上 海 交 通 大 学 试 卷

2021 – 2022 Academic Year (Spring Term)

Ve203 Discrete Mathematics
Midterm Exam

Name (Hanzi) _____ Name (Pinyin) _____

Student No. _____ Class No. _____

You have **100 minutes** to complete this evaluation. Please write your answers in this booklet. Remember to write neatly and clearly, so your answers can be fully understood. Make sure that you **explain your reasoning** in as detailed a manner as possible.

- You **may** bring a calculator of type "`Casio fx-991CN X`" or "`Casio fx-82`".
- You **may** use pencil, pen, eraser, ruler, compass and other non-electronic writing materials.
- You **may** use an English monolingual dictionary in book form — no electronic translators are allowed.
- The exam is **closed-book**. You may use the internet only for
  - Maintaining connection to Feishu;
  - Downloading exam paper from Feishu;
  - Uploading your answer files to canvas (or email to the instructor in case canvas malfunctions).

Pledge of Honor

The University of Michigan – Shanghai Jiao Tong University Joint Institute trusts its students to participate in examinations in an honorable and respectful manner, following a spirit of fairness and equality. Cheating, seeking unfair advantage and disturbing the safe and harmonious environment of examinations are contrary to the ethical principles of students of the Joint Institute. The letter and spirit of the Honor Code shall guide the behavior of students, faculty and all members of the Joint Institute. Therefore, I hereby declare that

(i) I will neither give nor receive unauthorized aid during the present examination, nor will I conceal any violations of the Honor Code by others or myself.

(ii) I confirm that I have read and understood the rules and procedures for examination set out by SJTU. I will follow them to the best of my ability.

(iii) I understand that violating the rules and procedures for examinations or the Honor Code will lead to administrative and/or academic sanctions.

Date: _____

Signature: _____

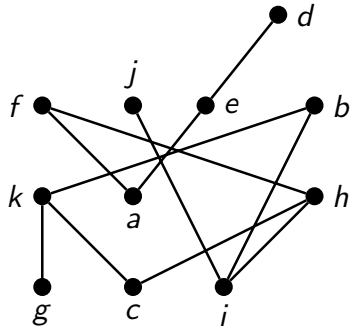
Exercise	Points	Score	Signature
1	10		
2	10		
3	20		
4	20		
5	20		
6	20		
Total	100		

Exercise 1 (10 points)
Given an infinite set A, show that A is **NOT** equinumerous to its power set 2^A.

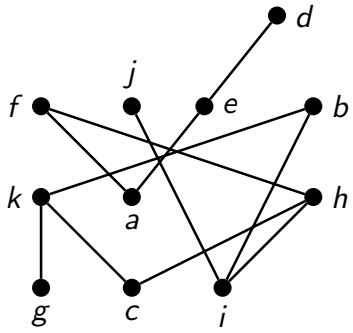
Exercise 2 (10 points)

Given group H. Define a map $i : \mathsf{Hom}(\mathbb{Z}, H) \to H$, that maps to each element $h \in H$ the group homomorphism $i_h : (\mathbb{Z}, +) \to (H, \cdot)$, $n \mapsto h^n$. Show that i (NOT i_h) is a bijection between the set of group homomorphisms $\mathbb{Z} \to H$ and the set of elements of H.

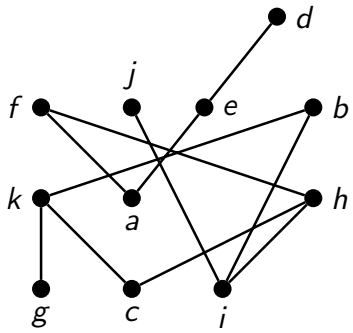
Exercise 3 (20 points)
Given a poset with the Hasse diagram below



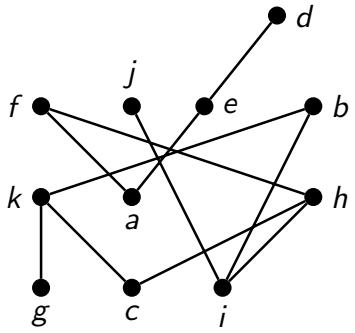
(i) (4 points) Find all points comparable to a. Write down the set explicitly as well as indicate it on the following diagram.



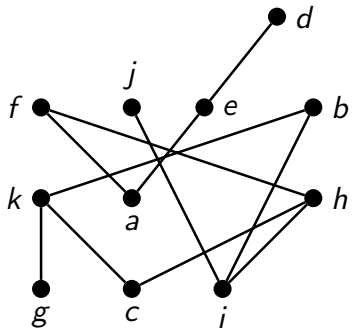
(ii) (4 points) Find all maximal chain(s) of size 2. Write down the set explicitly as well as indicate it on the following diagram.



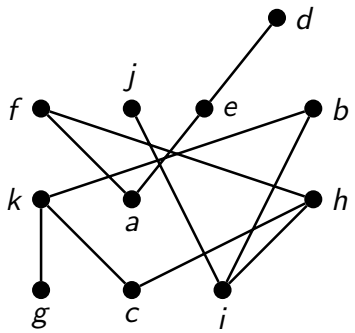
(iii) (4 points) Find a maximal antichain of size 3. Write down the set explicitly as well as indicate it on the following diagram.



(iv) (4 points) Find a chain partition of minimum size. Write down the partition explicitly as well as indicate it on the following diagram.



(v) (4 points) Find an antichain partition of minimum size. Write down the partition explicitly as well as indicate it on the following diagram.



Exercise 4 (20 points)

Given a poset $(P, \leq)$, let $\mathcal{M}(P)$ denote the set of all maximum antichains of P. Define the following relation on $\mathcal{M}(P)$ by

$$A \leq B \iff (\forall a \in A)(\exists b \in B)(a \leq b).$$

(i) (10 points) Show that $(\mathcal{M}(P), \leq)$ is a poset.

(ii) (10 points) Does $\mathcal{M}(P)$ always admit a MAXIMUM element? Prove or disprove (by exhibiting a counterexample) the statement.

Exercise 5 (20 points)

(i) (10 points) Given an odd integer a, use induction to show that for all $n \in \mathbb{N}$, $n \geq 3$,

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}$$

(ii) (10 points) Find all $n \in \mathbb{N} \setminus \{0\}$ such that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is cyclic. Explain.

Exercise 6 (20 points)

In an RSA procedure, the public key is chosen as $(n, E) = (2117, 97)$, i.e., the encryption function e is given by

$$e(x) = x^{97} \pmod{2117}$$

(Note that $2117 = 29 \times 73$.)

(i) (10 points) Compute the private key D, where $D = E^{-1} \pmod{\varphi(n)}$. Show your work.

(ii) (10 points) Decrypt the message 1465, that is, find x if $y = e(x) = 1465 \pmod{2117}$. Show your work.