Aristotle University of Thessaloniki
Faculty of Sciences
School of Informatics

Title...

A dissertation submitted to the School of Informatics of the Aristotle University of Thessaloniki in fulfillment of the requirements for the degree of doctor of philosophy
by

Name

Thessaloniki, 202x

Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
Σχολή Θετικών Επιστημών
Τμήμα Πληροφορικής

This PhD dissertation was examined and approved by the following committee:

Members of the committee

aaa bbb (Supervisor) Professor, ... , Aristotle University of Thessaloniki.

aaa bbb Professor, ... , Aristotle University of Thessaloniki.

aaa bbb Professor, ... , Aristotle University of Thessaloniki.

aaa bbb Professor, ... , Aristotle University of Thessaloniki.

aaa bbb Professor, ... , Aristotle University of Thessaloniki.

aaa bbb Professor, ... , Aristotle University of Thessaloniki.

aaa bbb Professor, ... , Aristotle University of Thessaloniki.

ΠΕΡΙΛΗΨΗ

Σκοπός της παρούσας πτυχιακής εργασίας είναι η παρουσίαση και υλοποίηση του αλγορίθμου του Gauss Elimination modulo 2 ...

Λέξεις Κλειδιά. Γραμμική άλγεβρα, Γραμμικά Συστήματα, ..., CUDA, C

ABSTRACT

....

Key Words. Linear Algebra, Linear Systems, ..., CUDA, C

Acknowledgements

...

....

Contents

Abreviations

AES	:	Advanced Encryption Standard
AKS	:	Agrawal - Kayal - Saxena
CBC	:	Cipher Block Chaining
CCA	:	Chosen Ciphertext Attack
CPA	:	Chosen Plaintext Attack
CRC	:	Cyclic Redundancy Check

List of Figures

CHAPTER 1

Introduction

.....

1.1 a

...

1.1.1 b

...

CHAPTER 2

Gauss Reduction

2.1 Linear Systems

$$\begin{cases} x_1 = 2r + s - t \\ x_2 = \quad r \\ x_3 = -2s + 2t \\ x_4 = \quad s \\ x_5 = \quad t \end{cases}$$

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \qquad\qquad\qquad\qquad\quad \vdots \\ a_{k1}x_1 + \cdots + a_{kn}x_n = b_k \\ \qquad\qquad\qquad\qquad\quad \vdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n = b_n \end{cases}$$

$$A_{m,n} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

2.2 Linear Systems II

CHAPTER 3

GAUSS REDUCTION - SINGLE CORE CASE

.....

3.1 Algorithms in LaTeX

Alogrithm 3.1.0.1 *: Multiplication of Karatsuba*
input. a, b *integers*
output. $a \cdot b$

```
1  def karatsuba(a, b)
2   if a < 100 or b < 100 then
    |   return a · b
    end
3   m = max(log_10(a), log_10(b))
4   m_2 = floor(m/2)
5   high(a) = take the first m_2 decimal digits of a
6   low(a) = take the last m_2 decimal digits of a
7   high(b) = take the first m_2 decimal digits of b
8   ...
9   ...
10  ....
11 print (z_2 · 10^(2m_2) + (z1 − z2 − z0) · 10^(m_2) + z_0
```

Alogrithm 3.1.0.2 *: Enumeration algorithm*
Είσοδος. *An ordered basis* $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{Z}^m$ *of the lattice* $\mathcal{L}(\mathcal{B})$ *and a positive real number R.*
΄Εξοδος. *All the vectors*$\mathbf{x} \in \ \mu\epsilon\ \|\mathbf{x}\| \leq R$.

01. Compute $\{\mu_{ij}\}$ and $B_i = \|\mathbf{b}_i^*\|^2$
02. $\mathbf{x} = (x_i) \leftarrow \mathbf{0}_n, \mathbf{c} = (c_i) \leftarrow \mathbf{0}_n,\ ` = (`_i) \leftarrow \mathbf{0}_n,\ sumli \leftarrow 0, S = \emptyset, i \leftarrow 1$
03. **While** $i \leq n$
04. $\quad c_i \leftarrow -\sum_{j=i+1}^{n} x_j \mu_{ji}$
05. ...

19. return S

CHAPTER 4

SOMETHING

.....

References

[1] Tolga Soyata. *GPU Parallel Program Development Using CUDA*. Chapman & Hall/CRC Computational Science. Chapman and Hall/CRC, 1st edition, 2018.

[2] Comissió Gauss. Presentació del volum gauss. pages 11–14. Facultat de Matemàtiques i Estadística (ed.), Barchelona, Spain, 2006. Conferències FME: volum III. Curs Gauss, 2005-2006.

[3] Joseph F. Grcar. Mathematitians of gauss elimination. *Notices of the American Mathematical Society*, 58(6):782–792, 2011.

[4] Michael McCool, Arch D. Robison, and James Reinders. Chapter 3 - patterns. In Michael McCool, Arch D. Robison, and James Reinders, editors, *Structured Parallel Programming*, pages 79 – 119. Morgan Kaufmann, Boston, 2012.

[5] Yadanar Mon and Lai Lai Win Kyi. Performance comparison of gauss elimination and guass-jordan elimination. *International Journal of Computer Science and Network Security*, 2(2):67–71, 2014.

Appendix

A title-1

....

B title-2

....