System and Network Security (CS 5470)

Mid Semester Examination - 1 (Spring 2017)

International Institute of Information Technology, Hyderabad

Time: 1 Hour and 30 Minutes Total Marks: 40

Instructions: Answer ALL questions.
This is a closed books and notes examination.
Write your answers sequentially as given in the question paper and also all the parts of a question at the same place.
No query is allowed in the examination hall.
Use of Regular Calculator is allowed.

A ≤ B , ∀ A∈NP

7^{17} mod 23)

196
−14
184

1. **(a)** Define the classes *NP-hard* and *NP-complete*.
Explain the significance of NP-hard problem in the context of cryptography.

(b) Define the class *P*.
Let $G = (V, E)$ be a directed graph, where V be the set of nodes and E the set of edges of G. Let $\langle G \rangle$ denote the encoding of the graph G either in adjacency matrix or link list representation. Define the following formal problem as given below:
$PATH := \{\langle G, s, t\rangle | G$ is a directed graph with a path from node s to node t.
Prove or disprove that $PATH \in P$.

[(2+3) + (1+4) = 10] 5+5

2. **(a)** Using the repeated square and multiply algorithm, compute the modular exponentiation 7^{38} (mod 23).

(b) What do you mean by *unconditionally secure* and *computationally secure* schemes?
Classify and explain the attacks based on passive and active attacks with respect to a two-party communication model.

(c) Find the probability of success in the Miller-Robin primality test algorithm that a tested number n is prime.

[4 + (2+3) + 3 = 12] 11.5 3.5+5+6 8.5

7 mod 23 = 7
7^2 mod — 3
7^4 — 9
7^8 — 12
7^{16} —
7^{32} =
3×9×13
6
24
18

3. **(a)** Consider the plaintext as "attack postponed until two am". Let the encryption key e be a permutation (4 3 6 1 2 5). Using the transposition technique, answer the following two parts:
6(i) Encrypt the plaintext message using the encryption key e.
13(ii) Decrypt the ciphertext produced in Part (i) with the key e.

4	3	6	1	2	5
a	t	t	a	c	k
~~o~~ p	o	s	t	p	
o	n	e	d	_	u
n	t	i	l	t	_
t	w	o	_	a	m

asdl_ct_latpntwa_ontkpu_mtoeio

1 2 3 4 5 6
a s d l _ c
t _ l a t p

351
26

529

2.5

(b) Explain how the confidentiality and authentication are achieved using the public key cryptosystem. Show it with a diagram.

[(2 + 2) + 4 = 8]

4. (a) Explain the RSA public key cryptosystem with the key generation, encryption and decryption phases.

(b) Briefly explain the architecture of the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool used to verify formally that whether a security protocol is safe or unsafe against an intruder for replay and man-in-the-middle attacks.
Also, mention the significance of the declarations: *secret*, *witness*, and *request* used in the high-level protocol specification language (HLPSL) of AVISPA tool.

[(2+1+1) + (3 + 3) = 10]

***************** End of Question Paper ********************

W

Database Systems: 1st Mid

Date: 7th February 2017

Duration: 1.5 hrs

1. **No clarifications during the exam.**
2. Make *reasonable assumptions* and *clearly state* them to answer *ambiguous* questions.
3. Show your steps. Be concise and organized.
4. Calculators allowed. Sharing of calculators *not* allowed.

1) The Megatron 747 disk has the following characteristics:

1. There are 4 platters providing 8 surfaces, with 8192 tracks per surface.
2. Tracks hold an average of 256 sectors of 512 bytes each.
3. 10% of each track is used for gaps.
4. The disk rotates at 3840 rpm.
5. The time it takes the head to move n tracks is 1+0.002n milliseconds.

(a) What is the capacity of the disk?

(b) If all tracks hold the same number of sectors, what is the density of bits in the sectors of a track?

(c) What is the maximum seek time?

(d) What is the maximum rotational latency?

(e) If a block is 16,384 bytes (i.e. 32 sectors), what is the transfer time of a block?
16384 bytes (ie 32 sectors)

2) We have a 1 GB sized relation R of 10,000,000 tuples. Each tuple of 100 bytes has several fields, one of which is the sort key field, which may not be a primary key. The machine on which sorting occurs has one Megatron 747 disk (described above in Q1) and 50 MB of main memory available. Disk blocks are 4096 bytes. How long would it take to sort R using 2-phase, multiway merge sort. **[10]**

3) Suppose we are using RAID level 4 (i.e. 1 redundant disk for parity), with 4 data disks and 1 redundant disk. For simplicity, assume blocks are a single byte. **[10]**

(a) Give the block of the redundant disk if the corresponding blocks of the data disks are: 01110010, 10000111, 10001011, and 11000011.

(b) Data disk 1 has failed. Recover the block of that disk if the contents of disks 2 through 4 are: 01110010, 10000111, 10001011, while the redundant disk holds 11000011.

[10]

4) Suppose we swizzle all pointers automatically, we can perform the swizzling in half the time it would take to swizzle each one separately. If the probability that a pointer in main memory will be followed at least once is *p*, for what values of *p* is it more efficient to swizzle automatically than on demand? **[10]**

5) Suppose blocks hold either 4 records, or 12 key-pointer pairs. As a function of *n*, the number of records, how many blocks do we need to hold a data file and:
(a) A dense index?   (b) A sparse index? **[10]**

automatic swizzing (as) – takes more time
for 'as' to be efficient, no. of accesses to be less
bcoz more accesses, more time
∴ $p < 1/2$

44.559 deg $\frac{3}{256} \times 36 + \frac{4}{256} \times 324$
5.484 deg

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

MID SEMESTER EXAMINATION-1
IIIT, Hyderabad, Spring 2017
Subject: Introduction to Parallel Scientific Computing (Code: TS17005)

08.02.2017
18:00 - 19:30

Duration: 1.5 hours

Instructor: Dr. P. Kumar

Maximum Marks: 41

Instructions

There are 2 pages and 7 questions. All questions are compulsory. This paper is divided into two sections: *Section A*: Basic Matrix Computations and *Section B*: Matrix Factorizations. It is not necessary to indicate section numbers in your answer sheet. Calculator is allowed.

Section A: Basic Matrix Computations (5 Questions, 15 Marks)

1. Given $A \in \mathbb{R}^{n\times n}, u, v \in \mathbb{R}^n$. Write an efficient algorithm to compute $A + uv^T$. Note that u and v are column vectors. Determine the flop count. [2]

2. Given a lower triangular matrix $L \in \mathbb{R}^{n\times n}$, a upper triangular matrix $U \in \mathbb{R}^{n\times n}$, a diagonal matrix $D \in \mathbb{R}^{n\times n}$, and a vector $b \in \mathbb{R}^n$. Write an efficient algorithm to compute x from $LDUx = b$. Determine flop count. [2]

3. Given a block matrix

$$A = \begin{bmatrix} A_{11} & A_{12} & A_{13} & \cdots & A_{1p} \\ A_{21} & A_{22} & A_{23} & \cdots & A_{2p} \\ \vdots & \vdots & \ddots & \cdots & \vdots \\ A_{p1} & A_{n2} & A_{n3} & \cdots & A_{pp} \end{bmatrix}_{np\times np} \begin{pmatrix} A_{11} \\ A_{12} \\ A_{13} \end{pmatrix}$$

where each block A_{ij} is a $n \times n$ matrix. Write an efficient algorithm to compute AA^T. Determine flop count. [2]

4. Given $A \in \mathbb{R}^{m\times n}$ and $B \in \mathbb{R}^{p\times q}$. Write an efficient algorithm to compute the tensor product $A \otimes B$. [4]

par 5. If $x \in \mathbb{C}^n$ and $n = 2^t$, where t is a positive integer, then write an algorithm that computes the discrete Fourier transform $y = F_n x$. Discuss the essential steps involved by doing a Fourier transform for [5]

algo par

$$x = \begin{bmatrix}1\\0\\0\\1\\0\\1\\0\\0\end{bmatrix}. \quad b(i) = \frac{b(i) - U(i, i+1:n)\, b(i+1:n)}{U(i,i)}$$

$b(2) = \frac{b(2) - U(1,2)\, b(1)}{U(1)}$

b1
b2
b3 = B

U(2, 2:n)

Section B: Matrix Factorizations (2 Questions, 26=9+17 Marks)

6. (LU Factorization) [1+1+1+3+3]

   i) Given a lower triangular matrix $L \in \mathbb{R}^{n\times n}$ and $b \in \mathbb{R}^n$, write an algorithm to solve $Lx = b$, which is a forward substitution.

   ii) Similarly, given an upper triangular matrix $U \in \mathbb{R}^{n\times n}$, write an algorithm to solve $Ux = b$, which is a backward substitution.

   iii) Write an algorithm to solve $LUx = b$ by first solving $Lt = b$ then by solving $Ux = t$. Determine flop counts.

   iv) Write an algorithm to compute the LU factorization for a given matrix $A \in \mathbb{R}^{n\times n}$. The L and U factors must be stored (overwritten) in A. Describe the steps of LU factorization for the following matrix

$$A = \begin{bmatrix} 3 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

$\frac{n(n-1)}{2}$

$2(1+3)$ $\quad n(n-1)$

$$\begin{bmatrix} 1 & & \\ 0 & 1 & \\ 1/3 & 1/2 & 1 \end{bmatrix} \begin{bmatrix} 3 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2/3 \end{bmatrix}$$

Estimate flop count.

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix} \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$$

$a_{11}c_{11}$ $\quad a_{11}c_{12}$ $\quad a_{12}c_{21}$ $\quad a_{12}c_{22}$

$\frac{n(n-1)}{2}$ $\quad \frac{1}{3} + \frac{2}{3}$

$I_4 \quad \sqrt{2} \quad -\sqrt{2}$

Please go on to the next page. . .

Student's name:

v) Describe a variant of Gaussian elimination that introduces zeros into the columns of A in the order $n : -1 : 1$, i.e., it first creates zeros above the diagonal in the last column, then it creates zeros above the diagonal in the second last column, and so on such that the matrix reduces to lower triangular matrix. This produces the (UL) factorization $A = UL$, where U is a unit upper triangular and L is a lower triangular matrix.

7. **(QR Factorization)** [3+3+3+3+2+3]

i) Given a vector $v \in \mathbb{R}^n$. Write an algorithm to compute the Householder matrix. Check your algorithm for the vector

$$v = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}.$$

ii) Write an algorithm to compute the QR factorization of a given matrix $A \in \mathbb{R}^{n \times n}$. Show the steps involved for the following matrix

$$A = \begin{bmatrix} 3 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

Determine the flops involved in the QR factorization.

iii) Write an algorithm to compute the LQ factorization of a given matrix $A \in \mathbb{R}^{n \times n}$, where L is now the lower triangular matrix, and Q is orthonormal. [Hint: In QR you create zeros below the diagonal, for LQ you need to create zeros above the diagonal.]

iv) Let $x \in \mathbb{R}^n$. Consider $G(i,k) \in \mathbb{R}^{n \times n}$ defined as follows

$$G(i,k) = \begin{bmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & c & \cdots & s & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & -s & \cdots & c & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{bmatrix}.$$

In the matrix above, (i,i)−th entry is c, the (i,k)−th entry is s, the (k,i)−th entry is $-s$, and the (k,k)−th entry is c. By choosing

$$c = \frac{x_i}{\sqrt{x_i^2 + x_k^2}}, \qquad s = -\frac{x_k}{\sqrt{x_i^2 + x_k^2}},$$

the kth entry of $y = G(i,k)^T x$ is zero. It can also be seen that by multiplying $G(i,k)^T$ with the vector x, only the i−th and k−th entries of vector x are modified. Use this idea to convert a matrix $A \in \mathbb{R}^{n \times n}$ given as follows

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & A_{1n} \\ a_{21} & a_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{bmatrix}$$

into an upper triangular matrix. [Hint: Create zeros below a_{11} in the first column, then create zeros below $(2,2)$−th entry in the second column (of the transformed matrix), and so on until you obtain an upper triangular matrix.]

v) Given $A \in \mathbb{R}^{m \times n}, m > n$, using QR factorization above, write an algorithm to find the least squares solution to the linear system $Ax = b$.

vi) Given a symmetric matrix $A \in \mathbb{R}^{n \times n}$, write an algorithm that transforms the matrix A into a tridiagonal matrix using Lanczos tridiagonalization. Estimate the flop count.

End of exam

Student's name:

International Institute of Information Technology, Hyderabad
CSC471 (Spring 2017): Statistical Methods in AI
Mid Term - 1

Instructions:

- *Be concise and precise in your answers and avoid verbosity.*
- *If any question is ambiguous, state so, and clearly write any assumption that you take before the answer.*
- *Clearly define every new mathematical notation used in the answer sheet and don't skip important algebraic manipulations in derivations.*
- *Use of scientific calculator is allowed.*

Max. Points: 25 [Time: 90 Mins]

1. Let $S = \{(\mathbf{x}_1, y_1), \ldots, (\mathbf{x}_m, y_m)\}$ be the training set where $\mathbf{x}_i \in \Re^d$, $y_i \in \{+1, -1\}$, $\forall i \in \{1, \ldots, m\}$. For every $\mathbf{x}_i \in C_1$, there exists a $-\mathbf{x}_i \in C_2$. Show that, in this case, the linear classifier learnt using least square approach must pass through the origin. [2 Points]

2. Let $V = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ and $W = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$ both form two different bases for the same vector space, then show that $m = n$. [5 Points]

3. Consider the following classification problem. $\mathbf{x}_1 = [1 \quad 1]^T$, $\mathbf{x}_2 = [2 \quad 2]^T$, $\mathbf{x}_3 = [2 \quad 0]^T$, $y_1 = 1$, $y_2 = 1$, $y_3 = -1$. Use the Perceptron learning algorithm to show that the decision boundary is $\mathbf{w}^T\mathbf{x} + b = 0$ where $\mathbf{w} = [-1 \quad 3]^T$, $b = 1$. [4 Points]

4. Given that $\mathbf{w}^T\mathbf{x} + b = 0$ represents a hyperplane in $\Re^d$ where $\mathbf{w} \in \Re^d$, $b \in \Re$.

   (a) Show that $\mathbf{w}$ is normal to the hyperplane. [1 Point]

   (b) Derive the formula for the distance of a point $\mathbf{x}_1$ from the hyperplane? [2 Points]

   (c) What is the distance of origin from the hyperplane? [1 Point]

5. Let $\mathbf{x}_1 = [2 \quad 1]^T$, $\mathbf{x}_2 = [3 \quad 4]^T$, $\mathbf{x}_3 = [5 \quad 0]^T$, $\mathbf{x}_4 = [7 \quad 6]^T$, $\mathbf{x}_5 = [9 \quad 2]^T$. Employ Principal Component Analysis (PCA) to find the one dimensional representation (along the direction of maximum variance) of the data points given below. Provide the eigen decomposition steps in detail. **[4 Points]**

6. Let $S = \{(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \ldots, (\mathbf{x}_m, y_m)\}$ be the training set where $\mathbf{x}_i \in \Re^d$; $y_i \in \{+1, -1\}$; $\forall i = 1 \ldots m$. Let $Y = [y_1 \quad y_2 \quad \cdots \quad y_m]^T$. Also, let $\hat{Y} = [\hat{y}_1 \quad \hat{y}_2 \quad \cdots \quad \hat{y}_m]^T$, where $\hat{y}_i$ be the predicted value for $\mathbf{x}_i$ using least square solution.

   (a) Derive the linear classifier learnt by least square method. [3 Points]

   (b) Show that $\hat{Y}$ is orthogonal to $Y - \hat{Y}$. [1 Point]

7. Let $\mathbf{x}_1 = [0 \quad 0]^T$, $\mathbf{x}_2 = [1 \quad 1]^T$, $\mathbf{x}_3 = [1 \quad 0]^T$, $\mathbf{x}_4 = [0 \quad 1]^T$, $y_1 = 1$, $y_2 = 1$, $y_3 = -1$, $y_4 = -1$. Algebraically show that this set is not linearly separable. (Hint : Show by contradiction.) [2 Point]