CSC3001 Discrete Mathematics

Final Examination

December 22, 2021: 7:30pm - 10:00pm

Name: ____________________ Student ID: ____________________

Answer ALL questions in the Answer Book.

Question	Points	Score
1	16	
2	16	
3	12	
4	18	
5	16	
6	22	
Total:	100	

1. (16 points) Let n and x be positive integers such that x has no positive divisors smaller than or equal to n except the divisor 1. Let p be a prime number.

   (a) (8 points) If $n = 4, x = 5, p = 3$, how many numbers in $\{x-1, x^2-1, \ldots, x^n-1\}$ are multiples of p?

   (b) (8 points) Show that at least $\lfloor n/p \rfloor$ numbers in $\{x-1, x^2-1, \ldots, x^n-1\}$ are multiples of p.

   ($\lfloor z \rfloor$ is the largest integer that is no larger than z, for $z \in \mathbb{R}$.)

Solution:

Part (a) There are 2 numbers (24 and 624) in $\{4, 24, 124, 624\}$ that are multiples of 3.

Part (b) If $n < p$ there is nothing to prove. Otherwise p and x are coprime. It follows that $x^{k(p-1)} \equiv 1 \pmod{p}$ by Fermat's little theorem. This implies that there are at least $\lfloor n/(p-1) \rfloor$ numbers in $\{x-1, x^2-1, \ldots, x^n-1\}$ that are multiples of p. Note that $n/(p-1) \geq n/p$, and thus the conclusion follows.

2. (16 points) Let $m \leq k < n$ be positive integers.

   (a) (8 points) Show that

$$\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}.$$

   (b) (8 points) Show that

$$\gcd\left(\binom{n}{m}, \binom{n}{k}\right) > 1.$$

Solution:

Part (a) The LHS gives the number of ways to choose a committee of k members and select a subcommittee of size m from the committee members.

The RHS gives the number of ways to choose the subcommittee first, then fill out the committee with $k - m$ other members for a total of k members on the committee.

Thus, LHS and RHS are counting the same number.

Part (b) We prove the claim by contradiction. Suppose that $\gcd\left(\binom{n}{m}, \binom{n}{k}\right) = 1$. By (a), $\dfrac{\binom{n}{k}\binom{k}{m}}{\binom{n}{m}} = \binom{n-m}{k-m}$. As $\gcd\left(\binom{n}{m}, \binom{n}{k}\right) = 1$ and $\binom{n-m}{k-m}$ is an integer, $\binom{k}{m}$ must be a multiple of $\binom{n}{m}$. However,

$\binom{n}{m} > \binom{k}{m}$, resulting in a contradiction. Thus, $\gcd\left(\binom{n}{m}, \binom{n}{k}\right) > 1$.

3. (12 points) Let d be a positive integer. T is a tree with at least 2 vertices and there is a vertex in T with degree at least d. Show that T has at least d leaves.
(A leave is a vertex with degree 1. The root of T is also a leave if its degree is 1.)

Solution:

We remove a vertex with degree at least d and the graph decomposes into at least d connected components. If a connected component is an isolated vertex then it was a leave in the tree. If a connected component is with at least 2 vertices, then it is a tree and it has at least 2 leaves and subsequently at least 1 out of the leaves was not connected to the removed vertex, which indicates that it was a leave in the tree. Thus there were at least d leaves in the tree.

4. (18 points) Let n be a positive even integer.
   (a) (6 points) How many functions $f\colon \{0,1\}^n \to \{0,1\}^n$ are there that satisfy $f(x) \neq x$ for all $x \in \{0,1\}^n$? Justify your answer.
   (b) (6 points) Given a bit string $x \in \{0,1\}^n$, let x^{rev} denote the string in $\{0,1\}^n$ obtained from x by reversing the ordering of the bits of x. (e.g., the first bit of x becomes the last bit of x^{rev}, etc.) How many strings $x \in \{0,1\}^n$ satisfy $x^{\text{rev}} = x$? Justify your answer.
   (c) (6 points) How many functions $f\colon \{0,1\}^n \to \{0,1\}^n$ are there that satisfy $f(x) \neq x$ and $f(x) \neq x^{\text{rev}}$ for all $x \in \{0,1\}^n$? Justify your answer.

Solution:

Part (a) $(2^n-1)^{(2^n)}$. There are 2^n elements in the domain $\{0,1\}^n$ of f and each of these elements can be mapped to any element in the codomain $\{0,1\}^n$ except for itself. Therefore, there are $2^n - 1$ choices for each of the 2^n elements in the domain.

Part (b) $2^{n/2}$. Since the first half of x^{rev} determines the entire string, to construct a string $x \in \{0,1\}^n$ such that $x = x^{\text{rev}}$, one only needs to specify the first $n/2$ bits of the string x. There are 2 choices (either 0 or 1) for each of these $n/2$ bits, resulting in $2^{n/2}$ strings in total.

Part (c) $(2^n-1)^{(2^{n/2})}(2^n-2)^{(2^n-2^{n/2})}$. There are $2^{n/2}$ choices of $x \in \{0,1\}^n$ such that $x = x^{\text{rev}}$. For each of these choices, it can be mapped to $2^n - 1$ elements in the codomain $\{0,1\}^n$ except itself. There are $2^n - 2^{n/2}$ choices of $x \in \{0,1\}^n$

such that $x \neq x^{\text{rev}}$. For each of these choices, it can be mapped to $2^n - 2$ elements in the codomain $\{0,1\}^n$ except itself and its reverse. In total, there are $(2^n - 1)^{2^{n/2}}(2^n - 2)^{2^n - 2^{n/2}}$ choices for f such that $f(x) \neq x$ and $f(x) \neq x^{\text{rev}}$.

5. (16 points) A multigraph is an undirected graph which is allowed to have multiple edges that have the same end vertices.
   (a) (6 points) Does there exist a multigraph without loops for the degree sequence $(3, 2, 1)$? Draw such a graph if it exists. If it does not exist, explain why.
   (b) (6 points) Does there exist a multigraph without loops for the degree sequence $(3, 3, 2, 1)$? Draw such a graph if it exists. If it does not exist, explain why.
   (c) (4 points) Let $0 \leq d_1 \leq d_2 \leq \cdots \leq d_n$ be integers. Show that $(d_n, d_{n-1}, \ldots, d_1)$ is a degree sequence of a multigraph without loops if $\sum_{i=1}^{n} d_i \equiv 0 \pmod 2$ and $d_n \leq \sum_{i=1}^{n-1} d_i$.

Solution:

Part (a) Yes. The drawing is omitted.

Part (b) No. By the handshaking lemma, the sum of the degrees must be even.

Part (c) If $d_n = 1$, then there are even number of vertices with degree 1 and a multigraph can be drawn immediately. We thereafter consider the case that $d_n > 1$. In this case, $\sum_{i=1}^{n} d_i$ is at least 4.

We prove the claim by induction on $\sum_{i=1}^{n} d_i$. The base case that $\sum_{i=1}^{n} d_i = 4$ is immediate. Assuming the induction hypothesis, we distinguish two cases.

If $d_{n-2} < d_n$, then $d_n - 1$ is the largest number in $d_1, d_2, \ldots, d_{n-2}, d_{n-1} - 1, d_n - 1$. Then,

$$d_1 + \ldots + d_{n-2} + (d_{n-1} - 1) + (d_n - 1) \equiv 0 \pmod 2\,,$$
$$d_1 + \ldots + d_{n-2} + (d_{n-1} - 1) \geq d_n - 1\,.$$

If $d_{n-2} = d_n$, then $d_{n-1} = d_n$ and d_{n-2} is the largest number in $d_1, d_2, \ldots, d_{n-2}, d_{n-1} - 1, d_n - 1$. Then, as $d_{n-2} = d_n \geq 2$,

$$d_1 + \ldots + d_{n-3} + d_{n-2} + (d_{n-1} - 1) + (d_n - 1) \equiv 0 \pmod 2\,,$$
$$d_1 + \ldots + d_{n-3} + (d_{n-1} - 1) + (d_n - 1) \geq d_{n-2}\,.$$

Thus, $d_1, \ldots, d_{n-2}, d_{n-1} - 1, d_n - 1$ satisfy the assumption of the problem and by induction there exists a multigraph without loops on n vertices realizing the degree sequence. Joining the vertices with degree $d_{n-1} - 1$ and $d_n - 1$ by a new edge, we obtain a multigraph with degree sequence $(d_n, \ldots, d_1)$.

6. (22 points) For $x, y \in \mathbb{Z}$, let predicate $P(x, y) = (|x| < |y|)$ or $(|x| = |y|$ and $x \leq y)$.
   (a) (6 points) Show that for $x \in \mathbb{Z}$, $P(x, x)$ is true.
   (b) (6 points) Show that for $x, y \in \mathbb{Z}$, $x = y$ if and only if $P(x, y) \wedge P(y, x)$.
   (c) (6 points) Show that for $x, y, z \in \mathbb{Z}$, $P(x, y) \wedge P(y, z)$ implies $P(x, z)$.
   (d) (4 points) Show that there exists a predicate $R(x, y)$ for $x, y \in \mathbb{Q}$ such that the following properties hold simultaneously:
      - For $x \in \mathbb{Q}$, $R(x, x)$ is true;
      - For $x, y \in \mathbb{Q}$, $x = y$ if and only if $R(x, y) \wedge R(y, x)$;
      - For $x, y, z \in \mathbb{Q}$, $R(x, y) \wedge R(y, z)$ implies $R(x, z)$;
      - For an arbitrary nonempty subset $B \subseteq \mathbb{Q}$ of rational numbers, there exists a unique element $x^* \in B$ such that for every $y \in B$ the predicate $R(x^*, y)$ is true.

Solution:

Part (a) $P(x, x) = \text{false} \ \vee \ (\text{true} \ \wedge \ \text{true}) = \text{true}$.

Part (b) If $x = y$ then $P(x, y) \wedge P(y, x) = \text{true} \wedge \text{true} = \text{true}$. If $P(x, y) \wedge P(y, x)$ is true, then $|x| \leq |y|$ by $P(x, y)$ and $|y| \leq |x|$ by $P(y, x)$. Then $|x| = |y|$. With this equality, $P(x, y)$ and $P(y, x)$ indicate $x \leq y$ and $y \leq x$ respectively. Subsequently, $x = y$. Thus, $x = y$ if and only if $P(x, y) \wedge P(y, x)$.

Part (c) $P(x, y)$ and $P(y, z)$ indicate that $|x| \leq |y|$ and $|y| \leq |z|$ respectively. If $|x| < |y|$ or $|y| < |z|$ then $|x| < |z|$, which implies $P(x, z)$. If none of $|x| < |y|$ and $|y| < |z|$ hold, then by $P(x, y) \wedge P(y, z)$ we have $|x| = |y|$ and $x \leq y$ and $|y| = |z|$ and $y \leq z$, which indicate that $|x| = |z|$ and $x \leq z$. $P(x, z)$ follows.

Part (d) We first show that for an arbitrary nonempty subset $B \subseteq \mathbb{Z}$ of integers, there exists a unique element $x^* \in B$ such that for every $y \in B$ the predicate $P(x^*, y)$ is true. We choose x^* as an element with the smallest absolute value, whose existence is guaranteed by the well-ordering principle. If there is a tie, it will tie for at most 2 numbers (x^*, $-x^*$), and we choose the negative one to ensure that $P(x^*, -x^*)$ is true. We verify that $P(x^*, y)$ is true for this x^* and $y \in B$. The uniqueness of x^* is guaranteed by (b).

As all 4 properties hold for P for domain $\mathbb{Z}$, it amounts to showing the existence of a bijection $f \colon \mathbb{Q} \to \mathbb{Z}$, with which $R(x, y) = P(f(x), f(y))$ will be the desired predicate for $x, y \in \mathbb{Q}$. Such a bijection can be explicitly constructed. Define $f(0) = 0$, $f(1) = 1$, $f(x) = -f(-x)$ when $x < 0$. When $x > 0$ and $x \neq 1$, we write x uniquely into $p_1^{n_1} \cdot \cdots \cdot p_k^{n_k}$ for primes $p_1, \ldots, p_k$. Then let $f(x) = p_1^{m_1} \cdot \cdots \cdot p_k^{m_k}$, where $m_i = 2n_i$ when $n_i \geq 0$ and $m_i = -2n_i - 1$ when $n_i < 0$. We verify that when $x \neq y$, $f(x) \neq f(y)$ and for every $z \in \mathbb{Z}$ by factorizing z one could obtain $f^{-1}(z)$. Thus, f is a bijection, as desired.

Remark:

The first three properties are known as reflexivity, antisymmetry, and transitivity, which guarantee that R is a partial order. The fourth property shows that there exists a *least* element under this partial order in every subset of $\mathbb{Q}$. As such, it concludes that $\mathbb{Q}$ is well-ordered.