Math/CSE 1019C: Discrete Mathematics for Computer Science

Fall 2012

Jessie Zhao
jessie@cse.yorku.ca

Course page: http://www.cse.yorku.ca/course/1019

Review of Proofs

- Inference Rules
  - ∵ Hypothesis
  - ∴ conclusion
- Direct Proof
  - Including proof by cases, proof by exhaustion
- Proof by contraposition
- Proof by contradiction
- Proof of Equivalences
- Uniqueness proofs
- Disproof by counterexample

Exercises

- If n+1 balls are distributed among n bins prove that at least one bin has more than 1 ball
  - Prove by contradiction
- Prove $|x-y| \le |x|+|y|$ for all real number x and y.
  - Prove by cases.

Proof of Existence

- How to prove $\exists x P(x)$?
- Constructive existence proof: Find an element c such that P(c) is true
- Nonconstructive existence proof:
  - Prove $\exists x P(x)$ is true in some other way
  - Assume no c exists which makes P(c) true and derive a contradiction

Constructive Existence Proof (Example)

There exists integers x,y,z satisfying $x^2+y^2 = z^2$

Proof: $x = 3$, $y = 4$, $z = 5$.

Nonconstructive Existence proof (Example)

- There exists irrational x,y, such that x^y is rational
- Proof (by non-construction):
  - By previous example: $\sqrt{2}$ is irrational
  - For $(\sqrt{2})^{\sqrt{2}}$
    - Case 1: If $(\sqrt{2})^{\sqrt{2}}$ is rational, then the theorem is proved
    - Case 2: If $(\sqrt{2})^{\sqrt{2}}$ is irrational, $((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$ is rational
  - Q.E.D.
- Attention: We did not find the actual pair of irrational x, y. It could be $x = \sqrt{2}$, $y = \sqrt{2}$, or $x = (\sqrt{2})^{\sqrt{2}}$, $y = \sqrt{2}$.

Disproof by Counterexample

- How to prove $\forall xP(x)$ is not true?

  $\neg\forall xP(x) \equiv \exists x\neg P(x)$
- Find a counterexample c such that P(c) is false
- Example: All prime numbers are odd
  - Proof: 2 is a prime number, and it is even.

Proof Strategies

- Finding proofs can be challenging
  - Replace terms by their definitions
  - Carefully analyze hypotheses and conclusion
  - Choose a proof method
  - Attempt to prove the theorem
  - If it fails try different proof methods

Sets

- Unordered collection of distinct objects (called the elements, or members, of the set)
- Elements could be:
  - Positive integers
  - Sides of a coin
  - Students enrolled in 1019A
  - Sets

Set Membership

- $a \in A$: a is an element of the set A
- $a \notin A$: a is not an element of the set A
- Example:
  - V: {a,e,i,o,u} -- $a \in V$, $b \notin V$
  - T: {1, 2, 3, 4, ..., 99} -- $55 \in T$, $100 \notin T$
  - S: {a, 2, {a}} -- $a \in S$, $\{a\} \in S$, $\{\{a\}\} \notin S$

Describing Sets

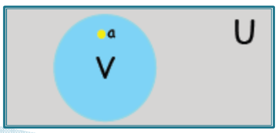
- Roster method

  {a, b, c, d}
- Set builder notation (specification by predicates):

  $S = \{x \mid P(x)\}$
  - S contains all the elements which make P(x) true
  - Characterize all elements in the set by stating properties they must have
  - E.g. O = {x | x is an odd positive integer less than 6}

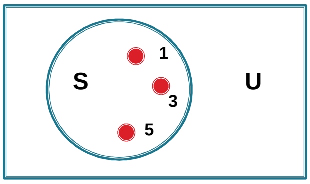
Venn Diagrams

- Venn Diagrams: Rectangle, circles, points
  - Rectangle: Universal set U contains all the objects under consideration
  - Circle and other geometrical figures: Sets
  - Points: Elements
  - Often used to show relationships between sets



Set Examples

- $S = \{1, 3, 5\}$
- $S = \{x \mid x$ is an odd positive integer less than 6$\}$
  - $S = \{x \mid x$ is odd and $x>0$ and $x<6\}$



Important Sets

- Set of natural numbers: N $= \{0,1,2,3,\ldots\}$
- Set of integers: Z $= \{\ldots,-2,-1,0,1,2,\ldots\}$
- Set of positive integers: $Z^+ = \{1,2,3,\ldots\}$
- Set of rational numbers: Q $= \{p/q \mid p\in Z, q\in Z,$
- and $q\neq 0\}$
- Set of real numbers: R

- Intervals
  - $[a,b] = \{x \mid a \le x \le b\}$
  - $[a,b) = \{x \mid a \le x < b\}$
  - $(a,b] = \{x \mid a < x \le b\}$
  - $(a,b) = \{x \mid a < x < b\}$
- In Computer Science, a data type is the concept of a set
  - Boolean
  - Integer

Size of Sets

- Let S be a set
  - Cardinality $|S|$: number of (distinct) elements
  - Finite set: cardinality is some finite integer n
  - Infinite set: a set that is not finite
- Special sets
  - Empty set: $\varnothing$ or { }
    - Cardinality=?
  - Singleton set: A set with one element

Equivalence of Sets

- Two sets A and B are equal iff they have the same elements.

$$A=B \text{ iff } \forall x(x\in A \leftrightarrow x\in B)$$

  - $\{1,2,3\} = \{3,1,2\}$
  - $\{1,1,1\} = \{1\}$
  - $\{\varnothing,\varnothing\} = \{\varnothing\} \neq \varnothing$
  - $Z \neq N$

Subsets

- Subset $A\subseteq B$: Every element of A is also an element of B.

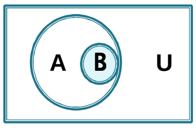
$$\forall x(x\in A \rightarrow x\in B)$$

- Proper subset $A\subset B$: $A\subseteq B$ but $A\neq B$

$$\forall x(x\in A \rightarrow x\in B) \land \exists x(x\in B \land x\notin A)$$

- $A=B$ if and only if $A\subseteq B$ and $B\subseteq A$

- Subset Venn Diagrams



- Special Subsets
  - $S \subseteq S$
  - $\varnothing \subseteq S$
  - $S \subseteq U$

Power Set

- Power Set P(S): set of all subsets of S
  - P(S) includes S, $\varnothing$
  - If $|S|=n$ then $|P(S)|=2^n$
- E.G.
  - If A = {a,b}, then P(A)={$\varnothing$,{a},{b},{a,b}}
  - Tricky question: What is P($\varnothing$) and P({$\varnothing$})?
    - P($\varnothing$)={$\varnothing$}
    - P({$\varnothing$}) = {$\varnothing$, {$\varnothing$}}

Cartesian Products

- The Cartesian product of A with B, denoted by AXB is the set of ordered pairs

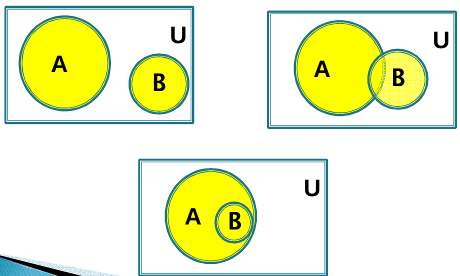
  AXB = {<a,b> | $a \in A \wedge b \in B$}
  - $A_1 X A_2 X \ldots X A_n = \{< a_1, a_2, \ldots, a_n > | a_i \in A_i\}$, for i=1,2,...,n}
- Example: A = {a,b}, B={1,2,3}
  - AxB = {<a,1>,<a,2>,<a,3>,<b,1>,<b,2>,<b,3>}
  - BxA = {<1,a>,<1,b>,<2,a>,<2,b>,<3,a>,<3,b>}
- If |A| = m and |B| = n, then |AxB| = mn.
- The cartesian product of anything with $\varnothing$ is $\varnothing$.

Set Operations

- Union: $A \cup B = \{x | (x \in A) \vee (x \in B)\}$
- Intersection: $A \cap B = \{x | (x \in A) \wedge (x \in B)\}$
- Disjoint sets: A, B are disjoint iff $A \cap B = \varnothing$
- Difference: $A - B = \{x | (x \in A) \wedge (x \notin B)\}$
- Complement: A^c or $\bar{A} = \{x | x \notin A\} = U - A$

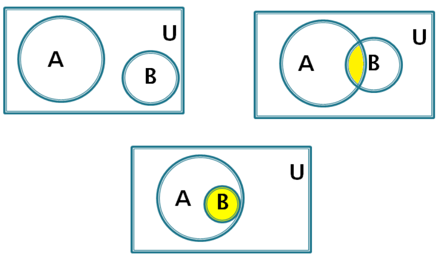
Union A∪B

- $A \cup B = \{x | (x \in A) \vee (x \in B)\}$



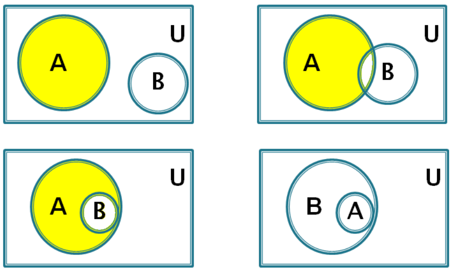
Intersection A∩B

- $A \cap B = \{x | (x \in A) \wedge (x \in B)\}$



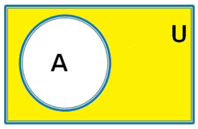
Difference A–B

- A–B = {x|(x∈A)∧(x∉B)}



Complement A^c or $\bar{A}$

- Complement: A^c or $\bar{A}$ = {x|x∉A} = U–A



Example

- For U = {0,1,2,3,4,5,6,7,8,9,10},
- If A = {1,2,3,4,5}, B = {4,5,6,7,8}, then:
  - A∪B = {1,2,3,4,5,6,7,8}
  - A∩B = {4,5}
  - A–B = {1,2,3}
  - B–A = {6,7,8}
  - $\bar{A}$ = {6,7,8,9,10}

Set Identities

- Set identities correspond to logical equivalences
- Important Set Identities: Page 130
- How to prove the set identities?
  - Show each set is a subset of the other
  - Use membership tables
- An example: De Morgan's Law

Example: De Morgan

Prove: $\overline{A \cup B} = \bar{A} \cap \bar{B}$

(1) Showing $\forall x(x \in \overline{A \cup B} \leftrightarrow x \in \bar{A} \cap \bar{B})$

Let x be arbitrary

Example: De Morgan

$x \in \overline{A \cup B}$	
$\equiv x \notin A \cup B$	Def. of complement
$\equiv \neg(x \in A \cup B)$	Def. of $\notin$
$\equiv \neg(x \in A \vee x \in B)$	Def. of $\cup$
$\equiv \neg(x \in A) \wedge \neg(x \in B)$	De Morgan's las
$\equiv x \notin A \wedge x \notin B$	Def. of $\notin$
$\equiv x \in \bar{A} \wedge x \in \bar{B}$	Def. of complement
$\equiv x \in \bar{A} \cap \bar{B}$	Def. of $\cap$

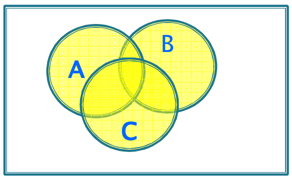
Example: De Morgan

(2) Proof by using a membership table

A	B	$A \cup B$	$\overline{A \cup B}$	$\overline{A}$	$\overline{B}$	$\overline{A} \cap \overline{B}$
1	1	1	0	0	0	0
1	0	1	0	0	1	0
0	1	1	0	1	0	0
0	0	0	1	1	1	1

Generalized Unions

- $A \cup B \cup C$

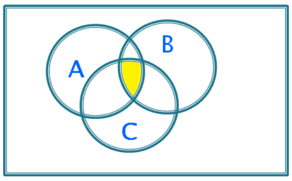


- Union of a collection of sets

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n$$

Generalized Intersections

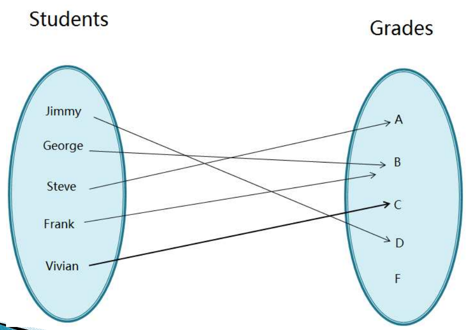
- $A \cap B \cap C$



- Intersection of a collection of sets

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n$$

Introduction to functions



Introduction to functions

- A function from A to B is an assignment of exactly one element of B to each element of A.

- Formal definition:
  f: A→B is a subset of AxB such that

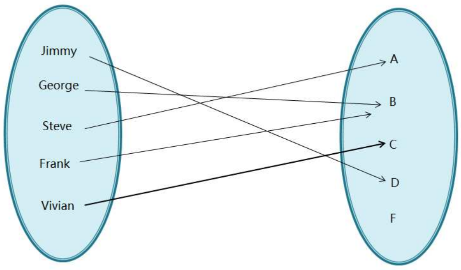
$$\forall x(x \in A \rightarrow \exists y(y \in B \wedge \langle x,y \rangle \in f))$$
and
$$(\langle x,y_1 \rangle \in f \wedge \langle x,y_2 \rangle \in f) \rightarrow y_1 = y_2$$

Example

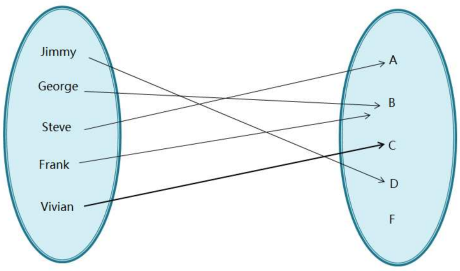
- Function
  - Let A = B = integers, $f(x) = x+10$
  - Let A = B = integers, $f(x) = x^2$
- Not a function
  - A = B = real numbers $f(x) = \sqrt{x}$
  - A = B = real numbers, $f(x) = 1/x$

Terminology

- For a function f: A→B
  - A is called the domain
  - B is called the co-domain
- If f(x)=y
  - y is called the image of x under f. The set of all images is called the range of f, denoted by f(A)
    - Note: range(f) = {y| ∃ x ∈ A f(x) = y} ⊆ B
  - x is called a preimage of y



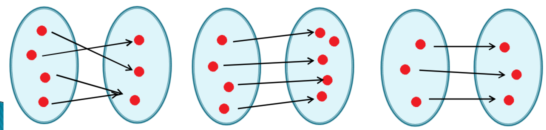
- f: S→G
  - The domain of f: S={Jimmy, George, Steve, Frank, Vivian}
  - The co-domain of f: G={A,B,C,D,F}



- f(George) = B
- The image of George is B.
- The preimages of B are George and Frank.
- The range of f: f(S)={A,B,C,D}

Surjections, Injections and Bijections

- f is surjective or onto if its range is equal to its codomain,
  - i.e. for every y in B there must be an x in A such that f(x)=y.
- f is injective or one-to-one (denoted 1-1), if it maps distinct elements of the domain to distinct elements of the range,
  - i.e. if a≠b then f(a)≠f(b).
- f is bijective or one-to-one correspondence if it is surjective and injective.



Examples

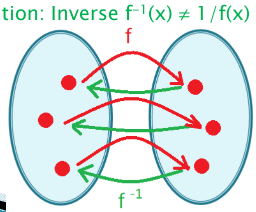
- Let A = B = R, the real numbers. Determine f: A->B, which are injections, surjections, bijections:
  - $f(x) = x$
  - $f(x) = x^2$
  - $f(x) = x^3$
  - $f(x) = |x|$

Inverse Functions

- Let f be a bijection from A to B, then the inverse of f, denoted f^{-1}:B→A is defined as

$$f^{-1}(y)=x \text{ iff } f(x)=y$$

  - A bijective function is called invertible
  - A non-bijective function is not invertible
  - Pay attention: Inverse $f^{-1}(x) \neq 1/f(x)$



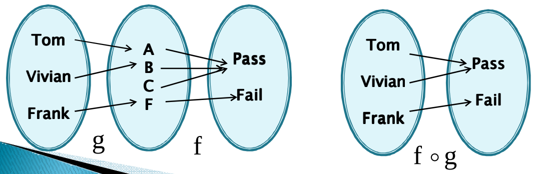
- Example:
  - Let f: {a,b,c}->{1,2,3} be such that f(a)=2, f(b)=1, f(c)=3.
  - Let f: R->R be such that $f(x) = x^2$
  - Let f: $R^+ \to R^+$ be such that $f(x) = x^2$

Composition of Functions

- Let g: A→B, f: B→C. The composition of f and g, denoted $f \circ g(x)$ is the function from A to C defined by

$$f \circ g(x) = f(g(x))$$

- Note that $f \circ g$ is not defined unless the range of g is a subset of the domain of f.



Example

- Let f: Z→Z defined by f(x)=2x and g:Z→Z defined by $g(x)=x^2$.
  - What is $f \circ g$ (x)?
  - What is $g \circ f$ (x)?
- Solution:

  $f \circ g(x)=f(g(x))=f(x^2)=2(x^2)=2x^2$

  $g \circ f(x)=g(f(x))=g(2x)=(2x)^2=4x^2$
- Note: $f \circ g$ (x) and $g \circ f$ (x) are not equal

Special functions

- Identity Id(x)=x

  Note: $f \circ f^{-1} = f^{-1} \circ f = Id$

- Floor
- Ceiling
- DecimalToBinary
- BinaryToDecimal

Special functions

- BinaryToDecimal
  - $n = 1001_2$
  - $n = 1*2^3 + 0*2^2 + 0*2^1 + 1*2^0 = 9$

- DecimalToBinary
  - n = 7
  - b_1 = n rem 2 = 1, n = n div 2 = 3

    b_2 = n rem 2 = 1, n = n div 2 = 1

    b_3 = n rem 2 = 1, n = n div 2 = 0.

    STOP

    Then we have $7 = 111_2$

Reading and Notes

- Read Section 1.8, 2.1-2.3
- Proofs
  - Practice proofs techniques and strategies.
- Sets
  - Understand the concept of sets, set membership, subset, cardinality, powerset, cartesian product of sets. Understand the relationship between set operations and logic operations. Practice proving set identities
- Functions
  - Understand the concept of function. Practice distinguishing injection (1-1), surjection (onto) and bijection. Practice finding the composition and inverse of functions