VGU WS19/20
Field of study: Computer Science
Lecturers: Huong Tran

Practice Test: Algebra

Personal information:

Your full name:	
Student ID:	
Signature:	

Remarks:

- This is a closed document exam. No calculator please.
- Duration of examination: 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.

1. (a) What is the inner product of $\vec{a} = (1, -3, 2, 9)$ and $\vec{b} = (2, -2, 1, 0)$? **Solution.** $(1, -3, 2, 9) \cdot (2, -2, 1, 0) = 1.2 + (-3).(-2) + 2.1 + 9.0 = 10$.

   (b) Let A, B, C be matrices as follows:

$$A = \begin{bmatrix} 1 & 2 & -1 \\ 2 & 3 & 0 \\ -1 & 3 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 1 & -1 \\ 2 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} -1 & 2 & 0 \\ 1 & 0 & -3 \end{bmatrix}.$$

   Find the matrix $AB + 2C^T$.

   Solution $AB + 2C^T = \begin{bmatrix} 1 & -3 \\ 5 & -3 \\ 6 & -1 \end{bmatrix} + \begin{bmatrix} -2 & 2 \\ 4 & 0 \\ 0 & -6 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 9 & -3 \\ 6 & -7 \end{bmatrix}$

   (c) Are these following vectors linearly independent or linearly dependent?

$$u = (1, 0, 0), \quad v = (0, 1, 1), \quad w = (1, 1, 1).$$

   Solution: Linearly dependent since $w = u + v$.

   (d) Given a matrix M of size 5×5 with $\det(M) = 2$. Then,

   - $\det(M^T) = \underline{2}$.
   - $\det(-2M^2) = (-2)^5(\det M)^2 = \underline{-128}$.

2. Consider the following system of equations in x in real numbers:

$$\begin{cases} x_1 + 2x_2 + \lambda x_3 = -3, \\ -2x_1 + x_2 - 2\lambda x_3 = 6, \\ 2x_1 + 5x_2 - x_3 = 3, \end{cases} \qquad (1)$$

   where $\lambda \in \mathbb{R}$ is a parameter.

   (a) Write down the coefficient matrix, and augmented matrix of system (1)

   Solution: The coefficient and augmented matrices respectively of the system are

$$A = \begin{pmatrix} 1 & 2 & \lambda \\ -2 & 1 & -2\lambda \\ 2 & 5 & -1 \end{pmatrix} \text{ and } A|b = \begin{pmatrix} 1 & 2 & \lambda & -3 \\ -2 & 1 & -2\lambda & 6 \\ 2 & 5 & -1 & 3 \end{pmatrix}.$$

(b) Determine the determinant of the coefficient matrix of system (1). For which λ the system has a unique solution?

Solution: Using the expansion along the first row we get

$$\det A = 1.(-1)^{1+1}\begin{vmatrix}1 & -2\lambda\\ 5 & -1\end{vmatrix} + 2.(-1)^{1+2}.\begin{vmatrix}-2 & -2\lambda\\ 2 & -1\end{vmatrix} + \lambda.(-1)^{1+3}.\begin{vmatrix}-2 & 1\\ 2 & 5\end{vmatrix} = -10\lambda - 5.$$

The system has unique solution if and only if $\det A \neq 0$. Hence, $-10\lambda - 5 \neq 0$, equivalently, $\lambda \neq -\frac{1}{2}$.

(c) For $\lambda = 1$, compute x_2 using Cramer's rule.

Solution: By Cramer's rule for $\lambda = 1$, we have

$$x_2 = \frac{\begin{vmatrix}1 & -3 & 1\\ -2 & 6 & -2\\ 2 & 3 & -1\end{vmatrix}}{\det A} = \frac{-3\begin{vmatrix}1 & 1 & 1\\ -2 & -2 & -2\\ 2 & -1 & -1\end{vmatrix}}{\det A} = 0,$$

since the numerator matrix has two columns equal.

3. **Elementary Operations and Null Spaces**

Given a matrix

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

(a) Use elementary row operations to reduce A to an echelon form A^* of A.

Solution: On the whiteboard!

(b) Circle pivot elements for A^*. What is the dimension for the null space of A?

Solution: A^* has 3 non-zero rows corresponding to 3 pivots. Hence, the system $Ax = 0$ has 3 dependent variables and 2 free variables. Therefore, $\dim Null(A) = 2$. Detailed solution is upon on the request!

(c) Find a basis for the null space of A.

Solution: On the whiteboard!

4. **Linear transformations**

Prove that following map is a linear transformation.

$$\begin{aligned} T : \mathbb{R}^3 &\to \mathbb{R}^2 \\ (x, y, z) &\mapsto (2x + y, 2y - z) \end{aligned}$$

It is straightforward that T is well defined. Let $u = (x, y, z)$ and $v = (x', y', z')$ be arbitrary vectors on $\mathbb{R}^3$. We have

- $$\begin{aligned} T(u + v) &= T(x + x', y + y', z + z') \\ &= (2(x + x') + (y + y'), 2(y + y') - (z + z') \\ &= (2x + y, 2y - z) + (2x' + y', 2y' - z') \\ &= T(u) + T(v). \end{aligned}$$

- $$\begin{aligned} T(\alpha u) &= T(\alpha x, \alpha y, \alpha z) \\ &= (2\alpha x + \alpha y, 2\alpha y - \alpha z) \\ &= \alpha(2x + y, 2y - z) \\ &= \alpha T(u). \end{aligned}$$

By the definition of linear map, T is linear.

5. Dual Choice Questions, 10 pts.

   This exercise presents assertions, which you shall evaluate as true or false. You are not expected to reason about your answers. Please proceed as follows:

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

   Solution:

$\underline{\text{t}}$ / f: We have $\varphi(1024) = 512$ for Euler's totient function.

t / $\underline{\text{f}}$: Let F and T denote False and True values respectively. Then, the truth value of the expression

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

is F if $p = F, q = T, r = T$.

t / $\underline{\text{f}}$: We have $11^{-1} \equiv 13 \bmod 16$, where 11^{-1} is the multiplicative inverse of 11 in $\mathbb{Z}_{16}$.

t / $\underline{\text{f}}$: Let $R = \{(a,a),(a,b),(b,a),(b,b),(c,a),(d,c),(d,d)\}$ be a binary relation on the set $\{a,b,c,d\}$. Then, R is reflexive.

t / $\underline{\text{f}}$: On the integer set $\mathbb{Z}$, the "divide relation",

$$R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : a \mid b\},$$

is an equivalence relation.

$\underline{\text{t}}$ / f: It is false that the solution set of an inhomogeneous set of linear equations always comprises at least one element.

$\underline{\text{t}}$ / f: Let $n \in \mathbb{N}_0$. If M is a set with $|M| = n$, then we have $|\mathcal{P}(M)| = 2^n$ for its power set $\mathcal{P}(M)$.

t / $\underline{\text{f}}$: Suppose that A and B are subsets of a set $U = \{1,2,3,4,5,6,7,8\}$. Knowing that corresponding binary strings of A and B are 1010 0010 and 1100 1011 respectively. Then, $1 \in A \cap B$ and $6 \in A \cup B$.

$\underline{\text{t}}$ / f: The encryption function of Turing's cipher (version 2) is $c \equiv m \cdot e \bmod n$, where m is the plaintext, c the corresponding ciphertext, and e is the private key such that $gcd(e,n) = 1$.

t / [✓ f]: Let n denote an RSA modulus and e an RSA public exponent. Then e must satisfy $\gcd(e, n) = 1$.

6. Propositional logic.

   (a) Please prove the following logical equivalence:

$$(\mathcal{A} \Rightarrow \mathcal{B}) \quad \Leftrightarrow \quad (\neg\mathcal{B} \Rightarrow \neg\mathcal{A}) \; .$$

Solution:

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \Rightarrow \mathcal{B}$	$\neg\mathcal{B}$	$\neg\mathcal{A}$	$\neg\mathcal{B} \Rightarrow \neg\mathcal{A}$	$(\mathcal{A} \Rightarrow \mathcal{B}) \Leftrightarrow (\neg\mathcal{B} \Rightarrow \neg\mathcal{A})$
w	w	w	f	f	w	w
w	f	f	w	f	f	w
f	w	w	f	w	w	w
f	f	w	w	w	w	w

   (b) Please negate the following propositions or terms:

   i. $\mathcal{A} \wedge \neg\mathcal{B}$

   ii. $(\mathcal{A} \wedge \mathcal{B}) \Rightarrow \mathcal{C}$

Solution:

i.

$$\neg(\mathcal{A} \wedge \neg\mathcal{B}) \Leftrightarrow \neg\mathcal{A} \vee \neg(\neg\mathcal{B}) \text{ de Morgan } \Leftrightarrow$$

$$\Leftrightarrow \neg\mathcal{A} \vee \mathcal{B} \text{ double negation is statement itself}$$

ii.

$$\neg((\mathcal{A} \wedge \mathcal{B}) \Rightarrow \mathcal{C}) \Leftrightarrow \neg(\neg(\mathcal{A} \wedge \mathcal{B}) \vee \mathcal{C}) \text{ Conditional disjunction } \Leftrightarrow$$

$$\Leftrightarrow \neg\neg(\mathcal{A} \wedge \mathcal{B}) \wedge \neg\mathcal{C} \text{ de Morgan } \Leftrightarrow$$

$$\Leftrightarrow (\mathcal{A} \wedge \mathcal{B}) \wedge \neg\mathcal{C} \text{ Double negation}$$

   (c) Rewrite the following statements without using the conditional:

   i. If it is cold he wears a hat.

   ii. If productivity increases, then wages rise.

Solution: Key aspect: Implication is equivalent to $\neg\mathcal{A} \vee \mathcal{B}$

   i. It is not cold or he wears a hat.

   ii. Productivity does not increase or wages rise.

7. **Relations**

On a website network, a binary relation R is defined as follows: A pair of two websites (A, B) is in R if and only if there is a link to website B from website A. Let us consider a website network of 4 websites $\{A, B, C, D\}$ such that there are links

- from A to C;
- from B to D;
- from C to A;
- from D to B;

(a) Find the boolean matrix representation M_R for R.

Solution:

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

(b) Which properties below does R have? Why?

- Reflexive **Solution:** No, since $(A, A) \notin R$.
- Symmetric
  Solution: Yes, since $M_R = M_R^T$.
- Transitive
  Solution: No since $(A, C) \in R$ and $(C, A) \in A$, but $(A, A) \notin A$.

(c) Find the transitive closure R^* for R.

Solution: Using Warshall's algorithm: $W_i = W_{i-1} \vee$ column i of $W_{i_1} \odot$ row i of W_{i-1} given $W_0 = M_R$. We get sequentially,

$$W_1 = M_R \vee \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

$$W_2 = W_1 \vee \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

$$W_3 = W_1 \vee \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

$$M_{R^*} = W_4 = W_3 \vee \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Hence, $R^* = \{(A, A), (A, C), (B, B), (B, D), (C, A), (C, C), (D, B), (D, D)\}$.

(d) Show that R^* is an equivalence relation. Find the partition of the network corresponding to the equivalence relation R^*?

Solution: From the matrix representation of R^*, we imply that R^* is symmetric since $M_{R^*} = M_{R^*}^T$ and R^* is reflexive since all elements on the diagonal of M_{R^*} are 1. Finally, R^* is transitive since it is the transitive closure of R. Hence, R^* is an equivalence relation. Equivalence classes of R^* are $[A] = [C] = \{A, C\}$ and $[B] = [D] = \{B, D\}$, equivalently, the corresponding partition of the network is $\{A, C\} \cup \{B, D\}$.

8. The group $(\mathbb{Z}_n^\times, \cdot)$ and RSA, 11 pts.

   (a) Enumerate explicitly the sets $\mathbb{Z}_8^\times$ and $\mathbb{Z}_{11}^\times$.

   Solution:

   $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$ **1 P.**

   $\mathbb{Z}_{11}^\times = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ **1 P.**

   (b) Please compute the value $|\mathbb{Z}_{75}^\times|$ using Euler's totient function $\varphi(n)$ and its properties.

   Solution: $|\mathbb{Z}_{75}^\times| = \varphi(75) = \varphi(3 \cdot 25) = \varphi(3) \cdot \varphi(5^2) = (3-1) \cdot (5^2 - 5) = 2 \cdot 20 = 40$ **2 P.**

   (c) We consider the small RSA cryptosystem with $n = 77$. Please compute the smallest valid public RSA exponent e.

   Solution: $\varphi(77) = \varphi(7 \cdot 11) = \varphi(7) \cdot \varphi(11) = (7-1) \cdot (11-1) = 6 \cdot 10 = 2^2 \cdot 3 \cdot 5$

   Hence $e = 7$ is the smallest choice, because it's the smallest number with $\gcd(e, \varphi(n)) = 1$.

   (d) Making use of the RSA parameters $(77, e)$ from the previous problem part (c), please compute the corresponding private exponent d (the multiplicative inverse of e in $\mathbb{Z}_{\phi n}$).

   Hint: If you did not solve the previous task, please make use of $(n, e) = (77, 19)$.

   Solution: We first apply the classical Euclidian algorithm:

$$\begin{aligned} 60 &= 8 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

   As we expected, the gcd of $\varphi(n)$ and e is 1. We compute the private exponent by going bottom up:

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (7 - 4) = -7 + 2 \cdot 4 \\ &= -7 + 2 \cdot (60 - 8 \cdot 7) = -17 \cdot 7 + 2 \cdot 60 \end{aligned}$$

   Hence we have $7^{-1} \equiv -17 \equiv 43 \bmod \varphi(n)$.