doc. Ing. Miloš Drutarovský, CSc.

Department of Electronics and Multimedia Communications
Faculty of Electrical Engineering and Informatics
Technical University of Kosice
Park Komenskeho 13, 041 20 Kosice
Slovak Republic
Tel.: +421 55 6024169
E-mail: Milos.Drutarovsky@tuke.sk

Doctoral Thesis Review

Properties and Implementation Aspects of Residue Arithmetic for a Hardware Solver of Systems of Linear Equations submitted by Ing. Jiří Buček

The thesis has been submitted to the Faculty of Information Technology, Czech Technical University in Prague, in Ph.D. study programme Informatics in August 2017.

Structure of the doctoral thesis

The manuscript text has 92 numbered pages and is divided into 6 chapters, bibliography with 39 items and three lists of author's publications (8 reviewed publications relevant to the thesis, 5 remaining publications relevant to the thesis and 15 remaining publications). The thesis is written in the form of a collection of relevant author's published papers, introductory chapters and conclusions. Chapter 1 explains research motivation, problem statement, goals and thesis organization. Chapter 2 provides basic definitions, terminology and background for operations used in Set of Linear Equations (SLE) solution based on Residue Number System (RNS) implemented in hardware. Chapter 3 summarizes the previous results and related work in the hardware based SLE solution, algorithms and processing elements used in this area. Chapter 4 shortly presents main architecture modifications proposed by author as introduction to the chapter 5. Chapter 5 presents main results in the form of a collection of 6 published papers denoted as RP1-RP6. Chapter 6 summarizes the results presented in the thesis and suggests themes for future work.

Relevance of the selected topic and aims of the doctoral thesis

The aim of the doctoral thesis is to develop the architecture of a system for efficient and error-free solving of SLE in embedded hardware based on FPGA and ASIC technology. Parallelization used in the proposed solution is a direct consequence of application of well-known Residual Number System. Proposed hardware architecture and system-dependant optimization are targeted to the modern target embedded hardware. Concentration to the efficient exploitation of these hardware resources for error-free modular arithmetic based solution, optimization of algorithms and processing elements, as well as development of efficient and compact embedded system is still relevant topic in research community. I consider given topic as valuable and sufficient for verification of the originality of the solution in the given filed.

Used methods of the solutions and level of the processing of the doctoral thesis

The submitted thesis offers a solution for solving a SLE without rounding errors in embedded hardware based on FPGA and ASIC technology. Proposed system uses the modular arithmetic approach based on RNS that can be naturally parallelized and the core of SLE solutions is executed on a set of independent processors. It concentrates to the optimization of system architecture implemented in FPGA and ASICs platforms for different word lengths and SLE matrix dimensions. The efficiency of implemented hardware solution of SLE was evaluated by using the metrics of time, area and time-area product.

The doctoral thesis is aimed at improving of existing algorithms for parallel error-free solution of SLE. This was done on implementation level by optimization and testing of several low-level processing algorithms and elements as well as on a system architecture level and system integration. Author proposed some optimizations for Montgomery multiplication by using modified carry-save encoding suitable for FPGA technology.

On the system level, author designed FPGA prototype system using an embedded processor and parallel peripherals were design enabling verification of the architecture and functional testing. System integration (Modular System) of one central processor with several peripherals (Residual Processors) enables running multiple SLE solvers using multiple moduli for computation of the system of linear congruences solution. Communication complexity was analyzed and total solution times estimated for several possible problem dimensions.

Author tested implemented solutions in target FPGA technology (Xilinx Virtex 6) and ASIC ones (130 nm, 110 nm and low-power 55 nm libraries).

The thesis is well written and contains only a small number of typographic errors (e.g. "cata flow" on page 32, RP "Residal Processor" in Abbreviations, posisble on page 81, ...), some errors in used equations (e.g. there should be 2s instead of 2r in the last row of Table 3.1 and Table 4.1). The list of abbreviations is not complete (e.g. abbreviations CPU, GPU, LU, PE, SIMD, AU, ... are missing). The usage of some variables is a little bit inconsistent in the introductory chapters (e.g. p is used as a prime number in some equations as well as a number of processors in Figure 3.1). The structure of submitted thesis is balanced and very well readable, it contains all relevant information in a compact form.

Original scientific contributions of the doctoral thesis and accomplishment of the stated aims

The thesis presents embedded error-free SLE solver embedded in modern FPGA and ASIC technology. The proposed solution and results provide interesting insight what is possible to reach in the area of SLE solution in modern embedded hardware. This is in my opinion the main thesis contribution. The main results were published in the indexed journal (RP6 publication) and can be used by research community as a reference solution.

Also achieved results of particular low-level optimization of processing elements and algorithms are quite interesting for design community. Especially comparison of substratcion-free and traditional Almost Montgomery Inversion (AMI) is the selected target technologies is very interesting and was already referenced in several (4 reported in the thesis) papers and books.

The thesis contains now a set of results that can be compared with computer based solutions and presents potentially interesting information for those who need to implement critical parts of SLE by means of RNS in modern embedded hardware.

Based on these facts I consider the aims of the doctoral thesis fulfilled.

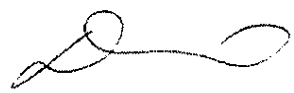
Comments and questions

Author used FPGA platform as a prototype one for verification of the proposed architecture and functional testing before porting proposed solution to the ASIC technology. Modern FPGA circuits contain also a large number of embedded multipliers. These embedded multipliers were not used in the proposed solution. Would it be possible to use these embedded multipliers for FPGA specific solution of RNS based SLE solver?

What are typical application that could benefit from availability of embedded error-free SLE solver? I was looking for a typical example or reference in the thesis but e.g. reference [2] in RP6 that probably contains some example is not complete. Can you mention some typical applications that could, in your opinion, use such embedded error-free SLE solver?

Conclusions

The submitted thesis of Ing. Jiří Buček addresses interesting and practical problem of efficient error-free solution of SLE by means of RNS in modern embedded hardware. The author of the thesis in my opinion **proved** clearly by presented thesis the ability to perform research and achieve scientific results. I **do recommend** the thesis for presentation and defense with the aim of receiving the Degree of Ph.D.



Košice, January 14, 2018

Miloš Drutarovský
reviewer

Dr. Kris Gaj
Associate Professor
ECE Department, MS 1G5
George Mason University
4400 University Drive
Fairfax, VA 22030
United States
Tel.: +1 571 354 8689
E-mail: kgaj@gmu.edu

Doctoral Thesis Review

Properties and Implementation Aspects of Residue Arithmetic for a Hardware Solver of Systems of Linear Equations

Submitted by Ing. Jiří Buček

The thesis has been submitted to the Faculty of Information Technology, Czech Technical University in Prague in the Ph.D. study program Informatics.

Up-to-datedness of the dissertation

In spite of multiple papers on solving a system of linear equations, the problem remains challenging and open for further exploration, especially for a large number of variables. The author makes it particularly original and relevant by considering the case of error-free solutions. He accomplishes such solutions by using the Residue Number System.

Practical implementation of a system solver for a large number of equations in reconfigurable hardware has become possible only in recent years due to the increased number of basic building components (Configurable Logic Blocks) and Block RAMs present in modern FPGAs. New types of devices, such as Zynq, facilitate hardware/software codesign, taking advantage of the close integration of microprocessors and FPGA fabric.

There is a strong demand for hardware accelerators in multiple domains of science and engineering, due to their performance and power advantage over microprocessor-based solutions. Additionally, new types of applications emerge over time, for example, implementing and breaking multivariate post-quantum cryptographic algorithms.

One of the important measures of the thesis up-to-datedness is the acceptance of the most comprehensive paper, RP6, based on and included in this Ph.D. thesis, to the prestigious Springer Journal of Signal Processing Systems, in 2017.

Formal structure and organization of the thesis

The structure and organization of the thesis is easy to follow.

The author uses a somewhat unconventional method of presenting the main body of his work using his major publications, preceded by short introductions. This approach has its advantages and disadvantages. On the positive side, it clearly demonstrates and documents a long history of persistent work on the thesis major topic, and its evolution from the development and optimization of basic building blocks to the development of the complete FPGA-based accelerator and the exploration of differences between the system performance in ASICs and FPGAs. On the negative side, it introduces an unavoidable redundancy in the form of similar introduction and previous work sections, used in multiple papers.

The relation between the publications RP1 and RP2 and the rest of the thesis is somewhat loose. In particular, RP1 talks about the hardware architecture for Montgomery Multiplication with Modified Carry-Save Encoding. However, the operand sizes considered are 512, 1024, and 2048 bits. On the other hand, in publications RP3-RP6, the operand sizes are reduced to 24 bits. Thus, it is somewhat hard to see how the optimum choices of the Montgomery multiplier parameters (such as w) would apply to the main design presented in the thesis. Similarly, RP2 talks about the choice of an optimal modular inversion unit, for operand sizes 64, 128, 162, and 256 bits. All these sizes are significantly greater than the one used for the calculation of modular inverses in RP3-RP6, which is 24 bits. Additionally, the publications RP3-RP6 all list the following publication, rather than RP2, as a reference describing the modular inverse algorithm used:
R. Lorencz, "New algorithm for classical modular inverse," in *4th International Workshop on Cryptographic Hardware and Embedded Systems*, CHES 2002, London, UK, Springer-Verlag, 2003, pp. 57–70.

The remaining chapters of the thesis, Chapter 1 Introduction, Chapter 2 Theoretical Background and State-of-the-Art, Chapter 3 Previous Results and Related Work, and Chapter 6 Conclusions, are succinct, consistent, and well written.

Completion of the dissertation objectives

The primary dissertation objectives were the development of optimal algorithms and hardware architectures for

- Montgomery Multiplier with operand sizes k=512, 1024, and 2048 bits
- Modular Inverse unit with operand sizes n=64, 128, 162, and 256 bits, and
- Error-Free Linear System Solver for the matrix sizes n between 20 and 4000.

All hardware architectures were optimized from the point of view of the time*area product.
The goals of the dissertation were achieved, as confirmed by the results of simulation, synthesis, and prototyping using modern FPGA devices and development boards, as well as front-end design using standard-cell 130/110 nm and 55nm ASIC libraries optimized for high speed and low power, accordingly.

Assessment of the methods used in the thesis

Scientific methods, techniques, and tools used in the dissertation are consistent with the state-of-the-art.

The digital system was developed using the Register-Transfer Level methodology (for maximum performance and minimum resource utilization), and the code was written in synthesizable VHDL. The final prototype was based on Xilinx ML605 board with a Virtex-6 LX240T FPGA, 1 GiB DDR3 SDRAM memory, gigabit Ethernet interface, and other peripherals. The digital system was implemented as a system-on-chip (SoC) located inside of an FPGA. It used an external on-board memory, and the Ethernet interface for communication with a personal computer (PC). The Central Control Unit of SoC was implemented using a MicroBlaze soft-processor, which was responsible for controlling the transfer of data between main memory and Residual Processors implemented in FPGA fabric. The software running on MicroBlaze was written in C.

Particularly impressive was the amount of effort devoted to the verification of the design. The verification was based on a comprehensive set of test vectors generated using Wolfram Mathematica and converted with a Python script into a file format suitable for logic simulation. The design was then simulated with Mentor ModelSim to solve systems of linear congruences (SLCs) and the obtained solutions were compared to solutions precomputed using Wolfram Mathematica. The simulation was performed for matrices up to the dimension $n = 100$.

The development of the SoC was based on the use of Xilinx Embedded Development Kit (EDK) and Xilinx Integrated Synthesis Environment (ISE). Although these tools were recently superseded by Xilinx Vivado, the new toolset could not have been used with the specific prototyping board, Xilinx ML605, based on Xilinx Virtex-6 FPGAs.

The second target technology was ASIC with standard-cell libraries from two different vendors – Synopsys/GlobalFoundries in 130 nm technology, and Faraday/UMC in 110 nm and 55 nm technologies. The 130 nm and 110 nm libraries were high performance libraries, while the 55 nm library was a low power library. The front-end design (logic synthesis and timing analysis) was performed using Synopsys Design Compiler 2005.09 SP2. The area and minimum clock period were post-synthesis estimates extracted from the synthesized netlist using time and area reporting capabilities of the Design Compiler. Although these estimates are not fully representative of the final values that could have been obtained using the back-end design (physical synthesis and timing analysis taking into account parasitic extraction), it is a common practice to use them as first-order estimates in scientific literature.

Evaluation of the results and contributions of the thesis

The contributions of the thesis are original and of practical value to multiple areas of science and engineering, e.g., physics, chemistry, computer science, economics, astrophysics, electrical and mechanical engineering, etc. Hardware accelerators are likely to be necessary for solving systems of linear equations with the number of variables in excess of 100, not to mention 1000. For the number of variables $n=1000$, the author demonstrates the speed up by a factor of 3.4 for the proof-of-concept FPGA implementation, and predicts the speed-up up to 10 times using state-of-the-art ASIC technologies. An additional advantage, not fully explored in the thesis, is a reduced power and energy consumption.

Remarks, objections, notes, and questions for the defense

The following problems have not been fully addressed in the text of the thesis, and may require additional explanation:

The terminology specific to algorithms for solving systems of linear equations (such as the concept of pivot) is not properly introduced, before being used in the thesis. See for example a proper introduction of a concept of pivot in Wikipedia at
https://en.wikipedia.org/wiki/Pivot_element

In Section 5.1 and the corresponding paper RP1, an optimum word size, optimizing the time*area product of the Montgomery Multiplier with Modified Carry-Save Encoding is determined to be w=4 for operand sizes of k=512 and 1024, and w=8 for k=2048. These values are determined based on the use of FPGAs available in 2004. It is not clear how these choices affect the choice of parameters in the subsequent sections 5.2-5.6 and the corresponding papers RP2-RP6, and whether the modified carry-save encoding is used in the implementations described in these sections/papers at all.

Table 6.1, used in the Conclusions, does not describe clearly the dependence of the total execution time on the number of Residual Processors. Table 6 from the paper RP6 seems to contain much more relevant information. However, in this table it is unclear how it is possible that the solution time is the same for $p=200 < r=314$ and for $p=500 > r=314$, where r represents the maximum number of moduli needed for the solution, and p represents the number of Residual Processors (one per each modulus). Additionally, the same holds true for $p=500 < r=632$ and $p=1000 > r=632$.

The paper RP6 states that the parameters p, n, q, e are configurable at synthesis time, where

- p is the number of Residual Processors
- n is the dimension of the matrix of integer coefficients
- q is the number of words in each element of the matrix
- e is the word length.

In publications RP3-RP6, e is set to 24 and q to 3. However, the justification for these choices is limited to the following statement from RP5: "The 24-bit word length was chosen as a compromise so that enough prime moduli can be generated to represent the largest number needed during solution of the system of linear equations. This follows from the Hadamard's inequality and its application on solving a linear system exactly [5]." However, it is not very clear what other values of e and q were considered, what was a factor limiting the value of e (total memory size, performance, other?), and why the selected values offered the best trade-off.

Similarly, it is not clear if any parameters selected by the author depend on the semiconductor technology used, including an FPGA family or an ASIC standard-cell library used.

Fig. 3 in RP5 shows the dependence between the maximum clock frequency, the matrix dimension n, and the technologies 130 nm, 110 nm and 55nm. However, the corresponding text does not clearly explain why the relation between maximum clock frequencies for 130 nm and 110 nm on one side and 55 nm on the other side significantly changes when n is modified from 100 to 300.

The publication RP6, the related chapter 5.6, and Chapter 6 Conclusions could be strengthened by comparing in the tabular form the obtained results with results achieved for other linear system solvers, reported earlier in the literature (even if the overall functionality and parameters of these solvers were not exactly the same).

Overall evaluation

I consider this dissertation successful, despite the critical remarks listed in the previous sections. The reason for this claim lies in the amount of work that the author had to do to achieve the presented results, and the level of expertise and fluency in modern digital system design methodologies and tools demonstrated. The dissertation is original, does not contain any significant formal or factual deficiencies, and is easy to follow.

Recommendation Statement

The author of the dissertation proved the ability to conduct research and achieve scientific results. In accordance with par. 47, letter (4) of the Law Nr. 111/1998 (The Higher Education Act) I do recommend the thesis for the presentation and defense with the aim of receiving the Ph.D. degree.

Fairfax, Virginia, U.S.A., March 12, 2018

KGaj

Kris Gaj

BRNO FACULTY
UNIVERSITY OF INFORMATION
OF TECHNOLOGY TECHNOLOGY

Brno, November 29, 2017

Review of Doctoral Thesis submitted to CVUT – Czech Technical University in Prague, Faculty of Information Technology

Title: Properties and Implementation Aspects of Residue Arithmetic for a Hardware Solver of Systems of Linear Equations

Author: Jiří Buček

The scope and contributions

This doctoral thesis addresses the problem of efficient solving of a system of linear equations (SLEs). Solving a system of linear equations represents a well-known an intensively studied problem, with many different methods and algorithms available in literature. In order to improve efficiency of current SLE solvers and improve their scalability, various approaches have been adopted and customized for a chosen target computational platform such as clusters of computers, Graphic Processing Units or Field Programmable Gates (FPGAs). The scalability issue, however, is not the only problem we have to face with. The difficulty of SLE solving is manifold. Among others, matrix density, conditioning, accuracy requirement or stability of solution represent serious issues. Typically, a floating point (FP) arithmetic is employed. Unfortunately, the FP arithmetic is inevitably connected with rounding errors and limited accuracy which may prevent in finding a solution of ill SLE instances. Hence, the doctoral thesis focuses on the problem of finding an error-free solution which is an important prerequisite for finding a solution of dense and ill-conditioned systems. Even though there is only a little work related to the error-free solution of SLEs and this topic does not represent a main-stream research problem, I consider the theme of the thesis as important and relevant for the author's field of study.

Goals of the thesis

The research objectives are not explicitly formulated, however, the goal of this work can be deduced from the introductory part and concluding remarks summarizing author's contributions. This thesis is in fact a continuation of a previous work of Morháč and Lórenz who proposed a HW architecture for error-free solving of SLEs based on Residual Number System (RNS). The goal of this thesis is to extend the system, implement it on a modern FPGA and evaluate its parameters. As the author has not specified the quality level that should be achieved, it is hard to evaluate to what extent the research objectives were accomplished. It is not clear,

for example, whether the achieved speedup is sufficient or not for practical problem instances. There is no comparison with an implementation based on a variant of more precise FP arithmetic. In addition to that, the scalability of the method has not been sufficiently discussed.

Methodology

The research methodology adopted in this thesis is sound. The author briefly reviews and discusses essential components of the SLE solver (Montgomery multiplier, Montgomery inverse, Linear congruence solver) before developing and implementing a final architecture of a hardware SLE solver. Firstly, the author introduced an efficient implementation of modular multiplication based on Montgomery multiplier optimized for modern FPGAs that are equipped with fast ripple-carry adders. Then, three different architectures of Montgomery inverse were implemented and evaluated in FPGA. These components were then employed in a linear congruence solver. The author addressed the problem of proper memory subsystem design which represents the main bottleneck of the solver. This work helped him to form the final architecture for solving system of linear congruencies. The resulting FPGA-based implementation enabled to confront the practical results with a theoretical analysis of the system performance for various linear system sizes. It is no doubt that the proposed approach is more efficient compared to a CPU-based implementation of the RNS-based SLE solver, but it is not clear whether the proposed architecture provides the best results. There is no direct comparison with other available approaches dealing with ill-conditioned systems. The absence of a more detailed evaluation represents the key weakness of the whole thesis. From the methodological point of view, I would expect a more detailed analysis of the achieved results (the speedup is reported only for a single problem instance in journal paper RP6). Interestingly, the power consumption (or even better the number of operations per a Watt) was neither reported nor compared with other implementations. As the current semiconductor industry is driven mainly by the power consumption, it would be nice to discuss the power efficiency of the proposed system which is undoubtedly much better compared to a CPU-based implementation.

Organization, style and language

The thesis is in a form of a collection of papers with an accompanying introductory part and is organized into six chapters. Chapter 1 consists of a brief introduction to the scope of the thesis and motivation. The motivation seems to be a bit shallow and it does not sound convincing (there are no references supporting the presented claims). Chapter 2 provides a necessary notion and mathematical background. The title of Chapter 2 advertises the state-of-the-art related to the SLE solvers, but the state-of-the-art is missing there. Four approaches relevant to the topic of the thesis (i.e. error-free SLE solvers) are mentioned in the introductory paragraph of Chapter 3. These approaches, however, are only referenced without any detailed analysis. A

more detailed introductory emphasizing the necessity to investigate the chosen topic is missing even in the enclosed papers. Chapter 3 briefly presents previous work of Morháč and Lórenz and then focuses on basic components such as Montgomery multiplication, Montgomery inverse and the state-of-the-art relevant to these problems. Chapter 4 provides an overview of the author's work relevant to the chosen topic. The description is sometimes redundant considering the content of Chapter 5 which describes the enclosed papers. Conclusions and future directions are given in Chapter 6. Similarly, the first section of Chapter 6 seems to be a bit redundant since it repeatedly summarizes the content of the enclosed papers. The overall organization of the text is excellent with a small exception. Instead of providing a deeper motivation and surveying open problems of the field which would help the author to formulate the research goals, Chapter 1 pointlessly presents particular algorithms and implementation details that are more suitable for subsequent chapters. It is unclear why the analysis of the RNS to binary conversion representing the main limiting factor of many RNS-based approaches is omitted in the text even though the impact of the conversion is substantial as it is nicely discussed and evaluated in authors' journal paper RP6. Generally, the use of language and grammar is excellent through the thesis and the contributed papers. The writing style is clear and concise.

Author's publications

The list of author's publications is impressive. There are 6 peer-reviewed relevant conference papers, one relevant journal article with IF and more than 20 additional papers. The reviewed papers were accepted at distinguished events such as DSD, ICECS or DDECS. The core ideas of the thesis have been published. The number of publications is sufficient in order to defend the submitted doctoral dissertation.

Questions

(1) The chosen FPGA chip enabled to evaluate the proposed SLE solver for problem instances consisting of up to 200 elements. Interestingly, the performance was reported for 1000 elements. Could you discuss the performance for the lower number of elements? Is there any point from which the proposed architecture performs worse than the current state-of-the-art CPU-based implementation?

(2) Could you discuss scalability of the proposed system? What is the maximum size of the system considering the biggest FPGA available on the market? What is the current bottleneck of the improved memory subsystem?

(3) The power consumption of the proposed FPGA-based solver was neither reported nor compared against other approaches used to evaluate the efficiency of the proposed approach. Is the proposed approach competitive in terms of the power consumption and implementation costs?

(4) The solution time depends not only on the problem size but also on the number of processing units synthesized in FPGA. It is no discussed, however, how to choose the number of units provided that we need to maximize the performance. The situation gets complicated especially due to the RNS to binary conversion which substantially contributes to the total time. Hence the problem of determining the number of units is a multi-objective optimization problem. Could you discuss this issue?

(5) According to the data presented in Table 5 (RP6), the elements of SLE were encoded using 9 bits. Is this resolution sufficient to solve practical SLE instances, especially the ill-conditioned cases?

Summary

Despite the critical comments given in the previous parts of my review, this is a well-written doctoral dissertation presenting new scientific results in the area of error-free solving of SLEs. In my opinion, the author of the thesis proved his ability to perform research and achieve original scientific results. The thesis contains new and original results that have already been published. **I do recommend the thesis for the presentation and defense with the aim of receiving the Ph.D. degree.**

Doc. Ing. Zdeněk Vašíček, Ph.D.
Reviewer of the thesis