VGU WS20/21
Study Program: Computer Science

Instructor: Huong Tran

Final exam: Algebra

Personal information:

Your full name:	
Student ID:	
Signature:	

Result (Please do not fill in these cells). 15.0 **points** is sufficient to pass the exam.

Problem	1	2	3	4	5	6	7	8	$\sum$
Maximum scores	5	5	3.5	3.5	2.5	3.0	3.5	4	30
Obtained scores									

Remarks:

- You are allowed to bring a two-sided A4 sheet with any contents. No calculator please.
- Exam duration: 90 minutes.
- Write on every page your name and your student ID.
- Hand in **all** results you want to be assessed.
- Copying and cheating in any form are strictly prohibited and result to a failing grade
- Write your answers in the blank space below each question. You could ask for another blank sheet in case you need more space.

Name: Student ID:

1 Guidelines

- There are 8 questions, 10 pages in the exam booklet.
- For questions $1 - 2$: You are not expected to reason about your answers.
- For questions $3 - 8$: Please write your answers on the given blank space right below each subquestion. Detailed explanations are required to enable to get the maximum scores.

Name: Student ID:

2 Exam Questions

1. Binary Choice Questions. **5 P.**

   This exercise presents assertions, which you shall evaluate as true or false. Please proceed as follows:

   - If you are convinced, that the assertion is true, please **circle** the letter t for *true* on the left margin of the assertion.
   - If you are convinced, that the assertion is false, please **circle** the letter f for *false* on the left margin of the assertion.

   Every correct answer yields you one point, every false answer results in a subtraction of one point. If you do not answer to an assertion, no point is given. If the sum of your points in this exercise is negative, this exercise is rated with 0 points.

   t / f: Transpose of an invertible matrix is invertible.

   t / f: Given a square matrix A such that $\det A = 0$. Then the system $Ax = 0$ is inconsistent.

   t / f: Let S be a spanning set for a finite dimensional vector space V. Then, the dimension of V is equal to $|S|$, where $|S|$ denotes the number of elements of S.

   t / f: $-2020 \mod 7 = 4$.

   t / f: Let n denote an RSA modulus and e an RSA public exponent. Then e must satisfy $\gcd(e, \phi(n)) = 1$, where $\phi(n)$ is Euler' totient function of n.

2. Please **insert your answers** to underlined blanks next to corresponding questions **5 P.**

   (a) Given matrices below

   $$B = \begin{bmatrix} 1 & 3 \\ 2 & -4 \\ 3 & 5 \end{bmatrix}, \quad C = \begin{bmatrix} -1 & 2 & -4 \\ 5 & 3 & -1 \end{bmatrix}.$$

   Then,

   $2B - C^T =$ _____

   (b) Given two vectors in $\mathbb{R}^2$: $u = (2, 3)$ and $v = (4, 1)$. The area of the parallelogram with edges u and v is equal to _____

   (c) Let A be a set $\{1, 2, \ldots, n\}$. There are total _____ subsets of A which contains both 1 and n.

(d) Given the matrix representation M_R for a binary relation R from a set of {**mouse, case**} to the set of {**black, white, orrange**} as below

$$M_R = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

All elements of R are

$R =$ {(M, b), (M, O), (C, W), (C, O)}.

(e) The plaintext of the cipher message **PHV CXII** using the Ceasar cipher, in which each letter is shifted 3 places(the alphabet [1] is given at the footnote.) to the right, is MES ZUFF

[1] A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Name: Student ID:

3. Consider the homogeneous linear system below **3.5 P.**

$$\begin{cases} x + 2y - z + 2t = 0 \\ 2x + 4y + z - 2t = 0 \\ 3x + 6y + 2z - 6t = 0 \end{cases} \quad (1)$$

(a) Write the coefficient matrix for the system 1. **1 P.**

$$\begin{pmatrix} 2 & 1 & -1 & 2 \\ 2 & 4 & 1 & -2 \\ 3 & 6 & 2 & -6 \end{pmatrix}$$

(b) Let W be the set of all solutions to the system. Prove that W is a vector subspace of $\mathbb{R}^4$. **1 P.**

(c) Find a basis and the dimension for W. **1.5 P.**

$\dim W = 1.$

Name: Student ID:

4. Given a matrix **3.5 P.**

$$A = \begin{pmatrix} 2 & 1 & 2 \\ 0 & 3 & -1 \\ 4 & 1 & 1 \end{pmatrix}.$$

(a) Prove that A is invertible **1 P.**

$\det A = 28 \neq 0 \Rightarrow A$ is invertible

(b) Find the inverse of A. **1.5 P.**

$$A^{-1} = \begin{pmatrix} 1/7 & -3/28 & 5/28 \\ -1/7 & 5/14 & 1/14 \\ -3/7 & 1/14 & 3/14 \end{pmatrix}$$

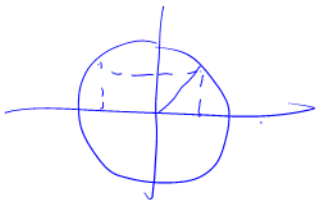
(c) Solve the system $Ax = b$, where $b = (1, 2, 1)$. **1 P.**

$$x = \begin{pmatrix} 3/28 \\ 9/14 \\ -1/14 \end{pmatrix}$$

Name: Student ID:

5. Let T be the rotation counterclockwise around the origin by an angle $\frac{\pi}{4}$. Knowing that T is a linear map from $\mathbb{R}^2$ to $\mathbb{R}^2$. Let $e_1 = (1,0)$ and $e_2 = (0,1)$ be two identity vectors in the standard basis of $\mathbb{R}^2$. **2.5 P.**

(a) Find $T(e_1)$ and $T(e_2)$. **1 P.**



$$T(e_1) = \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)$$

$$T(e_2) = \left(-\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)$$

(b) What is the matrix representation A for T in the standard basis $\{e_1, e_2\}$? **0.5 P.**

$$A = \begin{pmatrix} \sqrt{2}/2 & -\sqrt{2}/2 \\ \sqrt{2}/2 & \sqrt{2}/2 \end{pmatrix}$$

(c) Find $T^2(3e_1 - 2e_2)$, where T^2 denote the composition map of T and itself. **1 P.**

$$T^2(3e_1 - 2e_2) = A^2 \begin{pmatrix} 3 \\ -2 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

other way:

- T^2 is the rotation around the origin by angle $\frac{\pi}{4} \cdot 2 = \frac{\pi}{2}$.

Name: Student ID:

6. Propositional logic **3 P.**

(a) Show that propositions **1 P.**

$$p \to q, \text{ and } \neg p \vee q$$

are logically equivalent?

(b) Please negate the following propositions without using conditional (Hint. the tautology in 6a may be useful for eliminating conditionals).

i. *I have no special talent and I am only passionately curious.* **0.5 P.**

I have a special talent or I am not only passionately curious

ii. $(p \vee q) \to r$ **0.5 P.**

$(p \vee q) \wedge \neg r$

(c) Use a truth table to determine the validity of the argument: **1 P.**

If the exam questions are easy, you will pass the exam. You passed the exam. Therefore, the exam questions are easy.

The argument is invalid.

Name: Student ID:

7. (Propositional logic)

(a) Use the truth table to verify the first De Morgan law:

$$\neg(p \vee q) = \neg p \wedge \neg q.$$

(b) Please negate the following propositions without using the conditional.

"If a machine is expected to be infallible, it cannot also be intelligent."

$p \to \neg q \quad = \quad \neg p \vee \neg q \quad = \quad p \wedge q.$

(c) A boolean formula is **satisfiable** if it is possible to find an assignment of variables to values that makes the formula true. For instance, the formula $\phi = p \vee q \wedge r$ is satisfiable as if we assign $p = T$, $q = F, r = T$, then $\phi = T \vee \mathbb{F} \wedge T = T \vee F = T$. Show that the following statement is satisfiable

$$(p \to q) \wedge (p \to \neg q).$$

$p = F, \; q = T.$

(d) Show the validity of the following inference:

Jasmine is skiing or it is not snowing. It is snowing or Bart is playing hockey. Therefore, Jasmine is skiing or Bart is playing hockey.

Name: Student ID:

8. (Relation) Let A_n be the set of bit strings of length n. For instance, $A_1 = \{0, 1\}$ the set of strings of length 1. Let R_n be a binary relation on A_n such that $(s, t) \in R_n$ if s and t are strings of A_n with the same number of occurrences of 1s. For instance, $(001, 100) \in R_3$ and $(000, 110) \notin R_3$.

   (a) List all elements of R_2.

   $R_2 = \{(00,00), (01,01), (01,10), (10,01), (10,10), (11,11)\}$

   (b) Write down the matrix representation for R_2.

	00	01	10	11
00	1	0	0	0
01	0	1	1	0
10	0	1	1	0
11	0	0	0	1

   (c) Circle, you are not expected to reason about your answers, properties below that R_n is:

   i) Reflexive;
   ii) Symmetric;
   iii) Anti-symmetric;
   iv) Transitive;
   v) partial ordering;
   vi) equivalent.

   (d) Choose your appropriate question to follow:

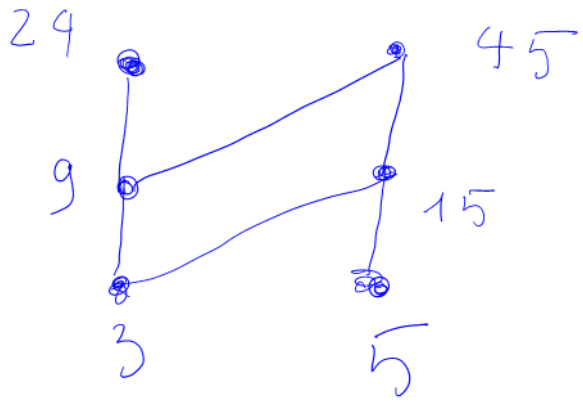
   I. If you circled item (v) above ((8c)), then draw the Hasse diagram for R_3.

   II. If you circle item (vi) above ((8c)), then show the partition on A_3 corresponding to the relation R_3.

   $A_3 = \{00\} \cup \{01, 10\} \cup \{11\}$

Name: Student ID:

III. Otherwise, draw Hasse diagram for the divisibility relation S on $B = \{3, 5, 9, 15, 24, 45\}$. Recall that the divisibility relation: $(a, b) \in S$ if and only if a divides b.



9. *Hint:* Please use your own matriculation number for doing this question. Assume that $x = x_1x_2 \dots x_k$ is your matriculation number.

   (a) Please find $\sum_{i=1}^{k} ix_i \mod 11$.

   (b) To reduce errors while inputting a matriculation number, one attaches a check-digit x_{k+1} to the last position of x such that $\sum_{i=1}^{k+1} ix_i \mod 11 = 0$. Notice that we denote the attached number 10 by the capital letter X if $x_{k+1} = 10$. Please find your own-check digit.

Name: Student ID:

10. Bob considers a small RSA public-key crypto-system with modulus $n = 91$ and the non-trivial second smallest valid exponent e.

(a) Find Euler's totient function $\phi(n)$.

$\phi(91) = \phi(7 \cdot 13) = (7-1)(13-1)$

$= 72$

(b) Please help Bob finding the public exponent e.

$\gcd(e, \phi(n)) = 1$

$\rightarrow e = 7$

(c) After finding e. He sends the public key which is a pair (n, e) to Alice. On behalf of Alice, please encrypt the message $x = 87$. In case you cannot find e in (10b), please assume that $(n, e) = (91, 11)$.

$y = x^e \bmod n$

$87^7 \bmod 91 = 87$

(d) Please help Bob finding the private exponent d using the extended Euclid's algorithm.

$(n, e) = (91, 7)$

$d = 31.$

(e) In a large RSA public-key crypto-system, what is the risk if Alice chooses the plaintext x which is not relatively prime with n? Propose an efficient way that the attacker may apply for finding the private exponent.