Discrete Mathematics
Lecture 2
Logic of Quantified Statements, Methods of Proof, Set Theory, Number Theory Introduction and General Good Times

Harper Langston

New York University

Predicates

- A predicate is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables
- The domain of a predicate variable is a set of all values that may be substituted in place of the variable
- P(x): x is a student at NYU

Predicates

- If P(x) is a predicate and x has domain D, the truth set of P(x) is the set of all elements in D that make P(x) true when substituted for x. The truth set is denoted as:

  $\{x \in D \mid P(x)\}$

- Let P(x) and Q(x) be predicates with the common domain D. $P(x) \Rightarrow Q(x)$ means that every element in the truth set of P(x) is in the truth set of Q(x). $P(x) \Leftrightarrow Q(x)$ means that P(x) and Q(x) have identical truth sets

Universal Quantifier

- Let P(x) be a predicate with domain D. A universal statement is a statement in the form "$\forall x \in D$, P(x)". It is true iff P(x) is true for every x from D. It is false iff P(x) is false for at least one x from D. A value of x form which P(x) is false is called a counterexample to the universal statement
- Examples
  - D = {1, 2, 3, 4, 5}: $\forall x \in D, x^2 >= x$

    $\forall x \in R, x^2 >= x$
- Method of exhaustion

Existential Quantifier

- Let P(x) be a predicate with domain D. An existential statement is a statement in the form "$\exists x \in D, P(x)$". It is true iff P(x) is true for at least one x from D. It is false iff P(x) is false for every x from D.
- Examples:

  $\exists m \in Z, m^2 = m$

  – $E = \{5, 6, 7, 8, 9\}, \exists x \in E, m^2 = m$

Universal Conditional Statement

- Universal conditional statement "$\forall x$, if P(x) then Q(x)":

  $\forall x$ R, if $x > 2$, then $x^2 > 4$

- Writing Conditional Statements Formally
- Universal conditional statement is called vacuously true or true by default iff P(x) is false for every x in D

Negation of Quantified Statements

- The negation of a universally quantified statement $\forall x \in D, P(x)$ is $\exists x \in D, \sim P(x)$
- "All balls in the bowl are red" – Vacuosly True Example for Universal Statements
- The negation of an existentially quantified statement $\exists x \in D, P(x)$ is $\forall x \in D, \sim P(x)$
- The negation of a universal conditional statement $\forall x \in D, P(x) \rightarrow Q(x)$ is $\exists x \in D, P(x) \wedge \sim Q(x)$

Exercises

- Write negations for each of the following statements:
  - All dinosaurs are extinct
  - No irrational numbers are integers
  - Some exercises have answers
  - All COBOL programs have at least 20 lines
  - The sum of any two even integers is even
  - The square of any even integer is even
- Let P(x) be some predicate defined for all real numbers x, let:

  $r = \forall x \in Z, P(x)$; $s = \forall x \in Q, P(x)$; $t = \forall x \in R, P(x)$
  - Find P(x) (but not $x \in Z$) so that r is true, but s and t are false
  - Find P(x) so that both r and s are true, but t is false

Variants of Conditionals

- Contrapositive
- Converse
- Inverse
- Generalization of relationships from before
- Examples

Necessary and Sufficient Conditions, Only If

- $\forall$ $\forall$x, r(x) is a sufficient condition for s(x) means: $\forall$x, if r(x) then s(x)
- $\forall$ $\forall$x, r(x) is a necessary condition for s(x) means: $\forall$x, if s(x) then r(x)
- $\forall$ $\forall$x, r(x) only if s(x) means: $\forall$x, if r(x) then s(x)

Multiply Quantified Statements

- For all positive numbers x, there exists number y such that $y < x$
- There exists number x such that for all positive numbers y, $y < x$
- For all people x there exists person y such that x loves y
- There exists person x such that for all people y, x loves y
- Definition of mathematical limit (pg 47)
- Order of quantifiers matters in some (most) cases (review pg 50)

Negation of Multiply Quantified Statements

- The negation of $\forall x, \exists y, P(x, y)$
  is logically equivalent to $\exists x, \forall y, \sim P(x, y)$
- The negation of $\exists x, \forall y, P(x, y)$
  is logically equivalent to $\forall x, \exists y, \sim P(x, y)$

Prolog Programming Language

- Can use parts of logic as programming lang.
- Simple statements:

  isabove(g, b), color(g, gray)
- Quantified statements:

  if isabove(X, Y) and isabove(Y, Z) then isabove(X, Z)
- Questions:

  ?color(b, blue), ?isabove(X, w)

Exercises

- Determine whether a pair of quantified statements have the same truth values

  $\forall x \in D, (P(x) \wedge Q(x))$ vs $(\forall x \in D, P(x)) \wedge (\forall x \in D, Q(x))$

  $\exists x \in D, (P(x) \wedge Q(x))$ vs $(\exists x \in D, P(x)) \wedge (\exists x \in D, Q(x))$

  $\forall x \in D, (P(x) \vee Q(x))$ vs $(\forall x \in D, P(x)) \vee (\forall x \in D, Q(x))$

  $\exists x \in D, (P(x) \vee Q(x))$ vs $(\exists x \in D, P(x)) \vee (\exists x \in D, Q(x))$

Arguments with Quantified Statements

- Rule of universal instantiation: if some property is true of everything in the domain, then this property is true for any subset in the domain
- Universal Modus Ponens:
  - Premises: ($\forall$x, if P(x) then Q(x)); P(a) for some a
  - Conclusion: Q(a)
- Universal Modus Tollens:
  - Premises: ($\forall$x, if P(x) then Q(x)); ~Q(a) for some a
  - Conclusion: ~P(a)
- Converse and inverse errors

Validity of Arguments using Diagrams

- Premises: All human beings are mortal; Zeus is not mortal. Conclusion: Zeus is not a human being
- Premises: All human beings are mortal; Felix is mortal. Conclusion: Felix is a human being
- Premises: No polynomial functions have horizontal asymptotes; This function has a horizontal asymptote. Conclusion: This function is not a polynomial

Proof and Counterexample

- Discovery and proof
- Even and odd numbers
  - number n from Z is called even if $\exists k \in Z, n = 2k$
  - number n from Z is called odd if $\exists k \in Z, n = 2k + 1$
- Prime and composite numbers
  - number n from Z is called prime if
    $\forall r, s \in Z, n = r * s \rightarrow r = 1 \vee s = 1$
  - number n from Z is called composite if
    $\exists r, s \in Z, n = r * s \wedge r > 1 \wedge s > 1$

Proving Statements

- Constructive proofs for existential statements
- Example: Show that there is a prime number that can be written as a sum of two perfect squares
- Universal statements: method of exhaustion and generalized proof
- Direct Proof:
  - Express the statement in the form: $\forall x \in D, P(x) \rightarrow Q(x)$
  - Take an arbitrary x from D so that P(x) is true
  - Show that Q(x) is true based on previous axioms, theorems, P(x) and rules of valid reasoning

Proof

- Show that if the sum of any two integers is even, then so is their difference
- Common mistakes in a proof
  - Arguing from example
  - Using the same symbol for different variables
  - Jumping to a conclusion
  - Begging the question

Counterexample

- To show that the statement in the form "$\forall x \in D, P(x) \rightarrow Q(x)$" is not true one needs to show that the negation, which has a form "$\exists x \in D, P(x) \wedge \sim Q(x)$" is true. **x** is called a counterexample.
- Famous conjectures:
  - Fermat big theorem: there are no non-zero integers x, y, z such that $x^n + y^n = z^n$, for $n > 2$
  - Goldbach conjecture: any even integer can be represented as a sum of two prime numbers
  - Euler's conjecture: no three perfect fourth powers add up to another perfect fourth power

Exercises

- Any product of four consecutive positive integers is one less than a perfect square
- To check that an integer is a prime it is sufficient to check that n is not divisible by any prime less than or equal to $\sqrt{n}$
- If p is a prime, is $2^p - 1$ a prime too?
- Does $15x^3 + 7x^2 - 8x - 27$ have an integer zero?

Rational Numbers

- Real number r is called rational if

  $\exists p,q \in Z,\ r = p / q$
- All real numbers which are not rational are called irrational
- Every integer is a rational number
- Sum of any two rational numbers is a rational number

Divisibility

- Integer n is a divisible by an integer d, when $\exists k \in Z, n = d * k$
- Notation: $d \mid n$
- Synonymous statements:
  - n is a multiple of d
  - d is a factor of n
  - d is a divisor of n
  - d divides n

Divisibility

- Divisibility is transitive: for all integers a, b, c, if a divides b and b divides c, then a divides c
- Any integer greater than 1 is divisible by a prime number
- If a | b and b | a, does it mean a = b?
- Any integer can be uniquely represented in the standard factored form:

  $n = p_1^{e_1} * p_2^{e_2} * \ldots * p_k^{e_k}$, $p_1 < p_2 < \ldots < p_k$, p_i is a prime number

Quotient and Remainder

- Given any integer n and positive integer d, there exist unique integers q and r, such that $n = d * q + r$ and $0 \leq r < d$
- Operations: div – quotient, mod – remainder
- Parity of an integer refers to the property of an integer to be even or odd
- Any two consecutive integers have opposite parity

Exercises

- Show that a product of any four consecutive integers is divisible by 8
- Show that the sum of any four consecutive integers is never divisible by 4
- Show that any prime number greater than 3 has remainder 1 or 5 when divided by 6

Floor and Ceiling

- For any real number x, the floor of x, written $\lfloor x \rfloor$, is the unique integer n such that $n \leq x < n + 1$. It is the max of all ints $\leq x$.
- For any real number x, the ceiling of x, written $\lceil x \rceil$, is the unique integer n such that $n - 1 < x \leq n$. What is n?
- If x is an integer, what are $\lfloor x \rfloor$ and $\lfloor x + 1/2 \rfloor$?
- Is $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$?
- For all real numbers x and all integers m, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$
- For any integer n, $\lfloor n/2 \rfloor$ is n/2 for even n and (n–1)/2 for odd n
- For positive integers n and d, $n = d * q + r$, where $d = \lfloor n / d \rfloor$ and $r = n - d * \lfloor n / d \rfloor$ with $0 \leq r < d$

Exercises

- Is it true that for all real numbers x and y:

  $\lfloor x - y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$

  $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$

  $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$

  $\lceil x + 1 \rceil = \lceil x \rceil + 1$

- Show that for all real x, $\lfloor \lfloor x/2 \rfloor /2 \rfloor = \lfloor x/4 \rfloor$

Contradiction

- Proof by contradiction
  - Suppose the statement to be proved is false
  - Show that this supposition leads logically to a contradiction
  - Conclude that the statement to be proved is true
- Square root of 2 is irrational
- There are infinite primes

Contraposition

- Proof by contraposition
  - Prepare the statement in the form: $\forall x \in D, P(x) \rightarrow Q(x)$
  - Rewrite this statement in the form: $\forall x \in D, \sim Q(x) \rightarrow \sim P(x)$
  - Prove the contrapositive by a direct proof
- Close relationship between proofs by contradiction and contraposition

Exercise

- Show that for integers n, n^2 is odd if and only if n is odd
- Show that for all integers n and all prime numbers p, if n^2 is divisible by p, then n is divisible by p
- For all integers m and n, if m+n is even then m and n are both even or m and n are both odd
- The product of any non-zero rational number and any irrational number is irrational
- If a, b, and c are integers and $a^2+b^2=c^2$, must at least one of a and b be even?
- Can you find two irrational numbers so that one raised to the power of another would produce a rational number?

Classic Number Theory Results

- Square root of 2 is irrational
- For any integer a and any integer $k > 1$,
  if $k \mid a$, then k does not divide $(a + 1)$
- The set of prime numbers is infinite

Exercises

- Show that
  - a square of 3 is irrational
  - for any integer a, 4 does not divide $(a^2 - 2)$
  - if n is not a perfect square then its square is irrational

    $\sqrt{2} + \sqrt{3}$ is irrational
  - $\log_2(3)$ is irrational
  - every integer greater than 11 is a sum of two composite numbers
  - if $p_1, p_2, \ldots, p_n$ are distinct prime numbers with $p_1 = 2$, then $p_1 p_2 \ldots p_n + 1$ has remainder 3 when divided by 4
  - for all integers n, if $n > 2$, then there exists prime number p, such that $n < p < n!$

Basics of Set Theory

- Set and element are undefined notions in the set theory and are taken for granted
- Set notation: $\{1, 2, 3\}$, $\{\{1, 2\}, \{3\}, \{1, 2, 3\}\}$, $\{1, 2, 3, \ldots\}$, $\emptyset$, $\{x \in R \mid -3 < x < 6\}$
- Set A is called a subset of set B, written as $A \subseteq B$, when $\forall x, x \in A \rightarrow x \in B$. What is negation?
- A is a proper subset of B, when A is a subset of B and $\exists x \in B$ and $x \notin A$
- Visual representation of the sets
- Distinction between $\subseteq$ and $\in$

Set Operations

- Set A equals set B, iff every element of set A is in set B and vice versa. $(A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A)$
- Proof technique for showing sets equality (example later for DeMorgan's Law)
- Union of two sets is a set of all elements that belong to at least one of the sets (notation on board)
- Intersection of two sets is a set of all elements that belong to both sets (notation on board)
- Difference of two sets is a set of elements in one set, but not the other (notation on board)
- Complement of a set is a difference between universal set and a given set (notation on board)
- Examples

Empty Set

- $S = \{x \in R, x^2 = -1\}$
- $X = \{1, 3\}$, $Y = \{2, 4\}$, $C = X \cap Y$ (X and Y are disjoint)
- Empty set has no elements $\varnothing$
- Empty set is a subset of any set
- There is exactly one empty set
- Properties of empty set:
  - $A \cup \varnothing = A$, $A \cap \varnothing = \varnothing$
  - $A \cap A^c = \varnothing$, $A \cup A^c = U$
  - $U^c = \varnothing$, $\varnothing^c = U$

Set Partitioning

- Two sets are called disjoint if they have no elements in common
- Theorem: A – B and B are disjoint
- A collection of sets $A_1, A_2, \ldots, A_n$ is called mutually disjoint when any pair of sets from this collection is disjoint
- A collection of non-empty sets $\{A_1, A_2, \ldots, A_n\}$ is called a partition of a set A when the union of these sets is A and this collection consists of mutually disjoint sets

Power Set

- Power set of A is the set of all subsets of A
- Example on board
- Theorem: if $A \subseteq B$, then $P(A) \subseteq P(B)$
- Theorem: If set X has n elements, then P(X) has 2^n elements

Cartesian Products

- Ordered n-tuple is a set of ordered n elements. Equality of n-tuples
- Cartesian product of n sets is a set of n-tuples, where each element in the n-tuple belongs to the respective set participating in the product

Set Properties

- Inclusion of Intersection:

  $A \cap B \subseteq A$ and $A \cap B \subseteq B$
- Inclusion in Union:

  $A \subseteq A \cup B$ and $B \subseteq A \cup B$
- Transitivity of Inclusion:

  $(A \subseteq B \wedge B \subseteq C) \rightarrow A \subseteq C$
- Set Definitions:

  $x \in X \cup Y \Leftrightarrow x \in X \vee y \in Y$

  $x \in X \cap Y \Leftrightarrow x \in X \wedge y \in Y$

  $x \in X - Y \Leftrightarrow x \in X \wedge y \notin Y$

  $x \in X^c \Leftrightarrow x \notin X$

  $(x, y) \in X \times Y \Leftrightarrow x \in X \wedge y \in Y$

Set Identities

- Commutative Laws: $A \cap B = A \cap B$ and $A \cup B = B \cup A$
- Associative Laws: $(A \cap B) \cap C = A \cap (B \cap C)$ and $(A \cup B) \cup C = A \cup (B \cup C)$
- Distributive Laws:

  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- Intersection and Union with universal set: $A \cap U = A$ and $A \cup U = U$
- Double Complement Law: $(A^c)^c = A$
- Idempotent Laws: $A \cap A = A$ and $A \cup A = A$
- De Morgan's Laws: $(A \cap B)^c = A^c \cup B^c$ and $(A \cup B)^c = A^c \cap B^c$
- Absorption Laws: $A \cup (A \cap B) = A$ and $A \cap (A \cup B) = A$
- Alternate Representation for Difference: $A - B = A \cap B^c$
- Intersection and Union with a subset: if $A \subseteq B$, then $A \cap B = A$ and $A \cup B = B$

Proving Equality

- First show that one set is a subset of another
- To show this, choose an arbitrary particular element as with direct proofs (call it x), and show that if x is in A then x is in B to show that A is a subset of B
- Example for DeMorgan's (step through all cases)

Disproofs, Counterexamples and Algebraic Proofs

- Is is true that $(A - B) \cup (B - C) = A - C$? (No via counterexample)
- Show that $(A \cup B) - C = (A - C) \cup (B - C)$ (Can do with an algebraic proof, slightly different)

Russell's Paradox

- Set of all integers, set of all abstract ideas
- Consider S = {A, A is a set and $A \notin A$}
- Is S an element of S?
- Barber puzzle: a male barber shaves all those men who do not shave themselves. Does the barber shave himself?
- Consider S = {$A \subseteq U$, $A \notin A$}. Is $S \in S$?
- Godel: No way to rigorously prove that mathematics is free of contradictions. ("This statement is not provable" is true but not provable) (consistency of an axiomatic system is not provable within that system)

Halting Problem

- There is no computer algorithm that will accept any algorithm X and data set D as input and then will output “halts” or “loops forever” to indicate whether X terminates in a finite number of steps when X is run with data set D.
- Proof is by contradiction (Read this pg 222, and we will review later)

Generic Functions

- A function f: X → Y is a relationship between elements of X to elements of Y, when each element from X is related to a unique element from Y
- X is called domain of f, range of f is a subset of Y so that for each element y of this subset there exists an element x from X such that y = f(x)
- Sample functions:
  - f : R → R, $f(x) = x^2$
  - f : Z → Z, f(x) = x + 1
  - f : Q → Z, f(x) = 2

Generic Functions

- Arrow diagrams for functions
- Non-functions
- Equality of functions:
  - $f(x) = |x|$ and $g(x) = \text{sqrt}(x^2)$
- Identity function
- Logarithmic function

One-to-One Functions

- Function $f : X \rightarrow Y$ is called one-to-one (injective) when for all elements x_1 and x_2 from X if $f(x_1) = f(x_2)$, then $x_1 = x_2$
- Determine whether the following functions are one-to-one:
  - $f : R \rightarrow R$, $f(x) = 4x - 1$
  - $g : Z \rightarrow Z$, $g(n) = n^2$
- Hash functions

Onto Functions

- Function $f : X \rightarrow Y$ is called onto (surjective) when given any element y from Y, there exists x in X so that $f(x) = y$
- Determine whether the following functions are onto:
  - $f : R \rightarrow R$, $f(x) = 4x - 1$
  - $f : Z \rightarrow Z$, $g(n) = 4n - 1$
- Bijection is one-to-one and onto
- Reversing strings function is bijective

Inverse Functions

- If $f : X \rightarrow Y$ is a bijective function, then it is possible to define an inverse function f^{-1}: $Y \rightarrow X$ so that $f^{-1}(y) = x$ whenever $f(x) = y$
- Find an inverse for the following functions:
  - String-reverse function
  - $f : R \rightarrow R$, $f(x) = 4x - 1$
- Inverse function of a bijective function is a bijective function itself

Composition of Functions

- Let f : X → Y and g : Y → Z, let range of f be a subset of the domain of g. The we can define a composition of g o f : X → Z
- Let f,g : Z → Z, f(n) = n + 1, g(n) = n^2. Find f o g and g o f. Are they equal?
- Composition with identity function
- Composition with an inverse function
- Composition of two one-to-one functions is one-to-one
- Composition of two onto functions is onto

Pigeonhole Principle

- If n pigeons fly into m pigeonholes and n > m, then at least one hole must contain two or more pigeons
- A function from one finite set to a smaller finite set cannot be one-to-one
- In a group of 13 people must there be at least two who have birthday in the same month?
- A drawer contains 10 black and 10 white socks. How many socks need to be picked to ensure that a pair is found?
- Let A = {1, 2, 3, 4, 5, 6, 7, 8}. If 5 integers are selected must at least one pair have sum of 9?

Pigeonhole Principle

- Generalized Pigeonhole Principle: For any function f : X → Y acting on finite sets, if n(X) > k * N(Y), then there exists some y from Y so that there are at least k + 1 distinct x's so that f(x) = y
- "If n pigeons fly into m pigeonholes, and, for some positive k, m >k*m, then at least one pigeonhole contains k+1 or more pigeons"
- In a group of 85 people at least 4 must have the same last initial.
- There are 42 students who are to share 12 computers. Each student uses exactly 1 computer and no computer is used by more than 6 students. Show that at least 5 computers are used by 3 or more students.

Cardinality

- Cardinality refers to the size of the set
- Finite and infinite sets
- Two sets have the same cardinality when there is bijective function associating them
- Cardinality is is reflexive, symmetric and transitive
- Countable sets: set of all integers, set of even numbers, positive rationals (Cantor diagonalization)
- Set of real numbers between 0 and 1 has same cardinality as set of all reals
- Computability of functions