ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΙΤΛΟΣ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

B. Riemann

ΕΠΙΒΛΕΠΩΝ: K.F.Gauss

Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
Σχολή Θετικών Επιστημών
Τμήμα Πληροφορικής

Το περιεχόμενο αυτής της εργασίας δεν απηχεί απαραίτητα τις απόψεις του Τμήματος, του Επιβλέποντα, ή της επιτροπής που την ενέκρινε.

Υπεύθυνη Δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας, και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης, βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Πληροφορικής του Αριστοτέλειου Πανεπιστημίου Θεσσαλονίκης.

(Υπογραφή) ....

Riemann

Abstract

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

The purpose of this thesis is to ....

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

Contents

Introduction bla bla

1 Turing Machine

1.0.1 Enigma

example of code

```
from itertools import imap

def KSA(key):
  S = range(256)
  j = 0
  for i in range(256):
    j = (j + S[i] + key[i % len(key)]) % 256
    S[i], S[j] = S[j], S[i]
  return S
```

2 Gauss Reduction

3 Background

bla bla

3.1 Linear Systems

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

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

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

4 Gauss reduction - single core case

4.1 Algorithms in LaTex

Alogrithm 4.1.1 *: Multiplication of Karatsuba*
input. a, b *integers*
output. $a \cdot b$

def karatsuba(a, b)
 if $a < 100$ *or* $b < 100$ **then**
  return $a \cdot b$
end
 $m = \max(\log_{10}(a), \log_{10}(b))$
 $m_2 = floor(m/2)$
 $high(a)$ = take the first m_2 decimal digits of a
 $low(a)$ = take the last m_2 decimal digits of a
 $high(b)$ = take the first m_2 decimal digits of b
 ...
 ...
 ....
print $(z_2 \cdot 10^{2m_2} + (z1 - z2 - z0) \cdot 10^{m_2} + z_0$

Alogrithm 4.1.2 *: Enumeration algorithm*

input. *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.

output. *All the vectors*$\mathbf{x} \in$ Š $\mu\epsilon$ $\|\mathbf{x}\| \leq R$.

Compute $\{\mu_{ij}\}$ and $B_i = \|\mathbf{b}_i^*\|^2$

$\mathbf{x} = (x_i) \leftarrow \mathbf{0}_n, \mathbf{c} = (c_i) \leftarrow \mathbf{0}_n$, ‘ = (‘$_i$) $\leftarrow \mathbf{0}_n$, *sumli* $\leftarrow 0, S = \emptyset, i \leftarrow 1$

While $i \leq n$

    $c_i \leftarrow -\sum_{j=i+1}^{n} x_j \mu_{ji}$

...

return S

5 see the tutorlias

Appendix

Installation of Cuda

bla bla

Experiments