Kenmerk: EWI2021/TW/MOR/MU/Mod7/Exam1

Exam 1 DM, Module 7, Codes 202001360 & 202001364

Discrete Mathematics

Friday, March 28, 2025, 13:45 - 15:45

Answers to questions 1-5 need to be motivated, arguments and proofs must be complete. You are allowed to use a handwritten cheat sheet (A4, both sides) during the exam.

For information: This is the DM part of the exam; the entire exam consists of two parts:

Algorithms & Data Structures (ADS)	1h	(30 points) **next Monday's test**
Discrete Mathematics (DM)	2h	(60 points) **today's test**

The total is 30+60=90 points. Your grade is $1+0.1x$, x being the number of points, rounded to one digit. That means, you need 45 points to get a 5.5.

---

1. (4+5 points)

   (a) Consider $a \in \mathbb{Z}_{>0}$, and a prime number p. Prove that if $p \nmid a$ then $\gcd(a, p) = 1$.

   (b) Consider $a, b, c \in \mathbb{Z}_{>0}$ with $\gcd(a, b) = 1$ and $a|c$, $b|c$. Prove that $ab|c$.

2. (8 points) Prove that any graph $G = (V, E)$ consisting of k connected components, is acyclic (i.e., contains no cycle) if and only if $|V| - |E| = k$.

3. (10 points) Consider a simple, capacitated network $G = (V, E, c)$, where $s, t \in V$, and $c(e) = 1$ for all $e \in E$ are the (unit) the edge capacities.

   Suppose you are given a maximum (s, t)-flow f with *val*$(f) \geq 2$. Suggest how to identify, in $O(|V| + |E|)$ time, an edge $e' \in E$, such that after reducing the capacity of e' by one unit, the maximum (s, t)-flow f^* in the remaining network satisfies *val*$(f^*) =$ *val*$(f) - 1$.

   Briefly explain (i) why your suggested algorithm is correct (ii) why it achieves the desired running time.
   [Hint: You may want to use the (s, t)-flow f as well as the residual graph for G_f with respect to f.]

4. (5+4 points)

   (a) Compute the solution to the recurrence relation

   $$a_n - 2a_{n-1} + a_{n-2} = 2^n \quad (n \geq 2) \quad \text{with} \quad a_0 = 25 \text{ and } a_1 = 16\,.$$

(b) Let b_n denote the number of ways that the set $\{1, 2, \ldots n\}, n \geq 1$, can be partitioned into two non-empty subsets. Find a recurrence relation for b_n. (You do not need to solve this recurrence relation.)

5. (9 points) Assume that Alice has published modulus $n = 77$, and exponent $e = 7$. Bob sends ciphertext $C = 8$ to Alice. You are eavesdropper Eve and you are interested in Bob's secret message M. Compute Bob's secret message M from ciphertext C. Write down all of the computational steps that you need to perform in order to obtain Bob's secret message M.

6. (3 points each) For each of the following five claims, decide if true or false or if you would rather not give an answer. A correct answer gives **3**, an incorrect answer **−3** and not giving an answer **0 points** (minimum total number of points for Question 6 is 0 points). **Instead of guessing, it may be better not giving an answer.**

(a) Consider a simple graph $G = (V, E)$ with edge weights $w_e \geq 0$, $e \in E$. If there is an edge e such that $w_e < w_{e'}$ for any edge $e' \in E$ with $e' \neq e$ (in other words, e has weight strictly less than any other edge in the graph), then e must be in every minimum spanning tree of G.

True . . . . ☒
False . . . . ☐
I prefer to not give an answer . . . . ☐

(b) Consider a capacitated network $G = (V, E, c)$, where V is the set of vertices, E is the set of directed edges, and $c : E \to \mathbb{Z}_{\geq}0$, are the edge capacities. Let f be some (s, t)-flow in G that is not a maximum flow, and let *val*(f) be its value. Then any (s, t)-cut (S, T) of G must have capacity *cap*$(S, T)) \geq$ *val*(f).

True . . . . ☒
False . . . . ☐
I prefer to not give an answer . . . . ☐

(c) Consider an undirected, simple graph $G = (V, E)$ with edge weights $w : E \to \mathbb{R}$, and a minimum spanning tree T on G. Then for every pair of vertices $u, v \in V$ the shortest (u, v)-path in G must be contained in (V, T).

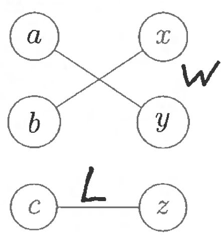
True . . . . ☐
False . . . . ☒
I prefer to not give an answer . . . . ☐

(d) Consider a complete bipartite graph $G = (V_n \cup V_m, E)$ with V_n and V_m being the two sides of the bipartition. Then G is Eulerian if and only if $|V_n| + |V_m|$ is even.

[Reminder: A complete bipartite graph *is a simple undirected graph whose vertices can be partitioned into two subsets V_n and V_m such that no edge has both endpoints in the same subset, and every possible edge that could connect vertices in different subsets is part of the graph.]*

True . . . . ☐
False . . . . ☒
I prefer to not give an answer . . . . ☐

(e) Consider the depicted matching M and corresponding preference lists. Then M is a stable matching.



$x >_a y >_a z$
$y >_b x >_b z$
$x >_c y >_c z$
$b >_x a >_x c$
$a >_y b >_y c$
$a >_z b >_z c$

[Reminder: $p >_i q$ indicates that i prefers to be matched with p over q.]

True . . . . ☒
False . . . . ☐
I prefer to not give an answer . . . . ☐