Guest Editors’ Introduction:
Special Issue on Computer Arithmetic

Michael J. Schulte, Member, IEEE, and Jean-Claude Bajard, Member, IEEE Computer Society

Computer arithmetic is one of the oldest research topics. Early civilizations used marked bones to memorize numerical values. This approach can be viewed as a combination of read only memories and a unary number system in which addition was very efficient. Around 3300 BC, the first true number systems appeared when Sumerian clay tablets were used to implement a radix-60 number system. A variation of this system is still used today when dealing with minutes and seconds. The basis of our current decimal number system originated during the sixth century in India and was later adopted in Europe during the 12th century.

As mankind continues to advance and new applications and technologies emerge, innovative research in computer arithmetic is essential. Important applications, including multimedia processing, cryptography, and computer graphics, all need novel arithmetic algorithms and hardware designs to satisfy stringent area, delay, and power requirements. Furthermore, advances in VLSI technology, innovations in tools for electronic design automation, and the advent of nanotechnology and quantum computing offer new opportunities for implementing complex algorithms in hardware.

This special issue presents recent high-quality research in computer arithmetic. The 12 papers included in this special issue were selected from 36 papers submitted in response to an open call for papers. This call for papers followed the 16th IEEE Symposium on Computer Arithmetic, which took place in Santiago de Compostella in June 2003. Each paper received at least three reviews and the top papers were selected for inclusion in this special issue. Six papers are expanded versions of the papers presented at the 16th IEEE Symposium on Computer Arithmetic, three are expanded versions of papers presented at other conferences, and three are original contributions. The papers in the special issue are grouped into four categories: number systems, multiplication and division, elementary functions, and cryptography.

Number systems are an important research topic since they form the basis of computer arithmetic. In the 21st century, new number systems are needed that are well-suited to emerging technologies and applications. In the paper “Addition Related Arithmetic Operations via

- M.J. Schulte is with the University of Wisconsin-Madison, Madison, WI 53706. E-mail: schulte@engr.wisc.edu.
- J.-C. Bajard is with LIRMM CNRS, University of Montpellier II, 34392 Montpellier cedex 5, France. E-mail: Jean-Claude.Bajard@lirmm.fr.

Published online 18 Jan. 2005.
For information on obtaining reprints of this article, please send e-mail to: tc@computer.org.

0018-9340/05/$20.00 © 2005 IEEE
polynomial. In the paper “Multipartite Table Methods,” Florent de Dinechin and Arnaud Tisserand provide a unified view of previous function approximation techniques that use table lookup and addition. Their unified view enables a wider design space exploration of these methods and leads to tables that are up to 50 percent smaller than the best tables previously published. In the paper “A New Range-Reduction Algorithm,” Nicolas Brisebarre, David Defour, Peter Kornerup, Jean-Michel Muller, and Nathalie Revol introduce an algorithm for range reduction that is fast for input arguments belonging to the most common domains, yet accurate over the full range of double-precision numbers. Accurate range reduction is important since most elementary function evaluation techniques are efficient over a small domain. In the paper “Searching Worst Cases of a One-Variable Function Using Lattice Reduction,” Damien Stehlé, Vincent Lefèvre, and Paul Zimmermann propose a novel algorithm to find the worst case inputs for correct rounding of a given mathematical function. Their algorithm has lower complexity than previous algorithms and facilitates the design of efficient elementary function libraries that guarantee correct rounding. In the paper “High-Throughput CORDIC-Based Geometry Operations for 3D Computer Graphics,” Tomás Lang and Elisardo Antelo present the formulation of useful 3D computer graphics operations in terms of CORDIC-type primitives. They also give an overview of a stream processor that uses CORDIC-type modules to implement graphic operations and compare their design to current implementations.

New algorithms and architectures for cryptography are needed due to the growing importance of information security and the need to transmit secure information at very high speeds. Techniques for public key cryptography often perform operations on very large integers or large finite fields. In the paper “Five, Six, and Seven-Term Karatsuba-Like Formulas,” Peter L. Montgomery describes new techniques for multiplying polynomials in subquadratic time. These techniques can be used recursively to facilitate multiplication of high degree polynomials, which is an important operation in elliptic curve cryptography. In the paper “A Class of Unidirectional Bit Serial Systolic Architectures for Multiplicative Inversion and Division over GF(2^n),” Amir K. Daneshbeh and M. Anwar Hasan propose systolic architectures for finite field arithmetic that use both triangular and polynomial basis representations. These architectures are free of carry propagation and suitable for hardware implementations for which the dimension of the field is large and may vary.

We thank all of the authors who submitted to this special issue, including the authors whose submissions could not be included. We are very grateful to the anonymous reviewers for their thorough and timely evaluation of the manuscripts. Special thanks are due to the Editor-in-Chief, Viktor Prasanna, for hosting this special issue on Computer Arithmetic. We warmly thank Suzanne Werner and Joyce Arnold for providing much needed staff support.

Michael J. Schulte
Jean-Claude Bajard
Guest Editors