Intelligent Systems Reference Library

Volume 201

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

Springer

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

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. **LFSR**s (**L**inear **F**eedback **S**hift **R**egisters) and **CA**s (**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 **LFSR**s 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 GF(p) are introduced in this chapter, since modular operations for prime values of p have to be implemented in 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 redundance 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 **LFSR**s, 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 **CA**s studied in this chapter are mainly one-dimensional and linear, although two-dimensional **CA**s are also defined.

Chapter 10 is devoted to the Galois fields 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 GF($(2^n)^m$) are detailed.

Chapter 11 is parallel to Chap. 10, but refers to Galois fields GF(p^n) and 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 GF(2^{233}) is used. The second is devoted to elliptic curves, and as a real example, the Galois field 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