2017 IEEE 24th Symposium on Computer Arithmetic (ARITH 2017)

London, United Kingdom
24 – 26 July 2017

IEEE

IEEE Catalog Number: CFP17121-POD
ISBN: 978-1-5386-1966-7

IEEE Catalog Number:	CFP17121-POD
ISBN (Print-On-Demand):	978-1-5386-1966-7
ISBN (Online):	978-1-5386-1965-0
ISSN:	1063-6889

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2017 IEEE 24th Symposium on Computer Arithmetic

ARITH 2017

Table of Contents

Foreword viii

Committees x

Program Committee Members xi

Steering Committee xii

Session 1: Keynote Talk 1

The Rise of Multiprecision Arithmetic 1
Nicholas John Higham

Session 2: Multiprecision Arithmetic

Multiple Precision Floating-Point Arithmetic on SIMD Processors 2
Joris van der Hoeven

Multiprecision Multiplication on ARMv8 10
Zhe Liu, Kimmo Järvinen, Weiqiang Liu, and Hwajeong Seo

Optimized Binary64 and Binary128 Arithmetic with GNU MPFR 18
Vincent Lefèvre and Paul Zimmermann

Implementation and Performance Evaluation of an Extended Precision Floating-Point Arithmetic Library for High-Accuracy Semidefinite Programming 27
Mioara Joldes, Jean-Michel Muller, and Valentina Popescu

Session 3: Algorithms

A Parallel Method for the Computation of Matrix Exponential Based on Truncated Neumann Series 35
Vassil Dimitrov, Viduneth Ariyarathna, Diego F. G. Coelho, Logan Rakai, Arjuna Madanayake, and Renato J. Cintra

On Lifting-Based Fixed-Point Complex Multiplications and Rotations 43
Oscar Gustafsson

A Number System Approach for Adder Topologies 50
Alvaro Vázquez and Elisardo Antelo

Session 4 — Special Session: Computer Arithmetic and DSP

On Improving the Performance Per Area of ASTC with a Multi-output Decoder 58
Kenneth C. Rovers and Sam Elliott

Optimal Streamed Linear Permutations 60
François Serre and Markus Püschel

Approximate Neumann Series or Exact Matrix Inversion for Massive MIMO? 62
Oscar Gustafsson, Erik Bertilsson, Johannes Klasson, and Carl Ingemarsson

Floating Point Tangent Implementation for FPGAs 64
Martin Langhammer and Bogdan Pasca

Session 5: Floating-Point Error Analysis

The Classical Relative Error Bounds for Computing Sqrt(a^2 + b^2) and c / sqrt(a^2 + b^2) in Binary Floating-Point Arithmetic are Asymptotically Optimal 66
Claude-Pierre Jeannerod, Jean-Michel Muller, and Antoine Plet

Certified Roundoff Error Bounds Using Bernstein Expansions and Sparse Krivine-Stengle Representations 74
Alexandre Rocca, Victor Magron, and Thao Dang

Round-off Error Analysis of Explicit One-Step Numerical Integration Methods 82
Sylvie Boldo, Florian Faissole, and Alexandre Chapoutot

ULPs and Relative Error 90
Marius Cornea

Session 6: Hardware for Fast and Reproducible Arithmetic

High-Precision Anchored Accumulators for Reproducible Floating-Point Summation 98
David Raymond Lutz and Christopher Neal Hinds

Modified Fused Multiply and Add for Exact Low Precision Product Accumulation 106
Nicolas Brunie

A Hardware Accelerator for Computing an Exact Dot Product 114
Jack Koenig, David Biancolin, Jonathan Bachrach, and Krste Asanovic

Session 7: Keynote Talk 2

Large Scale Numerical Simulations of the Climate 122
Jean-Christophe Rioual

Session 8: Arithmetic in FPGAs

Flexible Fixed-Point Function Generation for FPGAs 123
Matei Iştoan and Bogdan Pasca

Resource Optimal Design of Large Multipliers for FPGAs 131
Martin Kumm, Johannes Kappauf, Matei Istoan, and Peter Zipf

Session 9 — Special Session: Realizing Efficient Matrix Computations

Accelerating Matrix Processing with GPUs 139
Nicholas Malaya, Shuai Che, Joseph L. Greathouse, René van Oostrum, and Michael J. Schulte

Algorithms and Arithmetic: Choose Wisely 142
George Anthony Constantinides

Optimizing Matrix Multiplication on Intel® Xeon Phi TH x200 Architecture 144
Murat Efe Guney, Kazushige Goto, Timothy B. Costa, Sarah Knepper, Louise Huot, Arthur Mitrano, and Shane Story

QRD for Parallel Arithmetic Structures 146
Martin Langhammer

Session 10: Cryptography

Fast Arithmetic Modulo 2^x p^y ± 1 148
Joppe W. Bos and Simon Friedberger

Efficient Leak Resistant Modular Exponentiation in RNS 156
Andrea Lesavourey, Christophe Negre, and Thomas Plantard

A New Multiplicative Inverse Architecture in Normal Basis Using Novel Concurrent Serial Squaring and Multiplication 164
Amin Monfared, Hayssam El-Razouk, and Arash Reyhani-Masoleh

Session 11: Miscellaneous Topics in Computer Arithmetic

A Sum Error Detection Scheme for Decimal Arithmetic 172
Alvaro Vazquez and Elisardo Antelo

Reliable Verification of Digital Implemented Filters Against Frequency Specifications 180
Anastasia Volkova, Christoph Lauter, and Thibault Hilaire

Normalizing or Not Normalizing? An Open Question for Floating-Point Arithmetic in Embedded Systems 188
Sonia Gonzalez-Navarro and Javier Hormigo

Author Index 196