Low-Power VLSI Architectures for Error Control Coding and Wavelets

Keshab K. Parhi

University of Minnesota
Department of Electrical and Computer Engineering
Minneapolis, MN, 55455

U. S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

This final report provides a brief summary of our research results supported by the above grant during the period from May 1, 1998 to November 30, 2001.

Our research has addressed design of high-speed, low-energy, low-area architectures for signal processing systems and error control coders. Contributions in the area of error control coding architectures include design of low-energy and low-complexity finite field arithmetic architectures and Reed-Solomon (RS) codecs. High-performance and low-power architectures for low-density parity-check (LDPC) codes have been developed.
MEMORANDUM OF TRANSMITTAL

U.S. Army Research Office
ATTN: AMSRL-RO-BI (TR)
P.O. Box 12211
Research Triangle Park, NC 27709-2211

☐ Reprint (Orig + 2 copies)    ☐ Technical Report (Orig + 2 copies)
☐ Manuscript (1 copy)        ☒ Final Progress Report (Orig + 2 copies)
☐ Related Materials, Abstracts, Theses (1 copy)

CONTRACT/GRANT NUMBER: DA/DAAG55-98-1-0315

REPORT TITLE: Low-Power VLSI Architectures for Error Control Coding and Wavelets

is forwarded for your information.

SUBMITTED FOR PUBLICATION TO (applicable only if report is manuscript):

Sincerely,

Keshab K. Parhi
University of Minnesota
Proposal #37239-EL
Final Report

Low-Power VLSI Architectures for Error Control Coding and Wavelets

ARO Grant Number: DA/DAAG55-98-1-0315 (37239-EL)
PI: Keshab K. Parhi, Distinguished McKnight University Professor
Department of Electrical & Computer Engineering
University of Minnesota
200 Union Street SE
Minneapolis, MN 55455
Tel: (612) 624-4116
Fax: (612) 625-4583
E-mail: parhi@ece.umn.edu

1 Introduction

This final report provides a brief summary of our research results supported by the above grant during the period from May 1, 1998 to November 30, 2001.

Our research has addressed design of high-speed, low-energy, low-area architectures for signal processing systems and error control coders [1]. Contributions in the area of error control coding architectures include design of low-energy and low-complexity finite field arithmetic architectures and Reed-Solomon (RS) codecs [2]-[8]. High-performance and low-power architectures for low-density parity-check (LDPC) codes have been developed [9]-[11]. Approaches for reducing area/power while maintaining performance of CMOS VLSI DSP systems have been developed at various levels of abstraction, with work concentrating at gate and transistor levels [12]-[24]. Examples of these techniques include coefficient switching activity reduction, use of multiple accumulators in a programmable DSP, appropriate bus coding, transistor sizing, retiming, and use of dual supply voltages and dual threshold voltages.

2 VLSI Finite Field Architectures and Reed-Solomon Coders

Finite fields are of great importance in modern applications in all areas of information and communication theory, i.e., coding theory, cryptography and digital signal processing. Our research has been directed towards design of low-energy, low-latency, hardware-efficient architectures for finite field arithmetic operations and their applications including Reed-Solomon error-control codecs and elliptic curve cryptosystems that are extensively used to
achieve secure and reliable transmission and storage in digital communication and recording systems. Our contributions include a hardware/software codesign approach for the design of low-energy high-performance programmable Reed-Solomon codecs, and a scheme for design of low-complexity low-power dedicated finite field multiplier.

2.1 VLSI Reed-Solomon Coders with Hardware/Software Codesign

We have considered hardware/software codesign of low-energy programmable Reed-Solomon (RS) codecs. These systems are to be implemented as a combination of hardware and software in application-specific DSP processors with specially designed programmable finite field datapath and dedicated and optimized software to reduce the total energy consumption. To obtain the best hardware and software combinations for low-energy RS codecs, we have considered the design of programmable finite field datapath (hardware), different RS coding algorithms and software scheduling schemes (software) \[2\][3]. A novel frequency-domain RS decoding procedure using division-free Berlekamp-Massey algorithm was proposed \[4\][5]. From extensive experimental results and cross-comparisons of both energy and energy-latency products, we concluded that RS decoders using the proposed frequency-domain RS decoding procedure with division-free Berlekamp-Massey algorithm based on finite field datapath with separate MAC (for polynomial multiply-accumulate operation) and DEGRED (for polynomial modulo operation) units have the best performance. Future work will be directed towards design of energy-scalable elliptic curve cryptosystems.

2.2 Systematic Design of Mastrovito Multipliers over Finite Field

In \[6\]-\[8\], we have modified and generalized the Mastrovito multiplication scheme such that low-complexity parallel multipliers for the finite field GF(2^m) can be designed with complexity proportional to minpwt, m-1-pwt (pwt denotes the Hamming weight of the irreducible polynomial). These designs are good for irreducible polynomials of both low and high Hamming weights. This completes the design space and offers more freedom on polynomial selection. This approach extensively exploits the spatial correlation of matrix elements in Mastrovito multiplication to reduce the complexity. The developed general Mastrovito multiplier is highly modular, which is desirable for VLSI hardware implementation. It is shown that this generalized Mastrovito multiplier generally has the lowest complexity, smallest latency and consumes the least power, compared with other standard-basis and dual-basis multipliers.

Furthermore, the proposed approach has been used to develop efficient Mastrovito multipliers for several special irreducible polynomials, such as trinomial and equally-spaced-polynomial (ESP), and the obtained complexity results match the best known results. Applying the proposed approach, we have discovered several other special irreducible polynomials which also lead to low-complexity Mastrovito multipliers, which is especially desirable when neither an irreducible trinomial nor an irreducible ESP exists.
3 Low-Density Parity-Check Coders

Today Low-Density Parity-Check (LDPC) codes great current interest and these codes are widely considered as a serious competitor to turbo codes. In the past few years, a lot of efforts have been devoted in this field and many new developments have been brought. With the amazing development of LDPC codes in the theoretical community, its real world applications continue to grow. We expect LDPC coding hardware design for communications and magnetic storage applications will definitely become an important topic in a few years.

We have analyzed the finite precision effects on the decoding performance of regular LDPC codes and have developed optimal finite word lengths of variables as far as the tradeoffs between the performance and hardware complexity are concerned [9].

As far as practical system implementation is concerned, the analysis of finite precision effects is an important issue to be considered. However, to our best knowledge, the precision effects on the performance of the LDPC codes decoder have not been addressed in the literature. We have analyzed the finite precision effects on the decoding performance of LDPC codes and developed optimal finite word lengths of variables as far as the tradeoffs between the performance and hardware complexity are concerned [2]. Through Monte Carlo simulation, we have found that 4 bits and 6 bits are adequate for representing the received data and extrinsic information, respectively. We also proposed a novel quantization scheme for extrinsic information to improve the performance compared with conventional scheme. Simulation results indicate that the quantization scheme we have developed for the LDPC decoder is effective in approximating the infinite precision implementation.

We have developed a joint code-decoder approach which can be implemented using less hardware. An approach has been developed to extend (2,K) codes to (3,K) codes. [10][11]. This work is ongoing and is being continued with the renewed ARO grant 42436-CI.

4 Synthesis of Low-Power VLSI Circuits

4.1 Manipulating Slack for Power Reduction

A new technique, UDF-displacement (Unit Delay Fictitious Buffer-displacement), was developed, which facilitates manipulation of the slack in a technology mapped circuit to address the dual supply voltage allocation [12], and the dual threshold voltage allocation problem [13]. Another problem which can be tackled in the same framework as the previous one is the low power gate resizing problem [14]. A journal paper has been written to present all applications of UDF-displacement at one place [15].

Dynamic power consumed in CMOS gates goes down quadratically with the supply voltage. By maintaining a high supply voltage for gates on the critical path and by using a low supply voltage for gates off the critical path it is possible to dramatically reduce power consumption in CMOS VLSI circuits without performance degradation. Interfacing gates operating under multiple supply voltages requires the use of level converters. Due to the non-negligible power consumed by level converters and the substantial propagation delay they might incur, it is necessary to develop a formal model that quantifies various design parameters such as delay and power. A formal model allows us to develop efficient heuristics
to address the problem. In this study we develop a formal model and develop an efficient heuristic for addressing the use of two supply voltages for low power CMOS VLSI circuits without performance degradation. Substantial improvements in power savings are demonstrated over existing methods. In [12], UDF-displacement is used to develop a novel technique for formally addressing the problem of dual supply voltage allocation that results in up to 25% power savings over other existing heuristics for the benchmark circuits in the ISCAS85 benchmark suite. The technique of UDF-displacement is used to address the problem of dual threshold voltage allocation in [13], and shows improvements of up to 16% over existing heuristic approaches for ISCAS85 benchmark circuits.

Low power gate resizing can decrease the power dissipated in a technology mapped circuit while maintaining its critical path. Gate resizing operates as a post-mapping technique for power reduction by replacing some gates, which are faster than necessary, with smaller and slower gates from the underlying gate library. In this study we propose a new transformation technique for combinational circuits referred to as buffer-redistribution. Buffer-redistribution is then used to model and solve the low-power discrete gate resizing problem in an exact manner in polynomial time and in a non-iterative fashion for a complete gate library. Suboptimal solutions are obtained with incomplete gate libraries. In contrast past polynomial time techniques for gate resizing were either based on heuristics or based on much slower iterative exact algorithms. Simulation results on ISCAS85 benchmark circuits demonstrate 2.1%-54.1% power reduction based on the proposed buffer-redistribution based low-power gate resizing. Power savings from 0%-44.13% are demonstrated over the same circuits mapped for minimum area. The time required for resizing varies from 2.77s-1256.76s. This research is presented in [14].

4.2 MARSH: Minimum Area Retiming With Setup and Hold Constraints

A polynomial technique for minimum area retiming with both long path and short path constraints incorporated simultaneously is demonstrated for the first time. A constraint pruning strategy is also shown that can make the technique far more practical [16][17].

4.3 Synthesis of Low Power Folded Programmable Coefficient FIR Digital Filters

Folding or time-multiplexing normally leads to increase in switching activity and power consumption. In this research, a novel methodology for synthesizing FIR digital filters with programmable coefficients is proposed that minimizes switching activity [18].

4.4 A Novel Multiply Multiple Accumulator for PDSPs

A novel Multiply Multiple Accumulator (MMAC) Component is designed that can lead to low power mapping of FIR filters onto it for the design of low power programmable digital signal processors [19][20].
4.5 BUS ENCODING FOR LOWERING PEAK AND AVERAGE POWER

A novel technique has been studied for finding the data-transmission capacity of busses that have a limit on their peak transition activity [21].

A novel technique for lowering average power consumed in Data-Busses that comes close to achieving an entropy based lower bound on the average transition activity has been developed in [22].

4.6 Transistor Sizing

A novel min-cost flow based transistor sizing tool has been developed [23]-[24]. This tool makes use of iterative relaxation and leads to fast and exact transistor sizing.

5 List of Publications


6 AWARDS

The PI was awarded a Golden Jubilee Medal from the IEEE Circuits and Systems society for exceptional contributions to the society in last 50 years in 1999.

The PI was awarded the 2001 IEEE W.R.G. Baker prize paper award.