Type 2 LFSRmodp	405
9.2.3	LFSRmodp ^m	408
9.3	Circuits for Operating with Polynomials	409
9.3.1	Circuits for Polynomial Addition and Subtraction	410
9.3.2	Circuits for Polynomial Multiplication	411
9.3.3	Circuits for Polynomial Division	417
9.3.4	Multipliers and Divisors as Filters	425
9.4	Cellular Automata	433
9.4.1	One-Dimensional Linear Cellular Automata	435
9.4.2	One-Dimensional Non-linear Cellular Automata	446
9.4.3	Bidimensional Cellular Automata	446
9.4.4	Mod2 ⁿ and Modp Cellular Automata	451
9.5	Conclusion	452
9.6	Exercises	452
	References	457
10	Galois Fields GF(2^m)	459
10.1	Addition Over GF(2 ^m)	459
10.2	Multiplication Over GF(2 ^m) with Power Representation	461
10.3	Multiplication Over GF(2 ^m) Using Standard Base	463
10.3.1	Modular Reduction	464
10.3.2	Parallel Multiplication	466
10.3.3	Serial-Parallel Multiplication	473
10.3.4	Serial Multiplication	478
10.4	Multiplication Over GF(2 ^m) Using the Normal Base	481
10.5	Multiplication Over GF(2 ^m) Using the Dual Base	489
10.6	Square and Square Root Over GF(2 ^m)	493
10.6.1	Square	493
10.6.2	Square Root	497
10.7	Exponentiation Over GF(2 ^m)	498
10.8	Inversion and Division Over GF(2 ^m)	500
10.9	Operations Over GF((2 ⁿ) ^m)	504
10.10	Conclusion	513
10.11	Exercises	513
	References	514
11	Galois Fields GF(pⁿ)	515
11.1	GF(p)	516
11.1.1	Modular Reduction	516
11.1.2	Inversion and Division	520
11.2	Addition and Subtraction Over GF(p ⁿ)	522
11.3	Product Over GF(p ⁿ) Using Power Representation	522
11.4	Product Over GF(p ⁿ) Using the Standard Base	523
11.4.1	Parallel Multiplication	525
11.4.2	Serial-Parallel Multiplication	527

11.4.3	Serial Multiplication	532
11.5	Multiplication Over $\text{GF}(p^m)$ Using the Normal Base	533
11.6	Multiplication Over $\text{GF}(p^m)$ Using the Dual Base	539
11.7	A^2 and A^p Over $\text{GF}(p^m)$	542
11.7.1	Square	543
11.7.2	A^p	544
11.8	Exponentiation Over $\text{GF}(p^m)$	544
11.9	Inversion and Division Over $\text{GF}(p^m)$	547
11.10	Operations Over $\text{GF}((p^n)^M)$	549
11.11	Conclusion	549
11.12	Exercises	549
	References	550
12	Two Galois Fields Cryptographic Applications	551
12.1	Introduction	551
12.2	Discrete Logarithm Based Cryptosystems	552
12.2.1	Fundamentals	552
12.2.2	A Real Example: $\text{GF}(2^{233})$	557
12.3	Elliptic Curve Cryptosystems	557
12.3.1	Fundamentals	557
12.3.2	A Real Example: $\text{GF}(2^{192} - 2^{64} - 1)$	562
12.4	Conclusion	564
12.5	Exercises	564
	References	564
	Appendix A: Finite or Galois Fields	567
	Appendix B Polynomial Algebra	575
	Appendix C Elliptic Curves	629
	Appendix D Errors	645
	Appendix E Algorithms for Function Approximation	655
	Index	673