

2009 19th IEEE International Symposium on Computer Arithmetic

(ARITH 2009)

**Portland, Oregon, USA
8-10 June 2009**



**IEEE Catalog Number: CFP09121-PRT
ISBN: 978-1-4244-4329-1**

2009 19th IEEE International Symposium on Computer Arithmetic

ARITH 2009

Table of Contents

Keynote Talk

Anton: A Specialized Machine for Millisecond-Scale Molecular Dynamics Simulations of Proteins	3
<i>David E. Shaw</i>	

Session 1: Algorithms and Number Systems

Efficient Data Structure and Algorithms for Sparse Integers, Sets and Predicates	7
<i>Jean E. Vuillemin</i>	
A Dual-Purpose Real/Complex Logarithmic Number System ALU	15
<i>Mark G. Arnold and Sylvain Collange</i>	
Selected RNS Bases for Modular Multiplication	25
<i>J. C. Bajard, M. Kaihara, and T. Plantard</i>	

Invited Talk

A Historical Perspective on Computer Arithmetic	35
<i>Stanley Mazor</i>	

Session 2: Arithmetic Hardware

Higher Radix Squaring Operations Employing Left-to-Right Dual Recoding	39
<i>David W. Matula</i>	
Advanced Clockgating Schemes for Fused-Multiply-Add-Type Floating-Point Units	48
<i>Jochen Preiss, Maarten Boersma, and Silvia Melitta Mueller</i>	
Unified Approach to the Design of Modulo-($2^n \pm 1$) Adders Based on Signed-LSB Representation of Residues	57
<i>Ghassem Jaberipur and Behrooz Parhami</i>	

Session 3: Finite Fields and Cryptography

Subquadratic Space Complexity Multiplier for a Class of Binary Fields Using Toeplitz Matrix Approach	67
<i>M. A. Hasan and C. Nègre</i>	
Hybrid Binary-Ternary Joint Form and Its Application in Elliptic Curve Cryptography	76
<i>Jithra Adikari, Vassil Dimitrov, and Laurent Imbert</i>	
Polynomial Multiplication over Finite Fields Using Field Extensions and Interpolation	84
<i>Murat Cenk, Cetin Kaya Koc, and Ferruh Ozbudak</i>	

Session 4: Mathematical Software

A New Binary Floating-Point Division Algorithm and Its Software Implementation on the ST231 Processor	95
<i>Claude-Pierre Jeannerod, Herve Knochel, Christophe Monat, Guillaume Revy, and Gilles Villard</i>	
Fast and Accurate Bessel Function Computation	104
<i>John Harrison</i>	
Implementation Specific Verification of Divide and Square Root Instructions	114
<i>Elena Guralnik, Ariel J. Birnbaum, Anatoly Koyfman, and Avi Kaplan</i>	

Session 5: Decimal Hardware

A Decimal Floating-Point Adder with Decoded Operands and a Decimal Leading-Zero Anticipator	125
<i>Liang-Kai Wang and Michael J. Schulte</i>	
A High-Performance Significand BCD Adder with IEEE 754-2008 Decimal Rounding	135
<i>Álvaro Vázquez and Elisardo Antelo</i>	
Fully Redundant Decimal Arithmetic	145
<i>Saeid Gorgin and Ghassem Jaberipur</i>	

Session 6: Floating-Point Techniques

On the Computation of Correctly-Rounded Sums	155
<i>P. Kornerup, V. Lefevre, N. Louvet, and J.M. Muller</i>	
Multi-operand Floating-Point Addition	161
<i>Alexandre F. Tenca</i>	
Certified and Fast Computation of Supremum Norms of Approximation Errors	169
<i>Sylvain Chevillard, Mioara Joldes, and Christoph Lauter</i>	

Session 7: Decimal Transcendentals

Computation of Decimal Transcendental Functions Using the CORDIC Algorithm	179
<i>Álvaro Vázquez, Julio Villalba, and Elisardo Antelo</i>	
Decimal Transcendentals via Binary	187
<i>John Harrison</i>	
A 32-bit Decimal Floating-Point Logarithmic Converter	195
<i>Dongdong Chen, Yu Zhang, Younhee Choi, Moon Ho Lee, and Seok-Bum Ko</i>	

Special Session on Automated Synthesis of Arithmetic Operations

Datapath Synthesis for Standard-Cell Design	207
<i>Reto Zimmermann</i>	
Design Space Exploration for Power-Efficient Mixed-Radix Ling Adders	212
<i>Chung-Kuan Cheng</i>	
Challenges in Automatic Optimization of Arithmetic Circuits	213
<i>Ajay K. Verma, Philip Brisk, and Paolo Ienne</i>	

Panel on Decimal Arithmetic in Industry

Energy and Delay Improvement via Decimal Floating Point Units	221
<i>Hossam A. H. Fahmy, Ramy Raafat, Amira M. Abdel-Majeed, Rodina Samy, Tarek ElDeeb, and Yasmin Farouk</i>	
IEEE 754-2008 Decimal Floating-Point for Intel® Architecture Processors	225
<i>Marius Cornea</i>	

Special Session on Interval Arithmetic

IEEE Interval Standard Working Group - P1788: Current Status	231
<i>William Edmonson and Guillaume Melquiond</i>	

Author Index