Guest Editors' Introduction: Special Section on Computer Arithmetic

Elisardo Antelo, David Hough, *Member*, *IEEE*, and Paolo Ienne, *Member*, *IEEE*

COMPUTER Arithmetic is a field that deals with the hardware/software design, implementation and verification of numerical algorithms, definition of new number systems and standardization of arithmetic systems for computers. It is an interdisciplinary field that draws upon mathematics, computer science and electrical engineering. Advances in this field span from highly theoretical (for instance, new exotic number systems) to highly practical (for instance, new floating-point units for microprocessors).

Computer Arithmetic is more than ever a hot topic of research with a strong industrial impact. We are now in the era of massive parallelism in processors, with dominant workloads oriented to throughput computing (multicore microprocessors, GPGPU's and FPGA accelerators). In this scenario, a massive amount of arithmetic resources are incorporated in processor engines, with the goal of maximizing the number of operations per watt and per square millimeter. This requires deep innovation in the design of new arithmetic units. For instance, it is estimated that in the near future a high performance GPGPU may have over 5000 floating-point units. Moreover, these systems will incorporate several specialized engines to provide power-efficient processing for specific tasks (cryptography, multimedia, network processing, etc). Additionally, mobile and embedded systems have extreme restrictions in terms of cost (area) and power (and energy), but at the same time require increasingly higher levels of arithmetic processing due to the sophistication of the algorithms implemented. On the other hand, recently a new version of the standard for floating-point arithmetic was released (IEEE Standard 754-2008), that includes new specifications that will require hard research efforts for its implementation in future microprocessor (for instance the decimal floating-point arithmetic specification). Formal verification and fault tolerance are also increasingly important in the context of highly dependable systems.

Since 1969 the IEEE Symposium on Computer Arithmetic is the premier international event for computer arithmetic research. The last was the 20th edition of the conference (held every two years since 1981), and it took place in Tübingen in July 2011. After the conference, an open call for papers (for extended versions of the conference papers and for new papers) was released for this special section on Computer Arithmetic. A total of 27 papers were submitted that received a total of 130 expert reviews, each paper receiving at least three reviews and most receiving at least four. Two rounds of reviews led to the selection of just four papers for this special section. The specific topics covered by these papers are the design of functional units for microprocessors, design of functional units for cryptography, floating-point decimal arithmetic and new number systems.

Division and square root are very important primitives that are usually implemented in hardware. Although less frequent than addition and multiplication, the higher latency and very low throughput of these operations sometimes result in a significant performance bottleneck. One approach to improve latency is the use of a higher radix in digit-by-digit algorithms but power and energy might be an issue. The paper, "Power Efficient Division and Square Root Unit," by Wei Liu and Alberto Nannarelli presents a combined radix-16 digit-by-digit division and square root unit based on the overlap of two radix-4 units. The authors show that this is a power-efficient design competitive with current industrial implementations, even with those based on multiplicative methods.

Modular exponentiation of large integers is a key operation for cryptography with high computational demand. Montgomery exponentiation is a popular implementation choice. The paper "An Algorithmic and Architectural Study on Montgomery Exponentiation in RNS," by Filippo Gandino, Fabrizio Lamberti, Gianluca Paravati, Jean-Claude Bajard, and Paolo Montuschi, presents a deep exploration of the design space, both at the algorithm and architecture level, for its implementation using the Residue Number System. New optimizations are introduced that lead to more efficient cryptography hardware implementations.

Decimal Floating-point Arithmetic (DFP) is now part of the IEEE Standard 754-2008 for floating-point arithmetic. Two approaches are being followed by industry: direct hardware implementation and software emulation. Direct computation of DFP operations with binary hardware leads to errors with strong practical and even legal implications, mostly related to the financial system. Emulation of DFP is a must for platforms with only hardware support for binary floating-point arithmetic. However, emulation might be a slow alternative for some applications. The paper "On basic financial decimal operations on binary machines," by

- *E. Antelo is with the Departamento de Electrónica e Computación, Universidade de Santiago de Compostela, 15706 Santiago de Compostela, Spain. E-mail: elisardo.antelo@usc.es.*
- *D. Hough is with Oracle Corporation, 4180 Network Circle, Santa Clara, CA 95054. E-mail: david.hough@oracle.com.*
- *P. Ienne is with École Polytechnique Fédérale de Lausanne (EPFL), School of Computer and Communication Sciences, 1015 Lausanne, CH-Switzerland. E-mail: paolo.ienne@epfl.ch.*

For information on obtaining reprints of this paper, please send e-mail to: tc@computer.org.

0018-9340/12/$31.00 © 2012 IEEE Published by the IEEE Computer Society

Abhilasha Aswal, M. Ganesh Perumal, and G.N. Srinivasa Prasanna, performs a deep analysis of errors that are introduced when binary arithmetic is used directly to implement DFP. A novel software approach for DFP is derived based on binary arithmetic with table-based error correction. This might be a faster alternative than emulation for implementing DFP.

"Fast arithmetical algorithms in Möbius number systems," by Petr Kůrka explores an entirely different method of representing real numbers. Asymptotic efficiency of these methods is measured by the "transaction quotient". The author describes methods with smaller transaction quotients than either conventional positional number representations or previously known Möbius systems. Can these asymptotic efficiencies translate into useful advantages for realistic problems? Time will tell. Research papers that probe the fundamental assumptions of our discipline shed new light on those assumptions.

On behalf of every reader of our published papers, the guest editors would like to thank all the authors who submitted papers and labored to respond to reviewers' suggestions, all the anonymous reviewers who evaluated submissions and suggested improvements, the Editor in Chief Professor Albert Zomaya, and the entire staff of *IEEE Transactions on Computers* who oversaw the whole process.

Elisardo Antelo
David Hough
Paolo Ienne
Guest Editors

Elisardo Antelo graduated with a degree in physics in 1991 and received the PhD in computer engineering in 1995 from the University of Santiago de Compostela, Spain. In 1992, he joined the Departamento de Electronica e Computacion at the University of Santiago de Compostela. From 1992 to 1998, he was an assistant professor and since 1998 he has been a tenured associate professor in this department. He was a research visitor at the University of California at Irvine several times between 1996 and 2000. Dr. Antelo is a member of the Computer Architecture group at the University of Santiago de Compostela. Since 2001, he has been involved in the program committee of the IEEE Symposium on Computer Arithmetic (program cochair in the 2011 edition). He also was involved with the program committees of the Real Numbers and Computers Conference since 2006 and EUROSIPCO since 2008. He is associate editor of the *IEEE Transactions on Computers* (since 2007), and of Integration, the *VLSI Journal* (since 2011). His primary research and teaching interest are in digital design and computer architecture with current emphasis on high-speed and low-power numerical processors, application-specific modules, computer arithmetic and design issues related to multicore processors.

David Hough is a graduate of Carleton College, with a BA in astronomy in 1968. He received the PhD in computer science in 1977 from the University of California. After working at Tektronix and Apple Computer, he joined Sun Microsystems in 1984, as a distinguished engineer since 1989. In 2010, Sun became part of Oracle Corporation, where he is now a senior principal software engineer, working in the areas of software and hardware support for numerical computation. In 1978, he became active in the P754 standardization effort for microprocessor arithmetic, which resulted in the ANSI/IEEE 754-1985 Standard for Binary Floating-Point Arithmetic and the ANSI/IEEE 854-1987 Standard for Radix-Independent Floating-Point Arithmetic. Likewise, beginning in 2000, he served in the effort to produce the revised ANSI/IEEE 754-2008 Standard for Floating-Point Arithmetic. He has served on the program committees for the IEEE Symposia on Computer Arithmetic since 1998. He is a member of the IEEE and the IEEE Computer Society.

Paolo Ienne has been a professor at the École Polytechnique Fédérale de Lausanne (EPFL) since 2000 and heads the Processor Architecture Laboratory (LAP). Prior to that, from 1990 to 1991, he was an undergraduate researcher with Brunel University, Uxbridge, United Kingdom. From 1992 to 1996, he was a research assistant at the Microcomputing Laboratory (LAMI) and at the MANTRA Center for Neuro-Mimetic Systems of the EPFL. In December, 1996, he joined the Semiconductors Group of Siemens AG, Munich, Germany (which later became Infineon Technologies AG). After working on datapath generation tools, he became head of the embedded memory unit in the Design Libraries division. Ienne was a recipient of the Best Paper Award at the 40th Design Automation Conference (DAC) in 2003, at the International Conference on Compilers, Architectures, and Synthesis for Embedded Systems (CASES) in 2007, at the 19th International Conference on Field-Programmable Logic and Applications (FPL) in 2009, and at the 20th ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA) in 2012. In 2008, he has been general cochair of the 6th IEEE Symposium on Application Specific Processors (SASP) and guest editor of a special section on application specific processors which appeared in October 2008 on the *IEEE Transactions on Very Large Scale Integration Systems*. In 2010, he has been the program subcommittee chair of the Design Automation Conference (DAC) on High-Level and Logic Synthesis. From 2010 to 2012, he was a topic cochair of Design Automation and Test in Europe (DATE) for the Architectural and High-Level Synthesis topic. In 2011, he was a program cochair of the 20th IEEE Symposium on Computer Arithmetic (ARITH) and a program cochair of the 22nd IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP). He is or has been a member of some fifty program committees of international workshops and conferences in the areas of design automation, computer architecture, embedded systems, compilers, FPGAs, and asynchronous design. Since 2011, he has been an associate editor of *ACM Transactions on Design Automation of Electronic Systems (TODAES)*. His research interests include various aspects of computer and processor architecture, electronic design automation, computer arithmetic, FPGAs and reconfigurable computing, and multiprocessor systems-on-chip. He is a member of the IEEE and the IEEE Computer Society.