Embedded Systems Design with Special Arithmetic and Number Systems

Amir Sabbagh Molahosseini
Leonel Seabra de Sousa • Chip-Hong Chang
Editors

Embedded Systems Design with Special Arithmetic and Number Systems

Springer

Editors
Amir Sabbagh Molahosseini
Department of Computer Engineering
Islamic Azad University, Kerman Branch
Kerman, Iran

Leonel Seabra de Sousa
INESC-ID, Instituto Superior Técnico
Universidade de Lisboa
Lisboa, Portugal

Chip-Hong Chang
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore, Singapore

ISBN 978-3-319-49741-9 ISBN 978-3-319-49742-6 (eBook)
DOI 10.1007/978-3-319-49742-6

Library of Congress Control Number: 2017934074

Printed on acid-free paper

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

Preface

For decades, innovation in the chip industry has been predominantly driven by the demand of personal computers (PCs). The central processing unit (CPU), which is the brain of a PC, is built from fundamental devices that follow a miniaturization path in close agreement with Moore's Law. Fifty years after the integrated circuit (IC) invention, the remarkable success in device geometry extrapolation and the seductive growth of chip content have changed the landscape of the platform of computing. New nano-/biocircuits and systems have emerged to take advantage of the increased integration density and connectivity to enhance living and lifestyles. The PC's influence on chip design is gradually eroded by the proliferation of connected mobile and portable devices due to the growth of consumer web and services of all types being made online and on demand. Tablets and mobile phones have overtaken the consumer market of desktops and laptops, and embedded systems permeate every aspect of work and life.

The new age of ubiquitous computing brings multifaceted challenges of versatility, portability, environmental friendliness, computational heterogeneity, and methodological pluralism into the design of embedded systems. It is time for a radical change in the algorithm and architecture of embedded system design to effect innovative solutions to the nascent multivariate optimization problems with new design constraints. Ironically, after more than 40 years of enormous R&D investment into renewing almost every relevant technology for IC design and manufacturing, the fundamental arithmetic operations and algebraic structures used in the prevalent embedded systems are still based on the same conventional weighted binary number representation inherited from the earliest microprocessor design. It is well understood that the way numbers are represented in a digital system has an impact on all levels of design abstraction from algorithm and architecture to circuit topology and layout. The choice of number systems influences the workload of an application by determining the number and complexity of operations required to accomplish a specific task. Since data activities depend on circuit topologies and stochastic properties of the inputs, the representation of data has a direct effect on the operator strength and the performance predictability.

Embedded systems implemented by algorithms based on the weighted binary number system suffer from the curse of dimensionality due to the inevitable long chain of carry propagation. It has limited "parallelism" and "modularity" to fully utilize the emerging VLSI technology on optimization of essential hardware attributes. Higher radix weighted number systems have reduced the word length of operations, and non-weighted number systems can limit the inter-digit carry propagation. Some alternative number systems inherently possess greater parallelism and sparser inter-digit communication amenable to speed enhancement and power reduction in a multi-ALU system and remain advantageous to layout and routing for the current and emerging 3D stacked IC technology. The design space of arithmetic functions based on different unconventional number systems and their potential have not been fully tapped. This book aims at overcoming issues and problems confronted by the use of different unconventional number systems to find a new avenue to sustain the continual design and development growth of the new generation of application-specific embedded systems.

Based on the chapter's content, we have divided the book into two parts. The first part is aimed to introduce the readers to the concepts, foundations, and design methods of circuits and systems for unconventional number systems including *residue number system*, *redundant number system*, *decimal floating-point number system*, and *continuous-valued number system*. Part two is dedicated to the applications of unconventional number systems in different areas of embedded system design from digital signal and image processing to emerging cryptographic algorithms. Chapter 1 introduces residue number systems and proposes a method to teach residue number systems in the context of embedded systems. Chapter 2 proposes a compact and scalable architecture for designing residue number system (RNS)-based programmable processors for general moduli sets. The design of an RNS processor has shown that performance and efficiency are improved by exploring the parallelism and carry-free characteristic of RNS.

The latest mathematical achievements in performing non-modular RNS operations using diagonal function are described in Chap. 3. Efficient implementation of non-modular RNS operations such as scaling, sign detection, magnitude comparison, and overflow detection could open the doors of general-purpose processors to RNS. Chapter 4 provides an overview of the principle of detecting, locating, and correcting single and multiple residue digit errors in arithmetic processing by redundant residue number system (RRNS) and highlights some applications that utilize RRNS codes. The location of erroneous residue digits is identified as the bottleneck operation for RRNS implementation. The complexity and latency of syndrome-based and CRT-based approaches are analyzed and compared. Inspired by the need for decimal floating-point numbers on computers, Chap. 5 presents efficient hardware implementations of a number of key arithmetic operations. It also discusses the intricacies of binary integer decimal and densely packed decimal encodings in migrating the designs from binary into decimal floating point and the functional verification approach to envisage future unified binary and decimal arithmetic units. Chapter 6 explores the design space of using redundant binary representation for high-performance Booth-encoded multiplier implementation.

It analyses the performance trade-offs of 21 different configurations of redundant binary multiplier architecture constructed from different binary to redundant binary encoding formats, different radices of binary, pseudo redundant binary and binary Booth encodings, and redundant binary to binary converters. Chapter 7 presents fundamentals of continuous-valued number system. The arithmetic operations in continuous-valued number system are performed using simple analog circuitry to provide arbitrary implementation precision. Potential applications of this number system are in the area of low noise and low cross-talk circuitry for arithmetic circuits used in mixed-signal systems and digitally assisted analog circuits. Chapter 8 reviews basic principles and hardware implementations of RNS-based digital signal processing (DSP) units by a team of researchers with 20 years of research experience in using RNS for DSP applications. They believe that RNS is promising with appropriate trade-offs between circuit parameters. The parallelism of RNS is advantageous in image processing applications where addition and multiplication are the dominant operations. This issue is comprehensively investigated in Chap. 9, where RNS-based realization of many important image processing applications such as edge detection, sharpening, smoothing, and wavelet processing is reviewed.

Chapter 10 introduces another unconventional number system called *logarithmic number system (LNS)*. This number system offers not only efficient multiplication but also division which is a difficult operation in both binary and residue number systems. It is shown that using LNS for FIR filter implementation can lead to significant saving in power consumption. Chapter 11 introduces canonical and extended double base number systems and the search algorithms for finding their minimum or quasi-minimum forms. Their applicability to efficient programmable FIR filter design is demonstrated by the direct mapping of these sparse double-based number representations into efficient time-multiplexed multiple-constant-multiplication architecture consisting of only adders, multiplexers, programmable shifters, and a lookup table. The results show that FIR filters designed with extended double base number system can reduce the logic complexity by up to 47.81 % and critical path delay by up to 14.32 % compared with the designs based on conventional binary number system. Chapter 12 addresses how RNS can be effectively used to design public-key cryptography systems. The design concepts, methodologies, and challenges of implementing RSA and elliptic curve public-key algorithms with residue arithmetic and security of RNS-based cryptosystems are presented and discussed in this chapter. Chapter 13 investigates the advantages of RNS arithmetic in *lattice-based cryptography*, an emerging cryptographic algorithm with post-quantum security. It is shown that the high parallelism of RNS is well suited to address the challenging problem of the efficient realization of this next-generation cryptographic algorithm. Finally, the last chapter introduces attractive applications of RNS in computer networks. In contrast to other applications, here RNS representation is used for routing, packet forwarding, and multicasting. Instead of using single regular large packet, distributive residues are used to achieve lower energy consumption of the sensor nodes and longer network lifetime.

To sum up, at the rate of growth of embedded processors and their increasing share and dominance in the consumer electronic markets, the university students

and professors, researchers, and industrial designers should be prepared for the bold and radical evolution of how future embedded systems will be designed. This book solicits alternative approaches to the design of efficient embedded systems effected by the change in the fundamental number representation for which digital arithmetic operations are performed. It is hoped that the comprehensive review, analysis, efficient implementation methods, and new applications covered in this book will stimulate and inspire more interesting applications, new developments, and exploration of these or other unconventional number systems.

Kerman, Iran — Amir Sabbagh Molahosseini
Lisboa, Portugal — Leonel Seabra de Sousa
Singapore, Singapore — Chip-Hong Chang

Contents