CMSC 141
Automata and Language Theory

chapter 0

preliminaries

- review proof techniques
  - direct proof
  - proof by contradiction
  - proof by mathematical induction

proof

- a sequence/series of formal statements
  - givens
  - deductions

direct proof

- a sequence of statements which are either givens or deductions from previous statements
  - deductions
    - established facts
    - axioms
    - lemmas
    - theorems

direct proof

- the sum of two even integers is an even integer
  - givens
    - even integers
    - definition
      - a number is said to be even if and only if it is of the 2k where k $\in \mathbb{Z}$
      - sample
        - 28, 2*14, 14 $\in \mathbb{Z}$
        - 38, 2*19, 19 $\in \mathbb{Z}$
        - -6, 2*(-3), -3 $\in \mathbb{Z}$

direct proof

- the sum of two even integers, a and b, is an even integer
  - $a = 2k$
  - $b = 2j$
  - $a + b = 2k + 2j$
  - $a + b = 2(k + j)$
    - $k \in Z$ and $j \in Z$, therefore $(k + j) \in \mathbb{Z}$
    - let $m = k + j$
    - $a + b = 2m$
    - h.n.

direct proof

- the sum of two odd numbers, a and b is even
  - givens
    - odd integers
    - definition
      - a number is said to be odd if and only if it is of the $2k + 1$ where $k \in \mathbb{Z}$
      - sample
        - $27, 2*13 + 1, 13 \in \mathbb{Z}$
        - $39, 2*19 + 1, 19 \in \mathbb{Z}$
        - $-7, 2*(-4) + 1, -4 \in \mathbb{Z}$

direct proof

- the sum of two odd numbers, a and b is even
  - a = 2k + 1
  - b = 2j + 1
  - a + b = 2k + 1 + 2j + 1
  - a + b = 2(k + j + 1)
    - let m = k + j + 1
    - a + b = 2m
    - h.n.

direct proof

- The summation of i from 1 to n is n(n+1)/2
  - n = 4
    - 1 + 2 + 3 + 4 = 10
    - 4(5)/2 = 10

direct proof

- The summation of i from 1 to n is n(n+1)/2
  - Let S be this sum
  - S = 1 + 2 + 3 + … n-1 + n
  - S = n+(n-1)+(n-2)+...+ 2 +1
  - 2S = (n+1)+(n+1)+(n+1)+...+(n+1)+(n+1)
  - 2S = n(n+1)
  - S = n(n+1)/2
  - h.n.

prove the following via direct proof

- sum of an even number and odd number is odd
- product of two odd numbers is odd
- the square of an even number is even

proof (disproof) by counterexample

- prove/disprove by giving one example or instance that disproves the case
  - $\forall$ real numbers a and b, if $a^2 = b^2$, then $a = b$
    - one counterexample is sufficient
    - $a = 2$, $b = -2$
    - $2^2 = 4$
    - $(-2)^2 = 4$
    - h.n.

proof (disproof) by counterexample

- ∀ positive integers n, if n is prime, then n is odd
  - Some prime numbers
    - 3, 5, 7 11, 23, 31
  - But 2 is prime
    - 2 is even
    - $2 = 2 * 1, 1 \in Z$
    - h.n.

proof by contradiction

- Assume that the opposite proposition is true then show or arrive at a contradiction

proof by contradiction

- Prove that the $\sqrt{2}$ is irrational
  - Assume that the opposite is true
    - $\sqrt{2}$ is rational
    - rational
      - any number that can be expressed as a quotient or ratio p/q, where p and $q \in Z$ and $q \neq 0$, and p/q is in lowest terms
    - $\sqrt{2} = p/q$

proof by contradiction

- Prove that the $\sqrt{2}$ is irrational
  - $\sqrt{2} = p/q$
  - $2 = p^2/q^2$
  - $2q^2 = p^2$
  - p^2 is even
  - p is even
  - $p = 2k$
  - $2q^2 = (2k)^2$
  - $q^2 = 2k^2$
  - q is even
  - since p and q are both even, they have a common factor and therefore not in lowest terms

proof by contradiction

- Show that $p^2 - q^2 = 1$ does not have positive integer solutions

proof by mathematical induction

- ❏ Base Step
- ❏ Inductive Hypothesis
- ❏ Inductive Step

proof by mathematical induction

- The summation of i from 1 to n is n(n+1)/2

Challenge

\---

Prove by Mathematical Induction that for any positive integer number n, $n^3 + 2n$ is divisible by 3.

- ❑ Base Step
- ❑ Inductive Hypothesis
- ❑ Inductive Step

sets

- A set is a collection (unordered) of objects
- Example:
  - Collection of four letters w, x, y, z (named L)
    - L = {w, x, y, z}
  - S = {red, blue, red}
  - S = {red, blue}
  - S = {blue, red}
    - Two sets are equal if they have the same elements

sets

- The objects comprising the set are called its elements or members
  - x is an element of the set L
  - $x \in L$

sets

- More samples
  - S = {3, red, {d, blue}}
    - How many elements?
    - cardinality of a set
      - |S|
  - T = {A}
    - singleton
  - Ø is called the empty set
    - |Ø|

sets

- Ways of specifying sets
  - Listing
  - Use of ellipsis
    - Z = {0, 1, 2, …}
  - Referring to other sets and to properties that elements may or may not have
    - I={1,3,9}, G={3,9}
    - G={x:x ϵ I and x is greater than 2}
    - Generally, S={x:xϵA and x has property P}
      - O={x:xϵN and x is not divisible by 2}

sets

- How do we prove that two sets are equal?
  - We may prove that $A \subseteq B$ and $B \subseteq A$
  - subset
    - A set A is a subset of a set B, $A \subset B$, if each element of A is also an element of B
    - If A is a subset of B but not the same as B,we say that A is proper subset of B, $A \subset B$

sets

- Let S be a set.
  - If there are exactly n distinct elements in S, where n is a non-negative integer, we say S is a finite set and that n is the cardinality of S.
  - The cardinality of S is denoted by |S|.
  - S = {1, 2, 3, 2, 5}
  - |S| = ?

set

- A set is infinite if it is not finite.
  - The set of natural numbers is an infinite set.
  - N = {1, 2, 3, ... }
  - The set of reals is an infinite set.

sets

- Given a set S, the powerset of S is the set of all subsets of S. The power set is denoted by P(S).
  - Assume an empty set ∅
    - What is the power set of ∅ ?
    - $P(\emptyset) = \{ \emptyset \}$
      - What is the cardinality of $P(\emptyset)$?
      - $|P(\emptyset)| = 1$.
    - Assume set $A = \{1\}$
      - $P(A) = ?$

sets

- Two sets can be combined to form a third set by various set operations.
  - union
    - $A \cup B = \{x : x \in A \text{ or } x \in B\}$
  - intersection
    - $A \cap B = \{x : x \in A \text{ and } x \in B\}$
  - difference
    - $A - B = \{x : x \in A \text{ and } x \notin B\}$
- $A = \{1, 2, 3, 4, 5\}$
- $B = \{9, 3, 6, 2, 10\}$

sets

- If A, B and C are sets, then following laws hold
  - $A \cup A = A$ (Idempotency)
  - $A \cap A = A$ (Idempotency)
  - $A \cup B = B \cup A$ (Commutativity)
  - $A \cap B = B \cap A$ (Commutativity)
  - $(A \cup B) \cup C = A \cup (B \cup C)$ (Associativity)
  - $(A \cap B) \cap C = A \cap (B \cap C)$ (Associativity)
  - $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ (Distributivity)
  - $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ (Distributivity)

sets

- If A, B and C are sets, then following laws hold
  - $(A \cup B) \cap A = A$ (Absorption)
  - $(A \cap B) \cup A = A$ (Absorption)
  - $A - (B \cup C) = (A-B) \cap (A-C)$ (DeMorgan's)
  - $A - (B \cap C) = (A-B) \cup (A-C)$ (DeMorgan's)

sets (challenge)

- Determine if each of the following is true or false
  - $\varnothing \subseteq \varnothing$
  - $\varnothing \in \{\varnothing\}$
  - $\varnothing \subseteq \{\varnothing\}$
  - $\{a,b\} \in \{a,b,c, \{a,b\}\}$
  - $\{a,b\} \subseteq \{a,b, \{a,b\}\}$
  - $\{a,b\} \subseteq 2^{\{a,b, \{a,b\}\}}$
  - $\{a,b\} \subseteq 2^{\{a,b, \{a,b\}\}}$
  - $\{a,b, \{a,b\}\} - \{a,b\} = \{a,b\}$

sets (challenge)

- What are these sets?
  - $(\{1,3,5\} \cup \{3,1\}) \cap \{3,5,7\}$
  - $(\{1,2,5\} - \{5,7,9\}) \cup (\{5,7,9\} - \{1,2,5\})$
  - $2^{\{7,8,9\}} - 2^{\{7,9\}}$
  - $\bigcup\{\{3\},\{3,5\}, \bigcap\{\{5,7\},\{7,9\}\}\}$

challenge

Show that the sum of the squares from 1 to n is (n(n+1)(2n+1))/6. Prove the claim via Mathematical Induction.

sets

- Prove the following:
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A - (B \cup C) = (A - B) \cap (A - C)$

sets

- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $u \in A \cup (B \cap C)$
  - $(u \in A)$ or $(u \in B \cap C)$
  - $(u \in A)$ or $((u \in B)$ and $(u \in C))$
  - $((u \in A)$ or $(u \in B))$ and $((u \in A)$ or $(u \in C))$
  - $(u \in A \cup B)$ and $(u \in A \cup C)$
  - $u \in (A \cup B) \cap (A \cup C)$

sets

- A – (B U C) = (A – B) ∩ (A – C)
- Let L = A – (B U C) and R = (A – B) ∩ (A – C)
- Show that each of them is a subset of each other
  - Let x be any element of L
    - x ϵ A but x is not ϵ of B and x is not ϵ C
    - Therefore, x ϵ A – B and A – C and thus is an element of R.

sets

- Let x be any element of R
  - x ∈ of both A – B and A – C which means x is in A but neither in B nor C
  - Therefore x ϵ A but x is not an element of B U C making x ∈ L

sets

- Two sets are disjoint if they have no element in common, that is, if their intersection is empty.
- A partition of a non-empty set A is a subset Π of 2^A such that ∅ is not an element of Π and such that each element of A is in one and only one set in Π.
    - Each element of Π is nonempty
    - Distinct members of Π are disjoint
    - $\bigcup \Pi = A$
    - A={a,b,c,d}
        - {{a,b},{c},{d}} or {{b,c},{c,d}}???

relations

- “less than”
  - 4 and 7
  - 7 and 4
  - 4 and 4
- relation
  - a set
    - elements
    - combinations of individuals for which that relation holds in the intuitive sense
  - “less than” relation
    - set of all pairs of numbers such that the first number is less than the second

relations

- how are the pairs written?
- how do we distinguish the first from the second?
    - {4,7}?
        - {7,4}
    - ordered pair
        - (a,b)
            - a and b are the components
            - (a,b) is different from (b,a)
                - order matters
            - (b,b)
                - need not be distinct

relations

- cartesian product of two sets A and B
  - A x B
  - set of all ordered pairs (a,b) with $a \in A$ and $b \in B$
    - {1,3,9} x {b, c, d}
    - {(1,b), (1, c), (1,d), (3,b), (3,c), (3,d), (9,b), (9,c), (9,d)}

relations

- A binary relation on two sets A and B is a subset of A x B.
  - $\{(i, j): i,j \in N \text{ and } i < j\}$
    - Subset of N x N
- More generally, let n be any natural number, then if $a_1, \ldots, a_n$ are any n objects, not necessarily distinct, $(a_1, \ldots, a_n)$ is an ordered tuple.

relations

- ordered 2-tuples are the same as the ordered pairs, and ordered 3-, 4-, 5-, and 6-tuples are called ordered **triples**, **quadruples**, **quintuples**, and **sextuples**, respectively
- an n-ary relation on sets A_1, ... ,A_n is a subset of A_1 x ... x A_n; 1-, 2-, and 3-ary relations are called **unary**, **binary**, and **ternary** relations, respectively

functions

- An association of each object of one kind with a unique object of another kind
  - Persons and ages
  - Dogs and owners
- A function from a set A to a set B is a binary relation R on A and B with the following property:
  - For each $a \in A$, there is exactly one ordered pair in R with first component a.

functions

- Let C be the set of cities in the Philippines and let P be the set of provinces and let
  - $R_1 = \{(x,y): x \in C,\ y \in P, \text{ and } x \text{ is a city in } y\}$
  - $R_2 = \{(x,y): x \in P,\ y \in C, \text{ and } y \text{ is a city in } x\}$
- We use the letters f, g and h for functions and we write
  - $f: A \rightarrow B$
  - A is the domain
  - f(a) is called the image of *a* under f, $a \in A$

functions

- A function $f: A \to B$ is one-to-one if for any two distinct elements $a, a' \in A$, $f(a) \neq f(a')$
- A function $f: A \to B$ is onto B if each element of B is the image under f of some element of A.
- A mapping $f: A \to B$ is a bijection between A and B if it is both one-to-one and onto
- The inverse of a binary $R \subseteq A \times B$, denoted by $R^{-1} \subseteq B \times A$, is simply the relation $\{(b,a): (a,b) \in R\}$.