Discrete Structures
Tutorial Solutions

Ashwin Abraham
Rishabh RP

September 24th, 2023

Contents

Chapter 1

Predicate Logic

Question 1

Assume the predicate $prime(n)$ is defined over positive integers, which is true if and only if n is a prime number. Express the following statements in predicate logic:

1. There exist infinitely many prime numbers.
2. There exists arbitrarily long sequences of consecutive numbers such that none of them are prime.
3. A number n is prime if and only if $(n-1)! + 1$ is divisible by n (Wilson's Theorem).
4. For all positive integers n, there exists a prime number p such that $n \leq p \leq 2n$.

Solution:

Author: Ashwin Abraham
A predicate is true for infinitely many natural numbers if and only if the set of numbers for which the predicate is true has no upper bound. This is as any subset of the natural numbers that has k as an upper bound can have at most k elements, and therefore cannot be infinite. Taking the subset of natural numbers as the numbers for which the predicate is true, the result follows. Using this, we can express statements including terms such as "infinitely many" and "arbitrary long" using first order predicate logic. While expressing the statements, we assume that arithmetic relations and operators over the natural numbers such as $+$, $\cdot$, $<$, etc have already been defined. The domain of all variables is assumed to be the set of natural numbers.

1. $\forall n \exists m(m > n \wedge prime(m))$
2. $\forall n \exists m \exists a \forall x(x \geq a \wedge x < a + m \implies \neg prime(x))$
3. $\forall n(prime(n) \iff \exists k((n-1)! + 1 = kn))$
4. $\forall n(n > 0 \implies \exists p(prime(p) \wedge n \leq p \wedge p \leq 2n))$

Question 2

These are some famous problems involving primes, some of which are still unsolved. Express them using predicate logic. Do NOT attempt to prove them or read the proofs, where available.

1. There exist infinitely many prime numbers p such that $p + 2$ is also a prime. This is also called the twin primes conjecture.
2. Every even number > 2 can be written as a sum of two (not necessarily distinct) prime numbers. This is called the Goldbach conjecture.
3. There exist arbitrarily long arithmetic progressions of prime numbers. This was proved in the early 2000's by Ben Green and Terrence Tao.
4. There exists a constant c such that there are infinitely many pairs of distinct prime numbers that differ by at most c. This was proved by Yitan Zhang in 2013 for c around 70 million. The value has now been reduced considerably. More generally, for every $k \geq 2$, there exists a constant c such that there are infinitely many k-tuples of distinct prime numbers such that any two differ by at most c.

Solution

Author: Ashwin Abraham
Again, the domain of all the variables is assumed to be $\mathbb{N}$.

1. $\forall n \exists p(p > n \wedge prime(p) \wedge prime(p + 2))$
2. $\forall n(n > 2 \wedge \exists k(n = 2k) \implies \exists p \exists q(prime(p) \wedge prime(q) \wedge n = p + q))$
3. $\forall n \exists a \exists d(d > 0 \wedge \forall i(i \geq 0 \wedge i < n \implies prime(a + id)))$
4. $\exists c \forall n \exists p \exists q(p > q \wedge p > n \wedge prime(p) \wedge prime(q) \wedge p \leq q + c)$

Question 3

This was observed by someone after the last class, and generalizes some properties that were used. Let P be a predicate over some domain. Consider the following two statements.

1. For all predicates Q, the statement "for all x $P(x)$ implies $Q(x)$" is equivalent to the statement "there exists x $P(x)$ and $Q(x)$".

2. "There exists a unique x $P(x)$".

Are the two statements equivalent to each other? If so, prove it, otherwise, give an example of a predicate P for which one is true but not the other.

Solution

Author: Ashwin Abraham

NB: The person who observed this is in fact the author :)

If (2) is true, ie there exists a unique x (call it x_0) such that $P(x)$ is true, then we will show that (1) is true. For any predicate Q, if there exists x such that $P(x) \wedge Q(x)$ is true, that x must be x_0, and $Q(x_0)$ must be true as well. Now, for $x = x_0$, since $P(x)$ and $Q(x)$ are both true, we have $P(x) \implies Q(x)$, and for $x \neq x_0$, $P(x)$ is false, and we therefore have $P(x) \implies Q(x)$ irrespective of $Q(x)$. Therefore, $P(x) \implies Q(x)$ is true for all x. On the other hand, if there doesn't exist an x such that $P(x) \wedge Q(x)$ holds, then $Q(x_0)$ must be false. In this case, for $x = x_0$, $P(x)$ is true but $Q(x)$ is false, and hence $P(x) \implies Q(x)$ is false, which means $P(x) \implies Q(x)$ does not hold for all x (in fact it fails to hold only at $x = x_0$, as $P(x)$ is false for other x). As you can see, in both cases "for all x $P(x)$ implies $Q(x)$" is equivalent to the statement "there exists x $P(x)$ and $Q(x)$" and therefore (1) is true.

If (2) is false, then either there are no x such that $P(x)$ is true, or there are distinct x_1 and x_2 such that $P(x_1)$ and $P(x_2)$ are both true true. If there are no x such that $P(x)$ is true, then for any predicate Q, "there exists x $P(x)$ and $Q(x)$" is clearly false, while "for all x $P(x) \implies Q(x)$" is true, as $P(x)$ is always false. Therefore those two statements are not equivalent, ie (1) is false. If there are distinct x_1 and x_2 such that P holds for both of them, then let us choose Q as the predicate $x = x_1$. For this predicate, there does exists an x such that $P(x) \wedge Q(x)$ hold (x_1) but at $x = x_2$, $P(x)$ is true whereas $Q(x)$ is false (since $x_1 \neq x_2$). Therefore, the two statements are not equivalent for all predicates Q.

We therefore have that (1) is true precisely when (2) is true, and therefore they are equivalent. Notice how the universal quantification on Q was critical to prove the theorem.

If we were to express this theorem in predicate logic, it would be:

$$\forall P([\forall Q(\forall x(P(x) \implies Q(x)) \iff \exists x(P(x) \wedge Q(x)))] \iff \exists^u x P(x))$$

where $\exists^u x P(x)$ represents that there exists a unique x such that $P(x)$ holds. In normal predicate logic, this would be written as $\exists x\,[P(x) \wedge \forall y(P(y) \implies y = x)]$. Note that this is a sentence in second order logic, as we quantify over predicates.

Question 4

Consider a game played between two players on an $n \times m$ matrix with 0,1 entries. Initially the matrix is all 0's. The two players take turns and play alternately. In each move, a player must select a 0 entry in some position (i, j) and convert all entries in positions (x, y) for $x \geq i$ and $y \geq j$ to 1, if they are not already 1. At each move at least one 0 gets converted to a 1. The player who selects the 0 in the position $(1, 1)$, after which the matrix has only 1 entries, loses the game. Prove that for all (n, m) except $(1, 1)$ the first player can win the game. It is possible to prove this without actually finding what the winning move is. Can you find this move for general n, m?

Solution

Author: Ashwin Abraham

This game is known as the game of Chomp. It is usually framed in terms of an $n \times m$ bar of chocolate where the piece at $(1, 1)$ is poisoned. The players have to eat parts of the chocolate in the way mentioned in the question - by choosing some piece at (i, j) and eating all the pieces (x, y) where $x \geq i$ and $y \geq j$. The person who eats the poisoned piece loses (clearly!).

First of all, observe that this game is guaranteed to terminate in at most mn moves, as in each move at least one 0 is converted to a 1. Also, one of the players is guaranteed to lose - the one who selects $(0, 0)$ in the end, when no other position is available. The other is then guaranteed to win. Let us establish some results for two player alternating games that are guaranteed to terminate in a win for one of the players.

We construct something known as the Game Tree, where the nodes correspond to possible histories of the game, where the history of the game is the sequence of states the game has been in, from the starting state to the current state. We connect one history to another if it is possible to go from the first history to the second by making a valid move. Note that the first history will then be a prefix of the second history. It is clear that this structure indeed corresponds to a tree, as cycles are not possible

(the length of the history increases by one each move) and each node - other than the root (which corresponds to the starting state) - has a unique parent (its prefix). Now, this tree is finite, as the game is guaranteed to terminate. The leaf nodes of the tree therefore correspond to its terminal states.

We know that at the terminal states, either player A has won or player B has won. Let us label[1] the leaf nodes corresponding to the wins of player A as A and those corresponding to the wins of player B as B. Note that every leaf node is labelled as exactly one of A and B. We extend this labelling to all the nodes of the tree, where nodes, from which A has a strategy with which he is guaranteed to win, no matter what B plays (this is called a winning strategy - note that the strategy itself may depend on what B plays) are labelled as A, and those where B has a winning strategy are labelled as B. Note that a node cannot be labelled with both A and B, as both A and B cannot have winning strategies at the same node. Claim: Every node in the tree will end up labelled by either A or B, ie at every node either A or B have winning strategies.

We prove this by strong induction on the depth of the game tree (the maximum distance from root to a leaf node). As we induct, we consider gameplay starting not just from the original starting state, but from any arbitrary (reachable) state. If the depth of the game tree is 1, then this game tree corresponds to a starting state that is already terminal, ie where no move can be made. We already know that terminal states can be labelled with A or B, as in the terminal states, one of the players must have one (for our game this is the player whose turn it is currently and who has no move to make). Assume that for all game trees of depth at most d, every node can be labelled as either A or B. A game tree of depth $d+1$ is made up of a root connected to multiple subtrees, each of height at most d. Each subtree corresponds to a subgame starting at a different state. Since the previous state of the game does not affect further gameplay, we can apply the inductive hypothesis on the subtrees, ie all their nodes are labelled as either A or B, including their root nodes. This means that all the children of the root node are labelled as either A or B. Now, if all the children are labelled as B, this means that whatever move A makes, he will end up in a state from which B can win. This means that the root should be labelled as B, as B has a winning strategy for any move that A makes. However, if one of the children of the root is labelled as A, then A can make the move that moves the state of the game to that node, from which A has a winning strategy. Therefore in this case A will have a winning strategy. In either case, the root node ends up labelled as either A or B, completing our inductive proof. The player with whom the root is labelled therefore has a winning strategy no matter what the other player plays[2].

[1] An alternative way to label the nodes would be as 1 if the player whose turn it is has a winning strategy, and 0 if the other player has a winning strategy.

[2] This analysis was originally done by Von Neumann on the game of chess, where he proved that

For the game corresponding to non-leaf node u, if the first player (say p) has a winning strategy, this means that there exists a child node of u winning for p. Since it isn't p's turn at the child node, this means that either the child node is a terminal state or every child node of this child is winning for p. Formally writing down the condition (ignoring the case where the child is terminal), we get $\exists v \in children(u) \forall w \in children(v) [win(w) = p]$. Such a game is called a $\exists\forall$ game. If the second player has a winning strategy, we get the condition $\forall v \in children(u) \forall w \in children(v) [win(w) \neq p]$. These are $\forall\exists$ games. This $\forall\exists$ alternation is characteristic of two player terminating games.

Since Chomp is a alternating two player game that always terminates in a win for one of the players, the result we've just proven implies that one of the players (either A the one who moves first or B who moves second) has a winning strategy no matter what the other player plays. If $m = n = 1$, then clearly the first player always loses and the second player always wins. Henceforth, we will assume that m and n are not both 1. We then have to show that the first player A, has a winning strategy (ie we have to show that Chomp is a $\exists\forall$ game).

We will prove this by contradiction. Assume Chomp is a $\forall\exists$ game. Now, the root r is not a terminal state and the only child of the root that is terminal is the one that corresponds to choosing $(1, 1)$ - call this t. We therefore have $\forall u \in children(r) [win(u) = B]$, and to be more specific, $\forall u \in children(r) - \{t\} \exists v \in children(u) [win(u) = B]$. Let us consider the move where the first player chooses (m, n). Since m and n are not both 1, this results in a transition to some $u \neq t$ that is not terminal. Now this node should have a child v that has $win(v) = B$. Now, v is a node in which it is A's turn to move but has $win(v) = B$. Notice that if the current state at node v is S, then A could have made a move directly taking the game to state S! The move A would make would be the same as the move that B just made. Formally speaking there is some node $w \in children(u)$ such that w and v have the same current state. At node v, it was A's turn, and we had $win(v) = B$. Since node w has the same current state as v, but instead it is B's turn, we have $win(w) = A$ (this is as the gameplay depends only on current state and not the entire history). This leads to a contradiction, as we had obtained $\forall u \in children(r) [win(u) = B]$. Therefore, the first player must have a winning strategy in Chomp, for m and n not both 1 (ie it is a $\exists\forall$ game). Arguments like the one we made are known as strategy stealing arguments.

For $m = 1$ or $n = 1$ it is easy to see the winning move is to choose the position adjacent to $(1, 1)$. For $m = n > 1$, the winning strategy is to first choose $(2, 2)$ and thereafter if the other player plays (p, q), play (q, p). The winning move for general m, n has not yet been found by us.

---

either one of the players can force a win or both players can force a draw.

Chapter 2

Induction and the Peano Axioms

Question 1

Define the addition and multiplication operation of numbers using the basic assumptions. Prove the basic properties of the addition and multiplication operations on numbers, such as commutativity, associativity and distributivity. Write your proof as a sequence of statements, and write down the rule used to derive the statement from the preceding statements. Henceforth, we will be assuming these properties of arithmetic operations.

Solution

Author: Ashwin Abraham
We define addition as the unique function $+ : \mathbb{N}^2 \to \mathbb{N}$ such that (we use infix notation from here on, ie $+(a, b)$ is written as $a + b$):

1. $\forall a \in \mathbb{N}, a + 0 = a$
2. $\forall a, b \in \mathbb{N}, a + next(b) = next(a + b)$

If such a function exists, it must be unique. Say two functions $+$ and $+'$ exist that satisfy these axioms. We show that $\forall a, b \in \mathbb{N} a + b = a +' b$ by induction on b. For $b = 0$, we have $\forall a \in \mathbb{N}, a + b = a + 0 = a = a +' 0 = a + b$. Now, assume that for some b, we have $a + b = a +' b$ for all naturals a. Now, $a + next(b) = next(a + b)$ and $a +' next(b) = next(a +' b)$, for any natural a. Since we have $a + b = a +' b$, we get $next(a + b) = next(a +' b)$, ie $a + next(b) = a +' next(b)$ for all naturals a. Therefore, by induction, we have $\forall a, b \in \mathbb{N}, a + b = a +' b$, ie $+$ is unique.

Question 2

Define the usual $<$ relation on natural numbers using induction. Note that this is just a predicate $<(m, n)$ which is true if $m < n$ in the usual sense. Instead of the induction principle, numbers can also be defined using the $<$ relation and the *next* function. The induction principle is replaced by the statement "for any predicate P, if there exists an n such that $P(n)$ is true, then there exists an n such that $P(n)$ is true and for all $m < n$, $P(m)$ is false". In other words, this says that if $P(n)$ is true for some n, then there is a smallest n for which it is true. This is known as the well ordering principle. What properties of the $<$ relation and *next* are needed so that this defines exactly the properties of natural numbers.

Solution

Question 3

The principle of strong induction states that for any predicate P, if for all n, assuming $P(m)$ is true for all $m < n$ implies $P(n)$, then $P(n)$ is true for all n. Express this using propositional logic and show that this is equivalent to the usual principle of induction. Use this to show that every number can be written as a product of prime numbers.

Question 4

Prove that for every natural number $m > 0$, for every number n, there exist unique natural numbers q and r such that $n = qm + r$ and $0 \leq r < m$. This is called the division property of numbers (ie Euclid's Lemma) and is the starting point for many basic results in number theory.

Question 5

Prove that for all positive integers k, the product of any k consecutive numbers is divisible by $k!$. There is a simple one line "combinatorial" proof of this using a counting argument, but try to prove it using only the basic properties of numbers.

Question 6

The axioms of numbers defines the "unary" representation of a number n, where n is considered to be obtained by adding 1 to 0 n times. An equivalent set of axioms can be defined using the "binary" representation. Instead of the *next* function, we assume two functions on numbers, $double(n)$ and then $double(n) + 1$. Write down the axioms needed using these two functions, to define the natural numbers. Show that these are equivalent to the Peano axioms. Define the addition and multiplication operations using these axioms.

Question 7

Let a, b be natural numbers. Consider the following statement. For all predicates $P(n)$, ($P(a)$ and $P(b)$ and for all n, m (($P(n)$ and $P(m)$) implies $P(n + m)$) implies ($P(n)$ is true for sufficiently large n)). Write down a simple statement equivalent to this, without using quantification over predicates, and prove that your statement is equivalent to this.

Chapter 3

Divisibility and GCD

Question 1

Let a, b be positive numbers and let X be the set of all positive numbers r such that $xa = yb + r$ for some natural numbers x, y. Prove that the set X is exactly the set of all multiples of $\gcd(a, b)$. First show that the smallest element must be $\gcd(a, b)$ and any other element must be a multiple of it.

Question 2

Let a, b be positive numbers such that $a \neq 0 \mod b$. Let $g > 0$ be the smallest number such that $xa = g \mod b$ for some number x. Prove that $g = \gcd(a, b)$. This implies that a has a multiplicative inverse mod b if and only if $\gcd(a, b) = 1$.

Question 3

Consider the following definition of a function $f(n, m)$. Define $f(0, n) = n$ for all n, $f(n, m) = f(m, n)$ for all m, n and $f(n, m) = f(n \mod m, m)$. Prove using strong induction that this defines f uniquely and that for all n, m, $f(n, m) = \gcd(n, m)$. This gives an algorithm to compute $\gcd(n, m)$ known as Euclid's Algorithm. If n and m are numbers with k bits in their binary representations, find an upper bound on the number of arithmetic operations required to compute their gcd. Modify the algorithm to find x, y such that $xn = ym + \gcd(n, m)$.

Question 4

Another algorithm for finding the gcd is given by a different definition. Again define $f(0,n) = f(n,0) = n$ for all n, and for any n, m the following hold: $f(2n,2m) = 2f(n,m)$, $f(2n,2m+1) = f(n,2m+1)$, $f(2n+1,2m) = f(2n+1,m)$, and $f(2n+1,2m+1) = f(2m+1,n-m)$ if $m \leq n$ and $f(2n+1,m-n)$ otherwise. Prove that this function is uniquely defined and gives exactly $\gcd(n,m)$ for all n, m. This needs the fact that any $n > 0$ is either $2m$ or $2m+1$ for some $m < n$. This algorithm has the advantage that it uses only subtraction and division by two, and is easier to implement in hardware.

Question 5

Prove that if $2^n - 1$ is prime then n must be prime. Give an example to show that converse is not true. Prove that $\gcd(2^m-1, 2^n-1) = 2^{\gcd(m,n)}-1$. More generally, show that if $\gcd(a,b) = 1$ and $0 \leq m < n$, then $\gcd(a^m - b^m, a^n - b^n) = a^{\gcd(m,n)} - b^{\gcd(m,n)}$. Hint: Use Euclid's algorithm.

Question 6

Let $n > m > 0$ be positive integers. Prove that if $\gcd(n,m) = 1$, then the binomial coefficient $\binom{n}{m}$ is divisible by n. Is the converse of this statement true? (Hint: There is a simple combinatorial proof for this.) Use this to prove Fermat's Little Theorem that for any prime p and for all x, $x^p - x$ is divisible by p. Prove that $2^n - 1$ is not divisible by n for any $n > 1$.

Question 7

Let m, n be positive integers such that m divides n. Show that there exist numbers a, b such that $a \leq b$, $\gcd(a,b) = m$ and $lcm(a,b) = n$. Find a necessary and sufficient condition on m and n such that there exists a unique such pair of numbers. Prove that in general the number of solutions is a power of 2.

Question 8

Consider two fractions $\frac{m}{n}$ and $\frac{m'}{n'}$ in lowest terms. In other words, $\gcd(m,n) = \gcd(m',n') = 1$. Prove that when the sum $\frac{m}{n} + \frac{m'}{n'}$ is reduced to lowest terms, the denominator will be nn' if and only if $\gcd(n,n') = 1$.

Question 9

Let a and b be positive irrational numbers such that $\frac{1}{a} + \frac{1}{b} = 1$. Prove that for every positive integer n there exists a positive integer k such that $n = \lfloor ka \rfloor$ or $n = \lfloor kb \rfloor$.

Question 10

Consider an $m \times n$ matrix A with integer entries. Let L be the set of all m-dimensional vectors v such that $v = Ax$ for some n-dimensional vector x with integer entries. The set L is called a lattice. Prove that for any such matrix A there exists an $m \times m$ matrix B such that L is exactly the set of vectors By, where y is any integral m-dimensional vector. Note that when A is the 1×2 dimensional matrix $\begin{bmatrix} a & b \end{bmatrix}$, then B is the 1×1 dimensional matrix $\begin{bmatrix} \gcd(a, b) \end{bmatrix}$. B is called a basis for L. A challenging problem is to find a basis with "smallest" possible entries and a vector in L with smallest possible magnitude. This is equivalent to finding gcd when $m = 1$ but is much more difficult for arbitrary m. Try to do it for $m = 2$. The dimension of L is the smallest k such that every vector in L can be written as an integral linear combination of k m-dimensional vectors. The dimension of L is at most m but may be less than m. Given the matrix A, can you give an efficient algorithm to find the dimension of L.

Chapter 4

Modular Arithmetic

Question 1

Let m, n be positive integers such that $\gcd(m, n) = 1$. Prove that for all $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$ there exists a unique number x in $\mathbb{Z}_{mn}$ such that $x = a \mod m$ and $x = b \mod n$. This is known as the Chinese Remainder Theorem. Suppose now that $\gcd(m, n) = d$ for some number d. Find a necessary and sufficient condition on a and b for such a number x to exist. If it exists, how many distinct such numbers exist in $\mathbb{Z}_{mn}$? Can you find an explicit description of all possible solutions?

Question 2

A number a such that $1 \leq a < n$ is called a quadratic residue modulo n iff the congruence $x^2 = a \mod n$ has a solution. If n is a prime number, how many quadratic residues are there modulo n? If $n = pq$ is a product of two distinct odd prime numbers, how many quadratic residues are there modulo n?

Question 3

Let n be a prime number and $P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{d-1} x^{d-1} + x^d$ be a monic polynomial of degree d with coefficients $a_i \in \mathbb{Z}_n$ for $0 \leq i < d$. An element $a \in \mathbb{Z}_n$ is called a root of the polynomial iff $P(a) = 0 \mod n$. Prove that a polynomial of degree $d \geq 1$ has at most d roots in $\mathbb{Z}_n$. For all primes n, prove that there exists a polynomial of degree 2 that has no roots in $\mathbb{Z}_n$. Such a polynomial is called irreducible modulo n. Try to explicitly construct such a polynomial for a general prime n. Try to generalize this to polynomials of degree d for $d \geq 2$.

Question 4

Let n be a prime number and a a number not divisible by n. The order of a modulo n is the smallest positive number k such that $a^k = 1 \mod n$. Prove that the order of a divides $n-1$. The number a is said to be a primitive root modulo n iff it's order is $n-1$. Prove that for all primes p, there exists a primitive root modulo n. Find all primitive roots modulo n for $n = 3, 5, 11, 13$. Prove that n is prime if and only if there exists a number $a \in \mathbb{Z}_n$ such that $a^{n-1} = 1 \mod n$ and $a^{\frac{n-1}{p}} \neq 1 \mod n$ for any prime p that divides $n-1$. Hint: Try to find for each divisor d of $n-1$ the number of elements in $\mathbb{Z}_n$ of order d. This may need some results from the previous problem.

Question 5

While Wilson's Theorem gives a necessary and sufficient condition for a number to be prime, Fermat's Little Theorem only gives a necessary condition which is not sufficient. There exist composite numbers n such that for all a, $\gcd(a, n) = 1$ implies $a^{n-1} = 1 \mod n$. Such numbers are called Carmichael numbers. Prove that a number n is a Carmichael number if and only if n is a product of distinct primes and for every prime p that divides n, $p-1$ divides $n-1$. The smallest Carmichael number is $561 = 3 \times 11 \times 17$, and it is known that there are infinitely many of them. Find small values of a for which 561 is declared to be composite by the Miller-Rabin test.

Chapter 5

Euler Totient Function

Question 1

Prove that $\sum_{d|n} \phi(d) = n$ for all positive integers n. Give a combinatorial proof of this by showing that there is a one-to-one and onto function from $\{1, 2, \ldots, n\}$ to the set of ordered pairs (d, e) where d is a divisor of n and $1 \leq e \leq d$ with $\gcd(e, d) = 1$.

Question 2

Use the previous result to prove that if p is a prime number, then for every divisor d of $p - 1$, $\mathbb{Z}_p^*$ contains exactly $\phi(d)$ elements of order d. Prove that $\mathbb{Z}_n^*$ has an element of order $\phi(n)$ (a generator) iff n is one of $2, 4, p^k$ or $2p^k$ for some odd prime p and integer $k \geq 1$.

Question 3

Prove that if m divides n, then $\phi(m)$ divides $\phi(n)$. Give a combinatorial proof of this by showing that $\mathbb{Z}_n^*$ can be partitioned into $\phi(m)$ parts of equal size or into some number of parts of size $\phi(m)$.

Question 4

The Mobius function $\mu(n)$ is defined as $\mu(1) = 1$, $\mu(n) = 0$ if n is divisible by p^2 for some prime p and $\mu(n) = (-1)^k$ if $n = p_1 p_2 \ldots p_k$ is a product of k distinct primes. Suppose $f(n)$ and $g(n)$ are functions such that for all $n \geq 1$, $g(n) = \sum_{d|n} f(d)$. Prove

that $f(n) = \sum_{d|n} g(d)\mu(\frac{n}{d})$. This is called Mobius inversion and is a special case of a more general result. Use this and the earlier proven result that $\sum_{d|n} \phi(d) = n$ to derive the expression for $\phi(n)$.

Question 5

Prove that $\sum_{k=1}^{n} \phi(k)\lfloor \frac{n}{k} \rfloor = \frac{n(n+1)}{2}$. Hint: Consider all possible rational numbers in $(0, 1)$ with denominator at most n, and consider their reduced forms.

Chapter 6

Boolean Algebra

Question 1

Prove that in any Boolean algebra B, $(xy)^c = x^c + y^c$ and $(x + y)^c = x^c y^c$, for all $x, y \in B$. These are called De Morgan's Laws. Also prove that $x + x^c y = x + y$.

Question 2

A Boolean expression with n variables $\{x_1, x_2, \cdots, x_n\}$ over a Boolean algebra B is defined recursively as follows. A single variable x_i is a Boolean expression. If e_1, e_2 are Boolean expressions then $e_1 + e_2$, $e_1 e_2$ and e_1^c are also Boolean expressions. Given an assignment of values $b_i \in B$ to each variable x_i, the value of an expression is defined recursively as $v(x_i) = b_i$, $v(e_1 + e_2) = v(e_1) + v(e_2)$, $v(e_1 e_2) = v(e_1)v(e_2)$ and $v(e_1^c) = v(e_1)^c$. A Boolean expression e with n variables therefore defines a function $f : B^n \to B$ as $f(b_1, b_2, \cdots, b_n) = v(e)$ for the assignment of values $v(x_i) = b_i$. Prove that every function $f : B^n \to B$ can be represented by a Boolean expression if B is a Boolean algebra with 2 elements. Is this true for any finite Boolean algebra? If so, prove it, otherwise give an example for which it is not possible. Say we modify the definition of an expression by allowing any constant $a \in B$ to be also considered an expression. These expressions are known as polynomial expressions. Show that for 2 element Boolean algebras, the set of polynomial expressions is the same as the set of Boolean expressions. For finite Boolean algebras B, can the set of polynomial expressions represent every function from B^n to B? If so, prove it, if not, find a counterexample. How will you modify the definition of an expression, so that all functions over any finite Boolean algebra can be represented? For 2 element Boolean algebras, the representation of a function as a Boolean expression is not unique, and a challenging problem is to find the "smallest" possible expression representing a given

function. We can define arithmetic expressions using $+$ and $\times$ over $\mathbb{N}$ in a similar way. Can the set arithmetic expression with n-variables represent every function from $\mathbb{N}^n$ to $\mathbb{N}$? What about the set of polynomial arithmetic expressions?

Question 3

Suppose e_1 and e_2 are two Boolean expressions with n variables over the Boolean algebra with two elements $\{0,1\}$ that represent the same function $\{0,1\}^n \to \{0,1\}$. Prove that they represent the same function over any Boolean algebra. Show that the statement for all $x_1, x_2, \cdots, x_n (e_1 = e_2)$ can be formally proven using just the axioms of Boolean algebras. De Morgan's Laws are examples of this. Can you think of a systematic way of finding such proofs that use only the axioms?

Question 4

We have seen that for any set S, its power set 2^S is a Boolean algebra with $X + Y = X \cup Y$, $XY = X \cap Y$ and $X^c = S - X$, for any $X, Y \subseteq S$. 0 here corresponds to $\emptyset$ and 1 to S. Now, show that for any finite Boolean algebra B there is an isomorphism from B to the power set of some finite set S. An isomorphism here refers to a bijection $f : B \to 2^S$ that satisfies $f(x + y) = f(x) \cup f(y)$, $f(xy) = f(x) \cap f(y)$ and $f(x^c) = S - f(x)$, for all $x, y \in B$. For a finite Boolean algebra B, suppose we drop the axiom of existence of a complement but instead add the axioms $a + 1 = 1$ and $a \cdot 0 = 0$ for all $a \in B$. As we have seen, the set of divisors of a number n, with $+$ as lcm and $\cdot$ as gcd is an example of such a structure, with 0 corresponding to 1 and 1 corresponding to n. This is equivalent to the set of multisubsets of a finite multiset, which is another example of a set satisfying these axioms with $+$ as $\cup$ and $\cdot$ as $\cap$. Show that any finite Boolean algebra with the modified axioms is isomorphic to the set of multisubsets of a multiset, with $+$ as $\cup$ and $\cdot$ as $\cap$. Hint: Try to find the "atoms" and a "multiplicity" for each "atom". Suppose we also drop the assumptions $a + 1 = 1$ and $a \cdot 0 = 0$ along with the axiom of complement and also drop the axioms of distributivity, and add the axioms $a(a + b) = a$ and $a + ab = a$ for all a, b in the Boolean algebra. There are many other mathematical objects that satisfy these weaker properties, with appropriate definitions of $+$ and $\cdot$ operations. Such structures are called lattices. Some examples are partitions of a finite set, subspaces of a vector space, rectangles with horizontal and vertical sides in the plane and many others. Try to appropriately define the $+$ and $\cdot$ operations for these lattices so that they satisfy the axioms.

Chapter 7

Sets, Relations and Functions

Question 1

For a relation $R \subseteq A \times B$, we define $R^{-1} = \{(b, a) | (a, b) \in R\}$ (called the converse of R). For any two relations $R_1 \subseteq A \times B$ and $R_2 \subseteq B \times C$, we define $R_1 \cdot R_2 = \{(a, c) | \exists b \in B : (a, b) \in R_1 \wedge (b, c) \in R_2\}$. The operation $\cdot$ is known as composition. Prove that $\cdot$ is an associative operation, ie $(R_1 R_2)R_3 = R_1(R_2 R_3)$ for all relations R_1, R_2 and R_3. A relation from a set A to itself is known as a relation on A. Prove that if R_1 and R_2 are functions/injections/surjections/bijections on A, $R_1 R_2$ satisfies the same property. Do the converses of these properties hold? A left identity is a relation A that satisfies $AR = R$ for all relations R, and a right identity is a relation B that satisfies $RB = R$ for all relations R. Prove that the identity relation $I = \{(a, a) | a \in A\}$ is both left indentity and a right identity for the composition operator. R' is said to be a left inverse of R iff $R'R = I$ and a right inverse of R iff $RR' = I$. Do right inverses and left inverses exist for every relations R on A? Is R^{-1} always a right inverse or left inverse for R? Show that for any relation R on A, R has both a left inverse and a right inverse if and only if R is a bijection, and in this case the left inverse and right inverse are both unique and equal to R^{-1}. For relations R_1, R_2, R_3 on a set A, do the following statements hold? Give proofs or counterexamples as appropriate.

1. $(R_1 R_2)^{-1} = R_2^{-1} R_1^{-1}$
2. $(R_1 \cup R_2)R_3 = R_1 R_3 \cup R_2 R_3$
3. $R_3(R_1 \cup R_2) = R_3 R_1 \cup R_3 R_2$
4. $(R_1 \cap R_2)R_3 = R_1 R_3 \cap R_2 R_3$
5. $R_3(R_1 \cap R_2) = R_3 R_1 \cap R_3 R_2$

6. R_1R_2 is a function if and only if R_1 and R_2 are functions

7. $R_1 \subseteq R_2$ implies that $R_1R_3 \subseteq R_2R_3$ and $R_3R_1 \subseteq R_3R_2$

Question 2

Suppose R is a relation from A to B such that R contains an injection f from A to B and R^{-1} contains an injection g from B to A. Prove that R contains a bijection from A to B. This is a stronger form of the Schröder-Bernstein Theorem, which is a particular case when $R = A \times B$. Note that your argument should hold for any sets A and B, not only finite sets. What properties of sets are used in the proof? Using this, show there exists a bijection from the real numbers to the power set of natural numbers.

Question 3

This is another (non-constructive) proof of Hall's Theorem by induction on $|R|$. Let R be a relation from A to B that satisfies Hall's condition $|R(X)| \geq |X|$ for all $X \subseteq A$. Suppose there exists a pair $(a, b) \in R$ such that $R - (a, b)$ saitsfies Hall's condition. Then we can find an injection in $R - (a, b)$. Suppose that for every pair (a, b) $R - (a, b)$ does not satisfy Hall's condition. Then prove that R itself must be an injection from A to B.

Question 4

Let R be a relation from A to B for finite sets A and B, such that there exists a number $k \geq 1$ such that $|R(a)| \geq k$ for all a in A and $|R^{-1}(b)| \leq k$ for all $b \in B$. Prove that R contains an injection from A to B. Let $\mathcal{A}$ be the set of all subsets of size k of $\{1, 2, \ldots, n\}$ where $k < \frac{n}{2}$. Let $\mathcal{B}$ be the set of all subsets of size $k + 1$ of $\{1, 2, \ldots, n\}$. The relation R from $\mathcal{A}$ to $\mathcal{B}$ is defined by $(X, Y) \in R$ iff $X \subseteq Y$, for subsets $X \in \mathcal{A}$ and $Y \in \mathcal{B}$. Prove that R contains an injective function from $\mathcal{A}$ to $\mathcal{B}$. Describe one such function f explicitly by showing how to calculate $f(X)$ given $X \in \mathcal{A}$. Try to extend this to the set of all multisubsets of size k of a multiset of size n.

Question 5

Suppose there are n students and m companies. A relation R from students to companies is defined by $(s, c) \in R$ iff student s is to be interviewed by company c. The interviews are conducted in slots of 15 minutes. A student can be interviewed by at most one company in a slot and a company can interview at most one student in a slot. Suppose that every student is to be interviewed by at most D companies and every company has to interview at most D students. Prove that it is always possible to schedule interviews such that at most D slots are required. Is it always possible to find such a schedule such that the slots for every company are consecutive, though they may start at different times? If so prove it, else find a counterexample.

Chapter 8

Equivalence Relations and Countability

Question 1

Prove that if A is a finite set, then any function on A is injective if and only if it is surjective. Use induction on the number of elements of A. Give examples of an injective function that is not surjective and a surjective function that is not injective for some set A. Show that if A is not finite, then there exists an injective function on A that is not surjective. Prove that every set is either finite or there exists an injection from $\mathbb{N}$ to A.

Question 2

Let R be a relation on a set A. We define R^k such that $R^0 = I$, and $R^{k+1} = R^k R$ for $k \geq 0$. For $k < 0$, we define $R^k = (R^{-1})^{-k}$. Do we have $R^{p+q} = R^p R^q$ for all $p, q \in \mathbb{Z}$? Show that for all $p, q \in \mathbb{Z}$, $R^{p+q} \subseteq R^p R^q$, and when p and q are either both non-negative or both non-positive, we have equality. Now, suppose there exists $k > 0$ such that $R^k = I$. Prove that R must be a bijection. You may use results from the previous question. Prove that if R is a bijection and A is finite, then there must exist a k such that $R^k = I$. Give an example to show that this may not be true if A is infinite. For a finite set A with n elements, what is the smallest number k such that for every bijection R on A, $R^k = I$? Prove your answer.

Question 3

Prove that the set of all finite subsets of $\mathbb{N}$ has the same cardinality as $\mathbb{N}$. Find an explicit bijection between these sets.In other words, given a finite subset of natural numbers, show how to compute a natural number from it, so that the original set can be recovered uniquely from the computed number. Do the same for all finite sequences of natural numbers. Note that there is no fixed bound on the size of the finite subset or the length of the finite sequence. All that is known is that it is some natural number.

Question 4

Let $A_0, A_1, \ldots$ be a countably infinite sequence of sets such that the intersection of any finite number of sets in the sequence is non-empty. Is it true that the intersection of all the sets is non-empty, ie there exists an x such that for all i $x \in A_i$? If so prove it, otherwise give a counterexample. What if one of the sets is finite? Suppose $a_0, a_1, \ldots$ is an infinite sequence of positive integers such that the gcd of any finite subsequence is greater than 1. Prove that there exists a prime p such that for all i, p divides a_i.

Question 5

Let R be an arbitrary relation defined on a set A. Write down an expression for the smallest equivalence relation E containing R. You can use the standard set theory operations along with the composition operation to obtain this expression. E is the smallest in the sense that any equivalence relation that contains R must also contain E. Suppose E is an equivalence relation on a finite set A with n elements and k equivalence classes. What is the minimum number of elements in a relation R on A such that the smallest equivalence relation containing R is the given relation E? Prove your answer using induction.

Question 6

Prove that the intersection of two equivalence relations on a set A (considered as a collection of ordered pairs) is also an equivalence relation. For any relation R on A, the smallest equivalence relation containing R, called the closure of R and denoted by R^c is the intersection of all equivalence relations containing R. Show that this is equivalent to the definition in the previous question. Let $\mathcal{E}$ be the set of all equivalence

relations on a set A. Define two operations $\cdot$ and $+$ on $\mathcal{E}$ as: $E_1 \cdot E_2 = E_1 \cap E_2$ and $E_1 + E_2 = (E_1 \cup E_2)^c$. Which axioms of a Boolean algebra do these operations satisfy? If they do not, give counterexamples, otherwise prove it. Prove that for all E_1 and E_2, $E_1 \cdot (E_1 + E_2) = E_1$ and $E_1 + E_1 \cdot E_2 = E_1$. These operations define a lattice called the lattice of partitions of A. An equivalence relation E_2 covers the equivalence relation E_1 iff $E_1 \subset E_2$ and there is no equivalence relation E such that $E_1 \subset E \subset E_2$. Prove that if E_1 covers $E_1 \cdot E_2$ then E_2 is covered by $E_1 + E_2$. Is the converse of this statement true?

Chapter 9

Partial Orders and Lattices

Question 1

Let $(A, \leq)$ be a partial order defined on a finite set A. Prove that there exists a total order on A that contains the $\leq$ relation. This is essentially topological sorting of a directed acyclic graph. Whether this holds for infinite sets or not is independent of the standard axioms of set theory. It depends on what is called the "axiom of choice" which is not a standard axiom. Can you think of how this could be proved for an infinite set? The dimension of a partial order is the minimum number of total orders whose intersection is the given partial order. In other words, $a \leq b$ holds in the partial order if and only if it holds in all the total orders. Prove that the dimension of any partial order on a set with n elements is at most $\lfloor \frac{n}{2} \rfloor + 1$. Give an example of a partial order on n elements whose dimension is $\lfloor \frac{n}{2} \rfloor + 1$.

Question 2

Let $a_1, a_2, \ldots, a_n$ be a sequence of numbers. Prove that for any number $k \geq 1$, either the sequence can be partitioned into k non-decreasing subsequences, or there exists a decreasing subsequence of $k + 1$ numbers (but not both). Using this or otherwise, give an efficient algorithm to find the longest subsequence that can be partitioned into k non decreasing subsequences.

Question 3

Let L be a lattice and let $\vee$ and $\wedge$ denote the *lub* and *glb* operations, also called the join and meet. Prove that these operations are commutative, associative and satisfy

the absorption laws $a \vee (a \wedge b) = a$ and $a \wedge (a \vee b) = a$, for all $a, b \in L$. Conversely, given two operations satisfying these properties, show that they define a lattice where $\wedge$ is the *glb* and $\vee$ is the *lub*. Note that it is not necessary to assume the existence of 1 and 0, as these may not exist for infinite lattices. The distributive property is not satisfied by many lattices. In particular, show that the partition lattice does not satisfy distributivity.

Question 4

Let $(A, \leq)$ be a partial order on a finite set A. A subset $I \subseteq A$ is called an ideal iff for all $a_1, a_2 \in A$, $a_1 \leq a_2$ and $a_2 \in I$ implies $a_1 \in I$. In other words, if an element belongs to I then all elements "smaller" than it belong to I. Prove that the union and intersection of any two ideals is an ideal. Let C be the collection of all ideals in A with the $\subseteq$ relation defined on it. Then C is a lattice with *glb* as intersection and *lub* as union, and therefore satisfies the distributivity property. Conversely, prove that if L is a finite distributive lattice, that is $\wedge$ and $\vee$ satisfy distributivity apart from the other lattice axioms, then it is isomorphic to a collection of ideals of some finite partially ordered set. First show that any such lattice is isomorphic to a collection of sets that is closed under union and intersection, and then show that any such collection is isomorphism to the collection of ideals of some poset.

Question 5

This problem was given to me by a past student, now a faculty member in NUS, (also a visiting faculty here, Kuldeep Meel) and considered one of the "rising stars" in AI. I don't know the application but the problem is on the Boolean lattice and is interesting by itself. I don't know the answer either (and neither did he, last I checked). Suppose I is an ideal in a finite Boolean lattice (set of all subsets of a k-element set for some k) with $|I| = n$. What is the minimum number of maximal elements in I? An element in I is maximal if it is not strictly less than any order element in I. For example, if $n = 2^k$, then a single maximal element is sufficient. Take any set with k elements, the ideal containing it will have 2^k elements (all subsets of the set), and the set will be the only maximal element. If $n = 2^k + 2^l - 1$ then 2 maximal elements, a subset of size k and a disjoint subset of size l, suffice. The -1 is because the empty set is counted twice. $n = 13$ is the smallest n for which 3 are needed, and a program, if correct, seemed to suggest that 419 is the smallest for which 4 are needed. It is not difficult to show that $O(\log n)$ elements suffice, but it seems like $O(\log \log n)$ are sufficient. Show that there are values of n for which $\Omega(\log \log n)$ are required. If you can prove the upper bound, write to him.

Chapter 10

Counting and Recurrences

Question 1

An involution is a bijection f from $[n]$ to itself such that f^2 is the identity function. A derangement is a bijection f such that $f(i) = i$ for all $i \in [n]$. Write down recurrence relations for the number of involutions and derangements. Given a bijection f on $[n]$ define an equivalence relation on $[n]$ by $i \equiv j$ iff there exists a number k such that $f^k(i) = j$. Let $S_{n,m}$ denote the number of bijections such that the corresponding equivalence relation has exactly m classes. Write down a recurrence relation for this in terms of n and m.

Question 2

Consider an arrangement of balls in layers such that the balls in each layer are placed consecutively touching each other, and except for the bottom layer, each ball is placed between two balls in the layer below. If there are n balls in the bottom layer, how many distinct arrangements are possible? For $n = 1$, there is only one, for $n = 2$, there are two, one in which there is only one layer and the other with a single ball in layer 2. For $n = 3$ there are 5, with distributions $(3), (3, 1), (3, 1), (3, 2)$ or $(3, 2, 1)$ of balls in layers. Prove that the number of possible arrangements is the Fibonacci number F_{2n-2}. Prove it using a recurrence and also by showing a bijection with the set of bit strings of length $2n - 3$ not containing 11, for $n > 1$.

Question 3

Prove that the number of bit strings of length n that do not contain any occurrence of 010 or 101 is $2F_n$. Prove it using a recurrence relation and also by giving a 1 to 2 function from the set of such bit strings to the set of bit strings of length $n-1$ not containing any occurrence of 11.

Question 4

Suppose a fair coin is tossed n times. Given that two consecutive heads did not occur in the n trials, what is the expected number of heads that have occurred? Let S be the set of sequences in which each entry is either +1 or -1 and the sum of entries in any prefix of the sequence is at least -2 and at most 2. How many such sequences of length n are possible? If each entry in the sequence is generated randomly with equal probability, and the sequence terminates as soon as the prefix condition is violated, what is the expected length of the sequence?

Question 5

The number of binary trees with n nodes T_n satisfies the recurrence $T_0 = 1$ and $T_n = \sum_{i=0}^{n-1} T_i T_{n-1-i}$. These numbers are called Catalan numbers. Find the generating function $T(x)$ of these numbers. Prove that T_n is odd if and only if $n = 2^k - 1$ for some $k \geq 0$. One way of doing it is by showing that binary trees can be paired up so that exactly one is left unpaired when $n = 2^k - 1$ and otherwise all are paired up. Ideally, the pairing should be such that only trees that are close to each other are paired up. The Catalan numbers also count a number of other objects (more than 200). For example, number of valid bracket strings, number of ways of partitioning a convex polygon into triangles (called triangulation), number of non-decreasing sequences $a_1 \leq a_2 \leq \cdots \leq a_n$ such that $a_i \leq i$ for each $1 \leq i \leq n$. In each case, the notion of "close" pairing may be different. In the bracket case, a string can be paired with one obtained by swapping some adjacent pair of characters. In the triangulation case, allow replacing one diagonal by another, in the sequence case, increase or decrease a number by 1. In each case, can you find such a "close pairing" with only one object left out when $n = 2^k - 1$?

Chapter 11

Undirected Graphs

Question 1

Give an example of a graph G for which the only automorphism is the identity function. An automorphism of G is a bijection from $V(G)$ to itself that preserves adjacency, that is, a bijection $f : V(G) \to V(G)$ such that vertex u is adjacent to vertex v if and only if $f(u)$ is adjacent to $f(v)$. How many automorphisms are there of the graphs P_n (path with n vertices), C_n (cycle with n vertices) and K_n (complete graph with n vertices)? If T_n is a tree with n vertices, what is the maximum possible number of automorphisms of T_n? Why? For which tree is the maximum value achieved?

Question 2

An edge e in a graph G is called a bridge if the graph $G - e$ obtained by deleting the edge e has more connected components than G. Prove that e is a bridge if and only if it is not contained in a cycle. Prove that if e is a bridge, then $G - e$ has exactly one more connected component than G and the endpoints of e are in different components of $G - e$. Prove that if for some vertices u, v there exists a path of odd length between u and v, and also a path of even length, then the graph must contain a cycle of odd length.

Question 3

Prove that every graph with n vertices and $n + 4$ edges must contain 2 cycles that have no edge in common with each other. Give examples of graphs with n vertices

and $n+3$ edges that do not contain two edge-disjoint cycles for $n \geq 6$. Prove that if $n \geq 6$, any graph with more than $3n-6$ edges must contain two vertex disjoint cycles. Give an example of a graph with n vertices and $3n-6$ edges that does not contain such cycles.

Question 4

Suppose G is a connected graph such that for any pair of vertices u and v all paths between u and v have the same length. The length may be different for different pairs of vertices. Prove that the graph must be a tree. Suppose now the path lengths can take at most two different values for each pair. What is the maximum possible number of edges in G, assuming it has n vertices?

Question 5

Prove that every graph with n vertices and more than $\frac{k(n-1)}{2}$ edges contains a path of length k. A famous conjecture of Erdős and Sős states that any such graph must contain as a subgraph any tree with k edges. This is known to be true for some special kinds of trees and for all trees when n is very large compared to k. Show that there are infinitely many n for which there are graphs with $\frac{k(n-1)}{2}$ edges that do not contain any tree with k edges. Try to find the minimum number of edges that an n vertex graph must have in order to contain a cycle of length at least k.