

2011 20th IEEE Symposium on Computer Arithmetic

(ARITH 2011)

Tuebingen, Germany
25-27 July 2011



IEEE Catalog Number: CFP11121-PRT
ISBN: 978-1-4244-9457-6

2011 20th IEEE Symposium on Computer Arithmetic

ARITH-20

Table of Contents

Foreword.....	ix
Dedication.....	x
Steering Committee.....	xv
Symposium Committee.....	xvi
Program Committee.....	xvii
Additional Reviewers.....	xviii
Corporate Sponsors.....	xix

Session 1: Keynote Talk

Chair: Eric Schwarz and Vojin G. Oklobdzija

High Intelligence Computing: The New Era of High Performance Computing	3
<i>Ralf Fischer</i>	

Session 2: Multiple-Precision Algorithms

Chair: Marius Cornea

Short Division of Long Integers	7
<i>David Harvey and Paul Zimmermann</i>	
High Degree Toom'n'Half for Balanced and Unbalanced Multiplication	15
<i>Marco Bodrato</i>	
Augmented Precision Square Roots and 2-D Norms, and Discussion on Correctly Rounding $\sqrt{x^2+y^2}$	23
<i>Nicolas Brisebarre, Mioara Joldeş, Peter Komerup, Érik Martin-Dorel, and Jean-Michel Muller</i>	

Session 3: Transcendental Methods

Chair: Naofumi Takagi

Towards a Quaternion Complex Logarithmic Number System	33
<i>Mark G. Arnold, John Cowles, Vassilis Paliouras, and Ioannis Kouretas</i>	
ROM-less LNS	43
<i>R. Che Ismail and J. N. Coleman</i>	

Composite Iterative Algorithm and Architecture for q -th Root Calculation	52
<i>Álvaro Vázquez and Javier D. Bruguera</i>	
On the Fixed-Point Accuracy Analysis and Optimization of FFT Units with CORDIC Multipliers	62
<i>Omid Sarbishei and Katarzyna Radecka</i>	

Session 4: Special Session on Industrial Practices

Chair: Mike Schulte

Self Checking in Current Floating-Point Units	73
<i>Daniel Lipetz and Eric Schwarz</i>	
How to Square Floats Accurately and Efficiently on the ST231 Integer Processor	77
<i>Claude-Pierre Jeannerod, Jingyan Jourdan-Lu, Christophe Monat, and Guillaume Revy</i>	
A 1.5 Ghz VLIW DSP CPU with Integrated Floating Point and Fixed Point Instructions in 40 nm CMOS	82
<i>Timothy Anderson, Duc Bui, Shriram Moharil, Soujanya Namur, Mujibur Rahman, Anthony Lell, Eric Biscondi, Ashish Shrivastava, Peter Dent, Mingjian Yan, and Hasan Mahmood</i>	
The POWER7 Binary Floating-Point Unit	87
<i>Maarten Boersma, Michael Kröner, Christophe Layer, Petra Leber, Silvia M. Müller, and Kerstin Schelm</i>	

Session 5: Addition

Chair: Alberto Nannarelli

Accelerating Computations on FPGA Carry Chains by Operand Compaction	95
<i>Thomas B. Preußner, Martin Zabel, and Rainer G. Spallek</i>	
Fast Ripple-Carry Adders in Standard-Cell CMOS VLSI	103
<i>Neil Burgess</i>	
A Family of High Radix Signed Digit Adders	112
<i>Saeid Gorgin and Ghassem Jaberipur</i>	

Session 6: Floating-Point Units

Chair: Javier Bruguera

Fused Multiply-Add Microarchitecture Comprising Separate Early-Normalizing Multiply and Add Pipelines	123
<i>David R. Lutz</i>	
Latency Sensitive FMA Design	129
<i>Sameh Galal and Mark Horowitz</i>	
The IBM zEnterprise-196 Decimal Floating-Point Accelerator	139
<i>Steven Carlough, Adam Collura, Silvia Mueller, and Michael Kroener</i>	

Session 7: Division, Square-Root and Reciprocal Square-Root

Chair: Peter Kornerup

Radix-8 Digit-by-Rounding: Achieving High-Performance Reciprocals, Square Roots, and Reciprocal Square Roots	149
<i>J. Adam Butts, Ping Tak Peter Tang, Ron O. Dror, and David E. Shaw</i>	
Tight Certification Techniques for Digit-by-Rounding Algorithms with Application to a New $1/\sqrt{x}$ Design	159
<i>Ping Tak Peter Tang, J. Adam Butts, Ron O. Dror, and David E. Shaw</i>	
Radix-16 Combined Division and Square Root Unit	169
<i>Alberto Nannarelli</i>	
A Prescale-Lookup-Postscale Additive Procedure for Obtaining a Single Precision Ulp Accurate Reciprocal	177
<i>David W. Matula and Mihai T. Panu</i>	

Session 8: Special Session on High Performance Arithmetic for FPGA's

Chair: Martin Langhammer

Teraflop FPGA Design	187
<i>Martin Langhammer</i>	
The Arithmetic Operators You Will Never See in a Microprocessor	189
<i>Florent de Dinechin</i>	
Accelerating Large-Scale HPC Applications Using FPGAs	191
<i>Rob Dimond, Sébastien Racanière, and Oliver Pell</i>	

Session 9: Arithmetic Algorithms for Cryptography

Chair: David Matula

A General Approach for Improving RNS Montgomery Exponentiation Using Pre-processing	195
<i>Filippo Gandino, Fabrizio Lamberti, Paolo Montuschi, and Jean-Claude Bajard</i>	
Bit-Sliced Binary Normal Basis Multiplication	205
<i>Billy Bob Brumley and Dan Page</i>	
Efficient SIMD Arithmetic Modulo a Mersenne Number	213
<i>Joppe W. Bos, Thorsten Kleinjung, Arjen K. Lenstra, and Peter L. Montgomery</i>	

Session 10: Tools for Formal Certified Code

Chair: Martin Schmookler

Automatic Generation of Code for the Evaluation of Constant Expressions at Any Precision with a Guaranteed Error Bound	225
<i>Sylvain Chevillard</i>	
Automatic Generation of Fast and Certified Code for Polynomial Evaluation	233
<i>Christophe Moulleron and Guillaume Revy</i>	
Flocq: A Unified Library for Proving Floating-Point Algorithms in Coq	243
<i>Sylvie Boldo and Guillaume Melquiond</i>	
Author Index	253