

ARITH-15 2001

Table of Contents

| | |
|--|-----|
| Foreword | ix |
| Committees..... | x |
| Additional Reviewers..... | xii |
| Keynote Speech | |
| <i>Chair: Neil Burgess</i> | |
| Computer Arithmetic—A Processor Architect's Perspective | 3 |
| <i>Ruby B. Lee</i> | |
| Session 1: Binary Strings in Computer Arithmetic | |
| <i>Chair: Luigi Ciminiera</i> | |
| Leading Zero Anticipation and Detection—A Comparison of Methods | 7 |
| <i>M. S. Schmookler and K. J. Nowka</i> | |
| Bounds on Runs of Zeros and Ones for Algebraic Functions..... | 13 |
| <i>T. Lang and J.-M. Muller</i> | |
| Session 2: Multiplication and Exponentiation | |
| <i>Chair: Vojin Oklobdzija</i> | |
| Binary Multiplication Radix-32 and Radix-256..... | 23 |
| <i>P. -M. Seidel, L. D. McFearin, and D. W. Matula</i> | |
| Analysis of Column Compression Multipliers..... | 33 |
| <i>K' A. C. Bickerstaff, E. E. Swartzlander, Jr., and M. J. Schulte</i> | |
| Faithful Powering Computation Using Table Look-Up and a Fused Accumulation Tree..... | 40 |
| <i>J. A. Piñeiro, J. D. Bruguera, and J.-M. Muller</i> | |
| Session 3: Cryptography | |
| <i>Chair: Luigi Dadda</i> | |
| Bit-Parallel Systolic Modular Multipliers for a Class of $GF(2^m)$ | 51 |
| <i>C. -Y. Lee, E. -H. Lu, and J.-Y. Lee</i> | |
| Modular Multiplication and Base Extensions in Residue Number Systems..... | 59 |
| <i>J. -C. Bajard, L.-S. Didier, and P. Kornerup</i> | |
| Efficient Computation of Multiplicative Inverses for Cryptographic Applications | 66 |
| <i>M. A. Hasan</i> | |
| Optimised Squaring of Long Integers Using Precomputed Partial Products..... | 73 |
| <i>B. Phillips</i> | |

Session 4: Division and Square Root

Chair: Mike Schulte

| | |
|--|-----|
| Correctly Rounded Reciprocal Square-Root by Digit Recurrence and Radix-4 Implementation | 83 |
| <i>T. Lang and E. Antelo</i> | |
| A Hardware Algorithm for Computing Reciprocal Square Root | 94 |
| <i>N. Takagi</i> | |
| Improved Table Lookup Algorithms for Postscaled Division | 101 |
| <i>D. W. Matula</i> | |

Session 5: Elementary Functions and Rounding

Chair: Paolo Montuschi

| | |
|--|-----|
| Worst Cases for Correct Rounding of the Elementary Functions in Double Precision | 111 |
| <i>V. Lefèvre and J.-M. Muller</i> | |
| Generation and Analysis of Hard to Round Cases for Binary Floating Point Division | 119 |
| <i>L. D. McFearn and D. W. Matula</i> | |
| Some Improvements on Multipartite Table Methods | 128 |
| <i>F. de Dinechin and A. Tisserand</i> | |
| High-Performance Architectures for Elementary Function Generation | 136 |
| <i>J. Cao, B. W. Y. Wei, and J. Cheng</i> | |

Session 6: Number Systems

Chair: Peter Kornerup

| | |
|--|-----|
| A Decimal Floating-Point Specification | 147 |
| <i>M. F. Cowlshaw, E. M. Schwarz, R. M. Smith, and C. F. Webb</i> | |
| Algorithms for Quad-Double Precision Floating Point Arithmetic | 155 |
| <i>Y. Hida, X. S. Li, and D. H. Bailey</i> | |
| Effective Continued Fractions | 163 |
| <i>D. Lester</i> | |

Session 7: Floating Point Units

Chair: David Hough

| | |
|--|-----|
| 1-GHz HAL SPARC64® Dual Floating Point Unit with RAS Features | 173 |
| <i>A. Naini, A. Dhablania, W. James, and D. Das Sarma</i> | |
| On the Design of Fast IEEE Floating-Point Adders | 184 |
| <i>P.-M. Seidel and G. Even</i> | |
| In-Order Issue Out-of-Order Execution Floating-Point Coprocessor for CalmRISC32 | 195 |
| <i>C.-H. Jeong, W.-C. Park, T.-D. Han, S.-W. Kim and M.-K. Lee</i> | |

Session 8: Addition

Chair: Simon Knowles

Using the Reverse-Carry Approach for Double-Datapath Floating-Point Addition..... 203
J. D. Bruguera and T. Lang

High Speed Parallel-Prefix Modulo 2^n+1 Adders for Diminished-One Operands 211
H. T. Vergos, C. Efstathiou, and D. Nikolos

Parallel Prefix Adder Design..... 218
A. Beaumont-Smith and C.-C. Lim

Session 9: Logarithmic Number Systems

Chair: Renato Stefanelli

Low-Power Properties of the Logarithmic Number System..... 229
V. Paliouras and T. Stouraitis

Unrestricted Faithful Rounding is Good Enough for Some LNS Applications..... 237
M. G. Arnold and C. Walter

The Use of the Multi-Dimensional Logarithmic Number System in DSP Applications 247
V. S. Dimitrov, J. Eskritt, L. Imbert, G. A. Jullien, and W. C. Miller

Session 10: On-Line Arithmetic

Chair: Milos Ercegovic

On-Line Arithmetic for Detection in Digital Communication Receivers 257
S. Rajagopal and J. R. Cavallaro

A Design of Radix-2 On-Line Division Using LSA Organization 266
A. F. Tenca and S. U. Hussaini

Addendum: Reprinted Paper from the 14th Computer Arithmetic Symposium

A Family of Adders 277
S. Knowles

Author Index..... 285