

# Table of Contents

Dedication .....	ii
Forward.....	v
Symposium Committee .....	vi
List of Referees .....	vii
Previous IEEE Symposia on Computer Arithmetic .....	viii
Keynote Speaker: Andrew D. Booth.....	ix

## Number Systems

**Chair: N. Burgess, Brunel University**

An Accurate LNS Arithmetic Unit Using Interleaved Memory Function Interpolator .....	2
<i>D.M. Lewis</i>	
An Underflow-Induced Graphics Failure Solved by SLI Arithmetic .....	10
<i>D.W. Lozier</i>	
Complex SLI Arithmetic: Representation, Algorithms, and Analysis .....	18
<i>P.R. Turner</i>	

## Residue Arithmetic

**Chair: Magdy Bayoumi, University of Southwestern Louisiana**

Combined System-Level Redundancy and Modular Arithmetic for Fault Tolerant Digital Signal Processing.....	28
<i>W.K. Jenkins, B.A. Schnauffer, and A.J. Mansen</i>	
Adaptive Beamforming Using RNS Arithmetic .....	36
<i>B.J. Kirsch and P.R. Turner</i>	
Integer Mapping Architectures for the Polynomial Ring Engine .....	44
<i>S.S. Bizzan, G.A. Jullien, N.M. Wigley, and W.C. Miller</i>	

## Multipliers and Dot Products

**Chair: Naofumi Takagi, Kyoto University**

$n \times n$ Carry-Save Multipliers Without Final Addition .....	54
<i>P. Montuschi and L. Ciminiera</i>	
Design of a Fast Validated Dot Product Operation.....	62
<i>M. Daumas and D.W. Matula</i>	
Multi-Parallel Convolvers.....	70
<i>L. Dadda, V. Piuri, and R. Stefanelli</i>	

## Division and Square Root

**Chair: Ted E. Williams, HAL Computer Systems**

New Algorithms and VLSI Architectures for SRT Division and Square Root.....	80
<i>S.E. McQuillan, J.V. McCanny, and R. Hamill</i>	
Division with Speculation of Quotient Digits.....	87
<i>J. Cortadella and T. Lang</i>	
Measuring the Accuracy of ROM Reciprocal Tables .....	95
<i>D.D. Sarma and D.W. Matula</i>	

Hardware Starting Approximation for the Square Root Operation.....	103
<i>E.M. Schwarz and M.J. Flynn</i>	
Very High Radix Division with Selection by Rounding and Prescaling .....	112
<i>M.D. Ercegovac, T. Lang, and P. Montuschi</i>	
<b>Elementary Function Evaluation</b>	
<b>Chair: D.M. Matula, SMU</b>	
Efficient Complex Matrix Transformations with CORDIC.....	122
<i>N.D. Hemkumar and J.R. Cavallaro</i>	
Floating Point Cordic.....	130
<i>G.J. Hekstra and E.F.A. Deprettiere</i>	
Exact Rounding of Certain Elementary Functions .....	138
<i>M. Schulte and E. Swartzlander</i>	
BKM: A New Hardware Algorithm for Complex Elementary Functions .....	146
<i>J.-C. Bajard, S. Kla, and J.-M. Muller</i>	
<b>Arithmetic Processor Design</b>	
<b>Chair: Simon Knowles, INMOS</b>	
The Gauss Machine: A Galois-Enhanced Quadratic Residue Number System Systolic Array.....	156
<i>J.D. Mellott, J.C. Smith, and F.J. Taylor</i>	
A 17 X 69 Bit Multiply and Add Unit with Redundant Binary Feedback and Single Cycle Latency .....	163
<i>W.S. Briggs and D.W. Matula</i>	
The Design of a 64-Bit Integer Multiplier/Divider Unit .....	171
<i>D. Eisig, J. Rotstain, and I. Koren</i>	
<b>Algorithms</b>	
<b>Chair: Peter Kornerup, Odense University</b>	
Comparing Several GCD Algorithms .....	180
<i>T. Jebelean</i>	
Fast Evaluation of Polynomials and Inverses of Polynomials .....	186
<i>X. Merrheim, J.-M. Muller, and H.-J. Yeh</i>	
<b>Circuit Technology</b>	
<b>Chair: Chris N. Hinds, Motorola</b>	
Algorithms and Multi-Valued Circuits for the Multioperand Addition in the Binary Stored-Carry Number System.....	194
<i>D. Etiemble and K. Navi</i>	
On Digit-Recurrence Division Implementations for Field Programmable Gate Arrays .....	202
<i>M.E. Louie and M.D. Ercegovac</i>	
Estimating the Power Consumption of CMOS Adders .....	210
<i>T.K. Callaway and E.E. Swartzlander, Jr.</i>	
<b>Panel — Arithmetic Standards</b>	
<b>Moderator: Willy McAllister</b>	

## **Compilers and Languages**

**Chair: D.M. Lewis, University of Toronto**

Exploiting Trivial and Redundant Computation.....	220
<i>S.E. Richardson</i>	
Efficient Multiprecision Floating Point Multiplication with Optimal Directional Rounding .....	228
<i>W. Krandick and J.R. Johnson</i>	
Faster Numerical Algorithms via Exception Handling.....	234
<i>J.W. Demmel and X. Li</i>	
A Lazy Exact Arithmetic .....	242
<i>M.O. Benouamer, P. Jaillon, D. Michelucci, and J.-M. Moreau</i>	

## **Cryptography**

**Chair: Luigi Dadda, Politecnico di Milano**

Fast Implementations of RSA Cryptography .....	252
<i>M. Shand and J. Vuillemin</i>	
On Squaring and Multiplying Large Integers .....	260
<i>D. Zuras</i>	
A Modular Multiplication Algorithm with Triangle Additions .....	272
<i>N. Takagi</i>	
High-Radix Modular Multiplication for Cryptosystems.....	277
<i>P. Kornerup</i>	
Author Index.....	284