CSN-106 Discrete Structures

INDIAN INSTITUTE OF TECHNOLOGY ROORKEE

NAME OF DEPT/CENTRE: **Computer Science and Engineering**

1. Subject Code: **CS - 106** Course Title: **Discrete Structures**

2. Contact Hours: **L: 3** **T: 1** **P: 0**

3. Examination Duration (Hrs.): **Theory** | 0 | 3 | **Practical** | 0 | 0 |

4. Relative Weight: **CWS** | 25 | **PRS** | 00 | **MTE** | 25 | **ETE** | 50 | **PRE** | 00 |

5. Credits: | 0 | 4 | 6. Semester **Spring**

7. Pre-requisite: **NIL**

8. Subject Area: **DCC**

9. Objective: To introduce to the students the fundamental discrete structures used in computer science.

10. Details of the Course:

10. Details of the Course:

Sl. No.	Contents	Contact Hours
1.	**Sets:** Properties, relations, functions, finite and infinite sets, lattice.	6
2.	**Graphs:** Directed, undirected, directed acyclic, and bipartite graphs; Connected components, Eulerian graphs, Hamiltonian cycles; Some fundamental theorems, applications.	10
3.	**Logic:** Propositional and predicate logic; Syntax, semantics, resolution principle, soundness, completeness, unification, inferencing; Applications.	10
4.	**Abstract Algebra:** Groups, rings, fields, Galois field, Euler's phi function, Fermat's theorem, discrete logarithm, applications.	10
5.	**Introduction to Number Theory:** Remainder theorem, gcd, factorization theorem.	6
	Total	**42**

11. Suggested Books:

Sl. No.	Name of Books/Authors	Year of Publication
1.	Herstein, I., "Abstract Algebra", Pearson Education.	2005
2.	Harary, F., "Graph Theory", Narosa Publishing House.	2001
3.	Huth, M. and Ryan, M., "Logic in Computer Science: Modeling and Reasoning About Systems", Cambridge University Press.	2005

Basic Definitions

- **Set -** Collection of objects, usually denoted by capital letter
- **Member, element -** Object in a set, usually denoted by lower case letter
- **Set Membership -** $a \in A$ denotes that a is an element of set A
- **Cardinality** of a set - Number of elements in a set, denoted $|S|$

Special Sets

- N - set of natural numbers = {1,2,3,4, …}
- P or Z+ - set of positive integers = {1,2,3,4, …}
- Z - set of all integers, positive, negative and zero
- R - set of all real numbers
- Ø or {} - empty set
- U - Universal set, set containing all elements under consideration

Set Builder Notation

Format:

“such that”

{[element structure] | [necessary properties to be members]}

Examples:

- $Q = \{m/n \mid m,n \in Z, n \neq 0\}$
  - Q is set of all rational numbers
  - Elements have structure m/n; must satisfy properties after the | to be set members.
- $\{x \in R \mid x^2 = 1\}$
  - {-1,1}

Subsets

- $S \subseteq T$ (S is a subset of T)
  - Every element of S is in T
  - $\forall x(x \in S \rightarrow x \in T)$
- $S = T$ (S equals T)
  - Exactly same elements in S and T
  - $(S \subseteq T) \wedge (T \subseteq S)$ ***Important for proofs!***
- $S \subset T$ (S is a proper subset of T
  - S is a subset of T but $S \neq T$
  - $(S \subseteq T) \wedge (S \neq T)$

Interval Notation - Special notation for subset of R

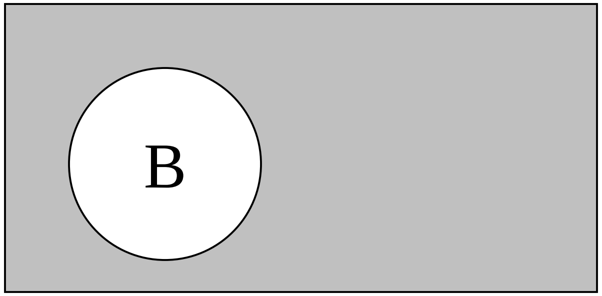
- $[a,b] = \{x \in R \mid a \leq x \leq b\}$
- $(a,b) = \{x \in R \mid a < x < b\}$
- $[a,b) = \{x \in R \mid a \leq x < b\}$
- $(a,b] = \{x \in R \mid a < x \leq b\}$

How many elements in [0,1]?

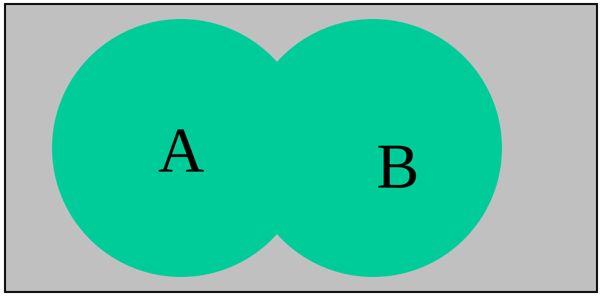
In (0,1)?

In {0,1}

Set Operations



- $\overline{B}$ (B complement)
  - $\{x \mid x \in U \wedge x \notin B\}$
  - Everything in the Universal set that is not in B
- $A \cup B$ (A union B)
  - $\{x \mid x \in A \vee x \in B\}$
  - Like inclusive or, can be in A or B or both



More Set Operations

- $A \cap B$ (A intersect B)
  - $\{x \mid x \in A \wedge x \in B\}$
  - A and B are disjoint if $A \cap B = \emptyset$
- $A - B$ (A minus B or difference)
  - $\{x \mid x \in A \wedge x \notin B\}$
  - $A - B = A \cap \overline{B}$
- $A \oplus B$ (symmetric difference)
  - $\{x \mid x \in A \oplus x \in B\} = (A \cup B) - (A \cap B)$
  - We have overloaded the symbol $\oplus$. Used in logic to mean exclusive or and in sets to mean symmetric difference

Simple Examples

Let $A = \{n^2 \mid n \in P \wedge n \leq 4\} = \{1,4,9,16\}$

Let $B = \{n^4 \mid n \in P \wedge n \leq 4\} = \{1,16,81,256\}$

- $A \cup B = \{1,4,9,16,81,256\}$
- $A \cap B = \{1,16\}$
- $A - B = \{4,9\}$
- $B - A = \{81, 256\}$
- $A \oplus B = \{4,9,81,256\}$

Approaches to Proofs

- Membership tables (similar to truth tables)
- Convert to a problem in propositional logic, prove, then convert back
- Use set identities for a tabular proof (similar to what we did for the propositional logic examples but using set identities)
- Do a logical (sentence-type) argument (similar to what we did for the number theory examples)

Prove $(A \cap B) \cup (\overline{A} \cap B) = B$

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

Prove $(A \cap B) \cup (\overline{A} \cap B) = B$

$(A \cap B) \cup (\overline{A} \cap B)$

$= \{x \mid x \in (A \cap B) \cup (\overline{A \cap B})\}$ Set builder notation

$= \{x \mid x \in (A \cap B) \vee x \in \overline{(A \cap B)}\}$ Def of $\cup$

$= \{x \mid (x \in A \wedge x \in B) \vee (x \notin A \wedge x \in B)\}$ Def of $\cap$ x2 and Def of complement

$= \{x \mid (x \in B \wedge x \in A) \vee (x \in B \wedge x \notin A)\}$ Commutative x2

$= \{x \mid (x \in B \wedge (x \in A \vee x \notin A)\}$ Distributive

$= \{x \mid (x \in B \wedge T\}$ Or tautology

$= \{x \mid (x \in B\}$ Identity

$= B$ Set Builder notation

Set Identities (Rosen, p. 89)

$A \cup \emptyset = A$
$A \cap U = A$
Identity Laws

$A \cup U = U$
$A \cap \emptyset = \emptyset$
Domination Laws

$A \cup A = A$
$A \cap A = A$
Idempotent Laws

$\overline{(\overline{A})} = A$
Complementation Law

Set Identities (cont.)

$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative Laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative Laws
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive Laws
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgan's Laws

Prove $(A \cap B) \cup (\overline{A} \cap B) = B$

$(A \cap B) \cup (\overline{A} \cap B) =$	
$(B \cap A) \cup (B \cap \overline{A})$	Commutative Law x2
$= B \cap (A \cup \overline{A})$	Distributive Law
$= B \cap U$	Definition of U
$= B$	Identity Law

Prove $(A \cap B) \cup (\overline{A} \cap B) = B$

Proof: We must show that $(A \cap B) \cup (\overline{A} \cap B) \subseteq B$ and that $B \subseteq (A \cap B) \cup (\overline{A} \cap B)$.

First we will show that $(A \cap B) \cup (\overline{A} \cap B) \subseteq B$.

Let e be an arbitrary element of $(A \cap B) \cup (\overline{A} \cap B)$. Then either $e \in (A \cap B)$ or $e \in (\overline{A} \cap B)$. If $e \in (A \cap B)$, then $e \in B$ and $e \in A$. If $e \in (\overline{A} \cap B)$, then $e \in B$ and $e \in \overline{A}$. In either case $e \in B$.

Prove $(A \cap B) \cup (\overline{A} \cap B) = B$

Now we will show that $B \subseteq (A \cap B) \cup (\overline{A} \cap B)$.

Let e be an arbitrary element of B. Then either $e \in A \cap B$ or $e \in \overline{A} \cap B$. Since e is in one or the other, then $e \in (A \cap B) \cup (A \cap B)$.

Prove: $[A \cup B \subseteq A \cap B] \rightarrow [A = B]$

Proof: We must show that when $A \cup B \subseteq A \cap B$ is true then $A=B$ is true. (Proof by contradiction) Assume that $A \cup B \subseteq A \cap B$ is true but $A \neq B$. If $A \neq B$ then this means that either $\exists\ x \in A$ but $x \notin B$, or $\exists\ x \in B$ but $x \notin A$. If $\exists\ x \in A$ but $x \notin B$, then $x \in A \cup B$ but $x \notin A \cap B$ so $A \cup B$ is not a subset of $A \cap B$ and we have a contradiction to our original assumption. By a similar argument $A \cup B$ is not a subset of $A \cap B$ if $\exists\ x \in B$ but $x \notin A$.

Therefore $[A \cup B \subseteq A \cap B] \rightarrow [A = B]$.

Prove or Disprove

$[A \cap B = A \cap C] \rightarrow [B = C]$

False! $A = \emptyset$, $B = \{a\}$, $C = \{b\}$

$[A \cup B = A \cup C] \rightarrow [B = C]$

False! $A = \{a\}$, $B = \emptyset$, $C = \{a\}$

Ordered n-tuple

The ordered n-tuple $(a_1, a_2, \ldots a_n)$ is the ordered collection that has a_1 as its first element, a_2 as its second element . . . And a_n as its nth element.

2-tuples are called ordered pairs.

Cartesian Product of A and B

Let A and B be sets. The Cartesian product of A and B, denoted A x B is the set of all ordered pairs (a,b) where a $\in$A and b $\in$ B. Hence

A x B = $\{(a,b) \mid a \in A \wedge b \in B\}$

The Cartesian product of the sets A1,A2, .. , An denoted by A1 x A2 x … x An is the set of ordered n-tuples (a1,a2,..,an) where ai belongs to Ai for I = 1,2,... ,n.

A1 x A2 x…x An = $\{(a1,a2,..,an) \mid ai \in Ai$ for I=1,2…,n$\}$

Prove $(A \oplus B) \oplus B = A$

A	B	$A \oplus B$	$(A \oplus B) \oplus B$
1	1	0	1
1	0	1	1
0	1	1	0
0	0	0	0

Prove $(A \oplus B) \oplus B = A$

Proof: We must show that $(A \oplus B) \oplus B \subseteq A$ and that $A \subseteq (A \oplus B) \oplus B$.

First we will show that $(A \oplus B) \oplus B \subseteq A$. Let $e \in (A \oplus B) \oplus B$. Then $e \in (A \oplus B)$ or $e \in B$ but not both. If $e \in (A \oplus B)$, then either $e \in A$ or $e \in B$. If $e \in A$ and $e \notin B$ then we are done. If $e \in B$, and $e \notin A$, then $e \in (A \oplus B)$ but can not be an element of $(A \oplus B) \oplus B$ by definition so this case can not exist.

Proof of $(A \oplus B) \oplus B = A$, cont.

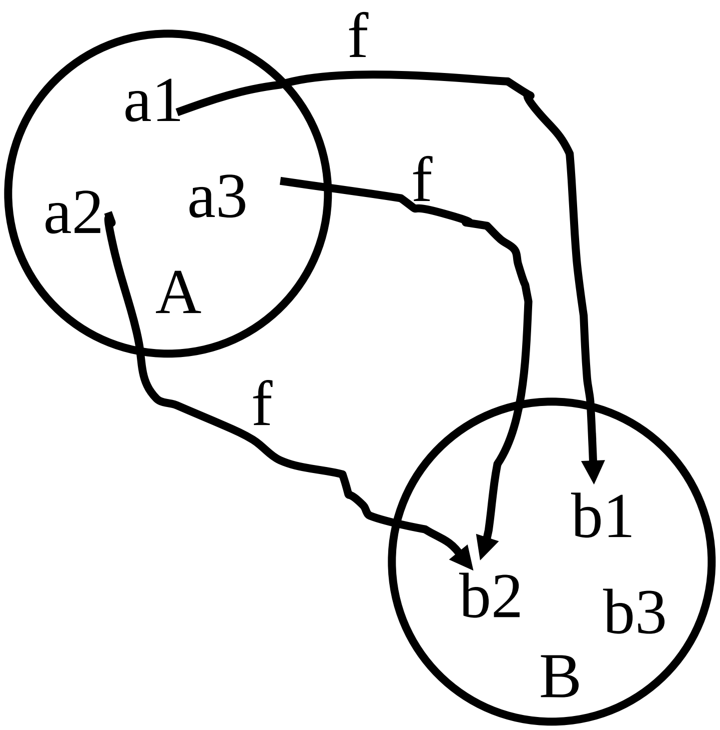
Now we will show that $A \subseteq (A \oplus B) \oplus B$. Let $e \in A$. Either e is also $\in B$ or $e \notin B$. If $e \in B$, then $e \notin (A \oplus B)$ so e is an element of $(A \oplus B) \oplus B$. If $e \notin B$, e is an element of $(A \oplus B)$ and e must be an element of $(A \oplus B) \oplus B$.

Thus $(A \oplus B) \oplus B = A$.

Definition of Function

Let A and B be sets.

- A **function f** from A to B is an assignment of exactly one element of B to each element of A.
- We write **f**(a) = b if b is the only element of B assigned by the function, **f**, to the element of A.
- If **f** is a function from A to B, we write **f**:A → B.



Addition and Multiplication

Let f1 and f2 be functions from A to **R** (real numbers).Then

- f1+f2 is defined as (f1+f2) (x) = f1(x) + f2(x).
- f1f2 is defined as (f1f2)(x) = f1(x)f2(x).

And both of these are also from A to **R**.

(Two real valued functions with the same domain can be added and multiplied.)

- **Example:** $f1(x) = x^2$; $f2 = x+x^2$
- $(f1+f2)(a) = a^2 + a + a^2 = 2a^2 + a$
- $f1f2(a) = (a^2)(a+a^2) = a^3+a^4$

Are f1+f2 and f1f2 Commutative?

Prove: (f1+f2)(x) = (f2+f1)x where $x \in R$

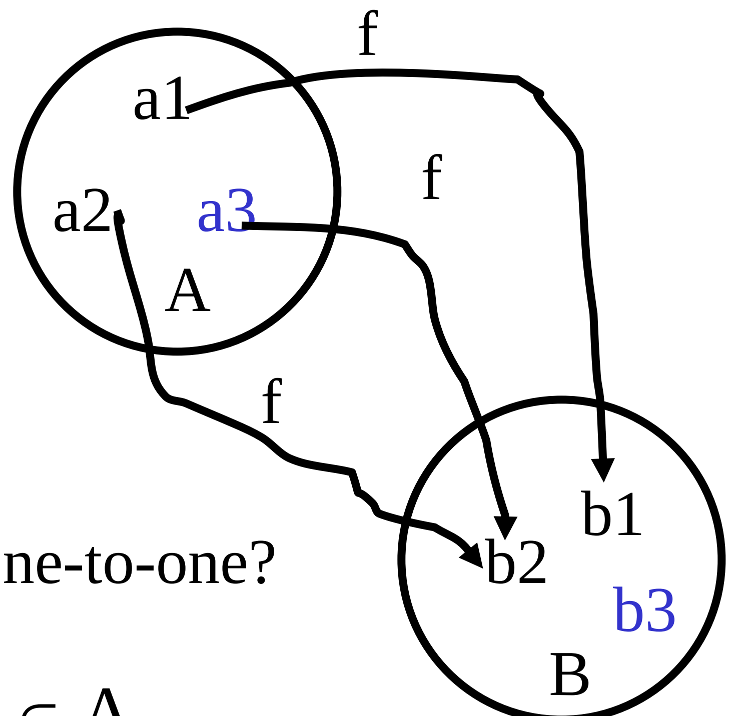
Proof: Let $x \in R$ be an arbitrary element in the domain of f1 and f2. Then (f1+f2)(x) = f1(x) + f2(x) = f2(x) + f1(x) = (f2+f1)(x).

Prove: (f1f2)(x) = (f2f1)(x) where $x \in R$

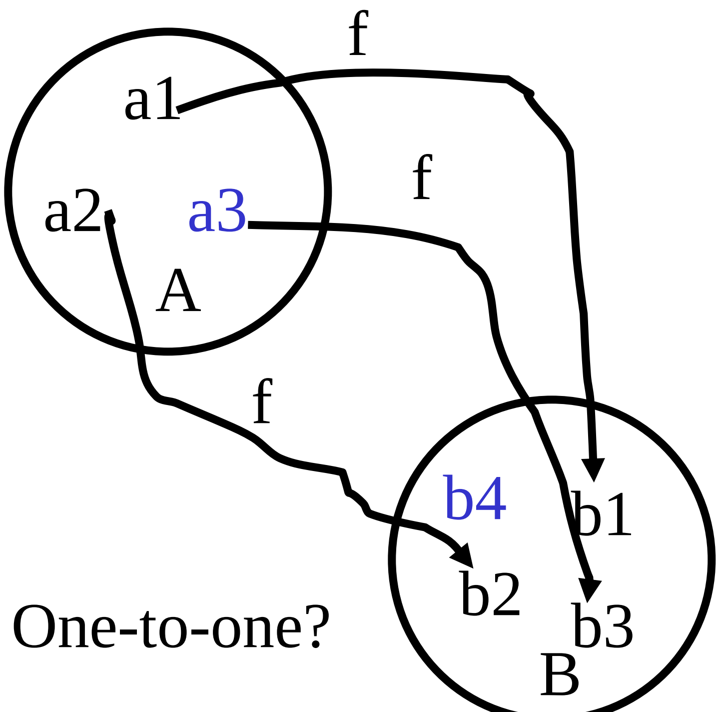
Proof: Let $x \in R$ be an arbitrary element in the domain of f1 and f2. Then (f1f2)(x) = f1(x)f2(x) = f2(x)f1(x) = (f2f1)(x).

One-to-one function

A function f is said to be **one-to-one, or injective**, if and only if f(x) = f(y) implies that x=y for all x and y in the domain of f.



One-to-one?



One-to-one?

$\forall a0, a1 \in A$

$[f(a0) = f(a1)] \rightarrow [a0 = a1]$

OR

$[a0 \neq a1] \rightarrow [f(a0) \neq f(a1)]$

		Conditional	Converse	Inverse	Contrapositive
p	q	$p \to q$	$q \to p$	$\sim p \to \sim q$	$\sim q \to \sim p$
T	T	T	T	T	T
T	F	F	T	T	F
F	T	T	F	F	T
F	F	T	T	T	T

Equivalent

Let $f:Z\rightarrow Z$, where $f(x) = 2x$

Prove that f is one-to-one

Proof: We must show that $\forall\ x_0, x_1 \in Z\ [f(x_0) = f(x_1) \rightarrow x_0 = x_1]$.

Consider arbitrary x0 and x1 that satisfy $f(x_0) = f(x_1)$. By the function's definition we know that $2x_0 = 2x_1$. Dividing both sides by 2, we get $x_0 = x_1$. Therefore f is one-to-one.

Let $g: Z \to Z$, where $g(x) = x^2 - x - 2$

Is g one-to-one?

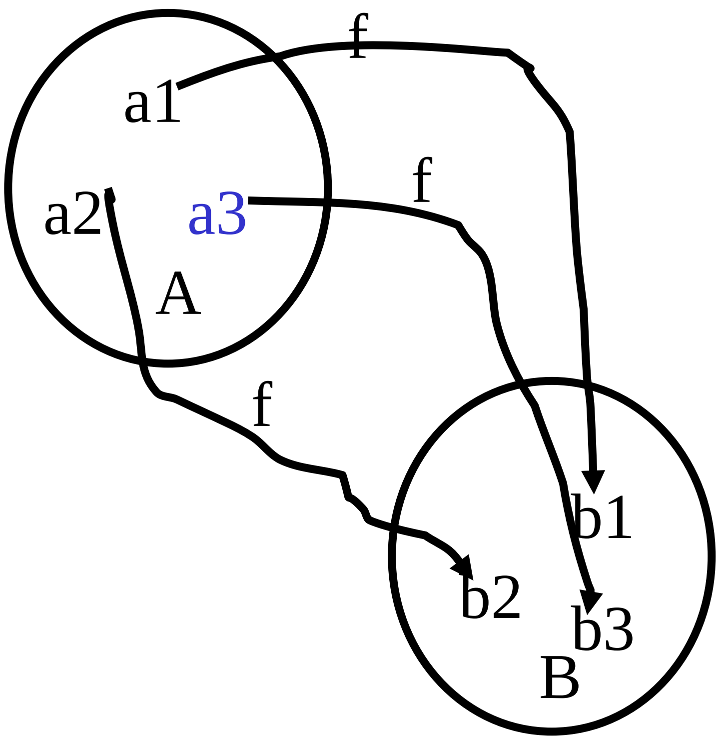
No! To prove a function is not one-to-one it is enough to give a counter example such that $f(x_1) = f(x_2)$ and $x_1 \neq x_2$.

Counter Example: Consider $x_1 = 2$ and $x_2 = -1$.

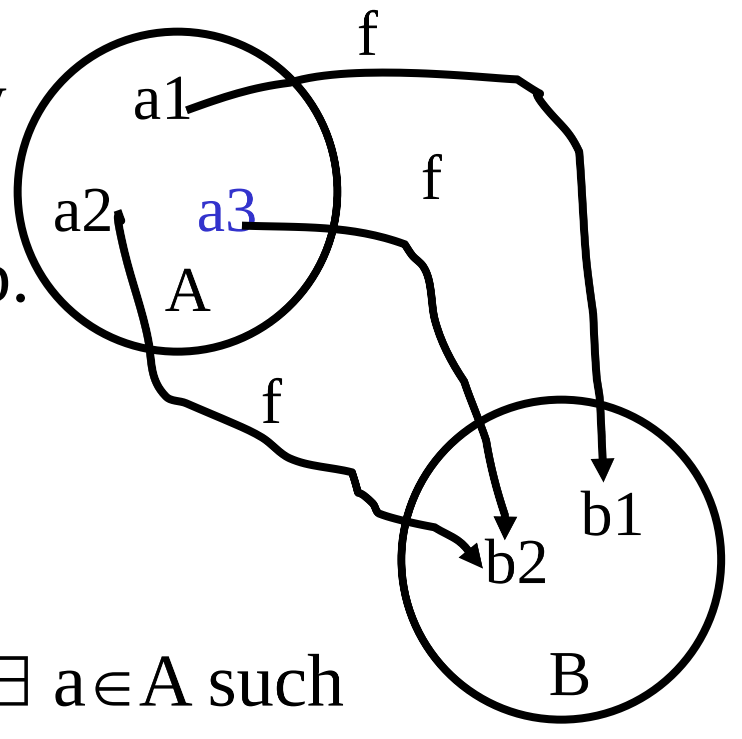
Then $g(2) = 2^2 - 2 - 2 = 0 = g(-1) = (-1)^2 + 1 - 2$. Since $g(2) = g(-1)$ and $2 \neq -1$, g is not one-to-one.

Onto Function

A function f from A to B is called **onto, or surjective**, if and only if for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$.



$\forall b \in B\ \exists\ a \in A$ such that $f(a) = b$



Let $f: R \to R$, where $f(x) = x^2+1$

Prove or disprove: f is onto

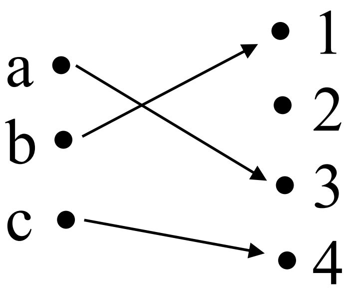
Counter Example: Let f = 0, then there does not exist an x such that $f(x) = x^2 + 1$ since x^2 is always positive.

Let g:R→R, where g(x) = 3x-5

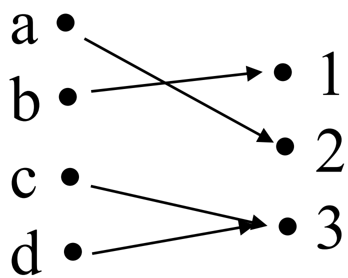
Prove: g(x) is onto.

Proof: Let y be an arbitrary real number (in g). For g to be onto, there must be an $x \in R$ such that $y = 3x-5$. Solving for x, $x = (y+5)/3$ which is a real number. Since x exists, then g is onto.

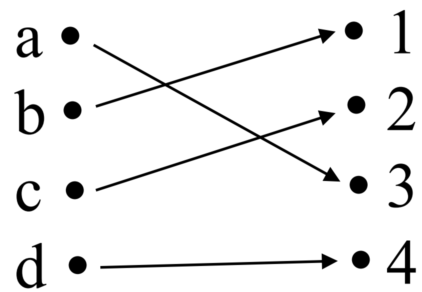
Correspondence Diagrams: One-to-One or Onto?



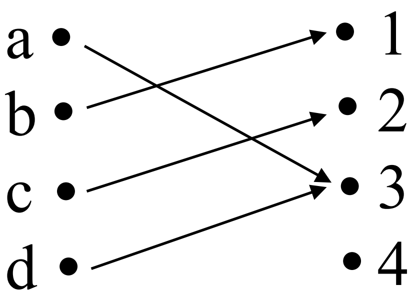
One-to-one, not onto



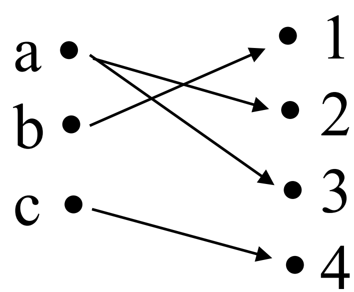
Onto, not one-to-one



One-to-one, and onto



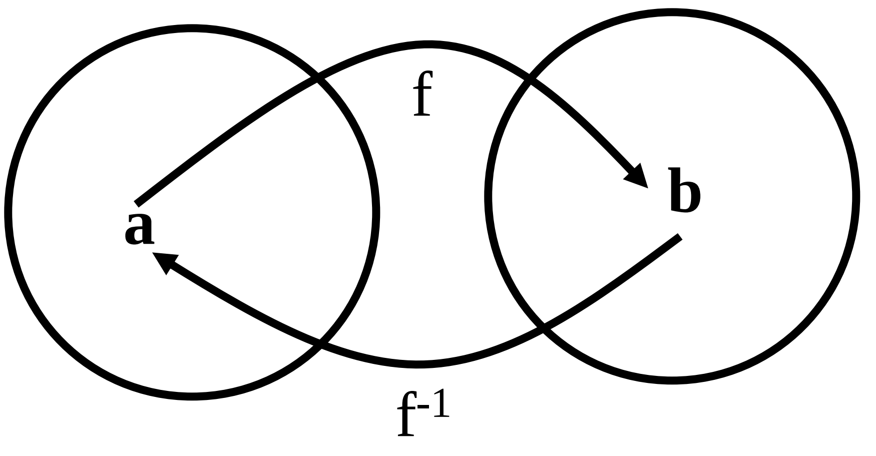
Neither one-to-one nor onto



Not a function!

Inverse Function, f^{-1}

Let f be a ***<u>one-to-one correspondence</u>*** from the set A to the set B. The inverse function of f is the function that assigns to an element b belonging to B the unique element a in A such that if $f(a) = b$, then $f^{-1}(b) = a$.



Example:

$f(a) = 3(a-1)$

$f^{-1}(b) = (b/3)+1$

Let f be an invertible function from A to B. Let S be a subset of B. Show that $f^{-1}(\overline{S}) = \overline{f^{-1}(S)}$

Proof: We must show that $f^{-1}(\overline{S}) \subseteq \overline{f^{-1}(S)}$ and that $\overline{f^{-1}(S)} \subseteq f^{-1}(\overline{S})$.

Let $x \in f^{-1}(\overline{S})$. Then $x \in A$ and $f(x) \in \overline{S}$. Since $f(x) \notin S$, $x \notin f^{-1}(S)$. Therefore $x \in \overline{f^{-1}(S)}$.

Now let $x \in \overline{f^{-1}(S)}$. Then $x \notin f^{-1}(S)$ which implies that $f(x) \notin S$. Therefore $f(x) \in \overline{S}$ and $x \in f^{-1}(\overline{S})$

Let f be an invertible function from A to B. Let S be a subset of B. Show that $f^{-1}(\overline{S}) = \overline{f^{-1}(S)}$

Proof:

$f^{-1}(\overline{S}) = \{x \in A \mid f(x) \notin S\}$ Set builder notation

$= \{x \in A \mid \overline{f(x) \in S\}}$ Def of Complement

$= \overline{f^{-1}(S)}$ Def of Complement

Sequence

- A sequence is a discrete structure used to represent an <u>ordered</u> list.
- A sequence is a function from a subset of the set of integers (usually either the set {0,1,2,. . .} or {1,2, 3,. . .}to a set S.
- We use the notation a_n to denote the image of the integer n. We call a_n a term of the sequence.
- Notation to represent sequence is $\{a_n\}$

Examples

- $\{1, 1/2, 1/3, 1/4, \ldots\}$ or the sequence $\{a_n\}$ where $a_n = 1/n$, $n \in Z^+$.

- $\{1,2,4,8,16, \ldots\} = \{a_n\}$ where $a_n = 2^n$, $n \in N$.

- $\{1^2,2^2,3^2,4^2,\ldots\} = \{a_n\}$ where $a_n = n^2$, $n \in Z^+$

Summations

- Notation for describing the sum of the terms $a_m, a_{m+1}, \ldots, a_n$ from the sequence, $\{a_n\}$

$$a_m + a_{m+1} + \ldots + a_n = \sum_{j=m}^{n} a_j$$

- j is the index of summation (dummy variable)
- The index of summation runs through all integers from its lower limit, m, to its upper limit, n.

Summations follow all the rules of multiplication and addition!

$$c\sum_{j=1}^{n} j = \sum_{j=1}^{n} cj = \text{c(1+2+…+n) = c + 2c +…+ nc}$$

$$r\sum_{j=0}^{n} ar^{j} = \sum_{j=0}^{n} ar^{j+1} = \sum_{k=1}^{n+1} ar^{k} =$$

$$ar^{n+1} + \sum_{k=1}^{n} ar^{k} = ar^{n+1} - a + \sum_{k=0}^{n} ar^{k}$$

Telescoping Sums

$$\sum_{j=1}^{n}(a_j - a_{j-1}) = (a_1 - a_0) + (a_2 - a_1) +$$

$$(a_3 - a_2) + \ldots + (a_n - a_{n-1}) = a_n - a_0$$

Example

$$\sum_{k=1}^{4}[k^2 - (k-1)^2] =$$

$$(1^2 - 0^2) + (2^2 - 1^2) + (3^2 - 2^2) + (4^2 - 3^2)$$

$$4^2 = 16 - 0 = 16$$

Closed Form Solutions

A simple formula that can be used to calculate a sum without doing all the additions.

Example:

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Proof: First we note that $k^2 - (k-1)^2 = k^2 - (k^2-2k+1) = 2k-1$. Since $k^2-(k-1)^2 = 2k-1$, then we can sum each side from k=1 to k=n

$$\sum_{k=1}^{n} [k^2 - (k-1)^2] = \sum_{k=1}^{n} (2k-1)$$

Proof (cont.)

$$\sum_{k=1}^{n}[k^2-(k-1)^2]=\sum_{k=1}^{n}(2k-1)$$

$$\sum_{k=1}^{n}[k^2-(k-1)^2]=\sum_{k=1}^{n}2k+\sum_{k=1}^{n}(-1)$$

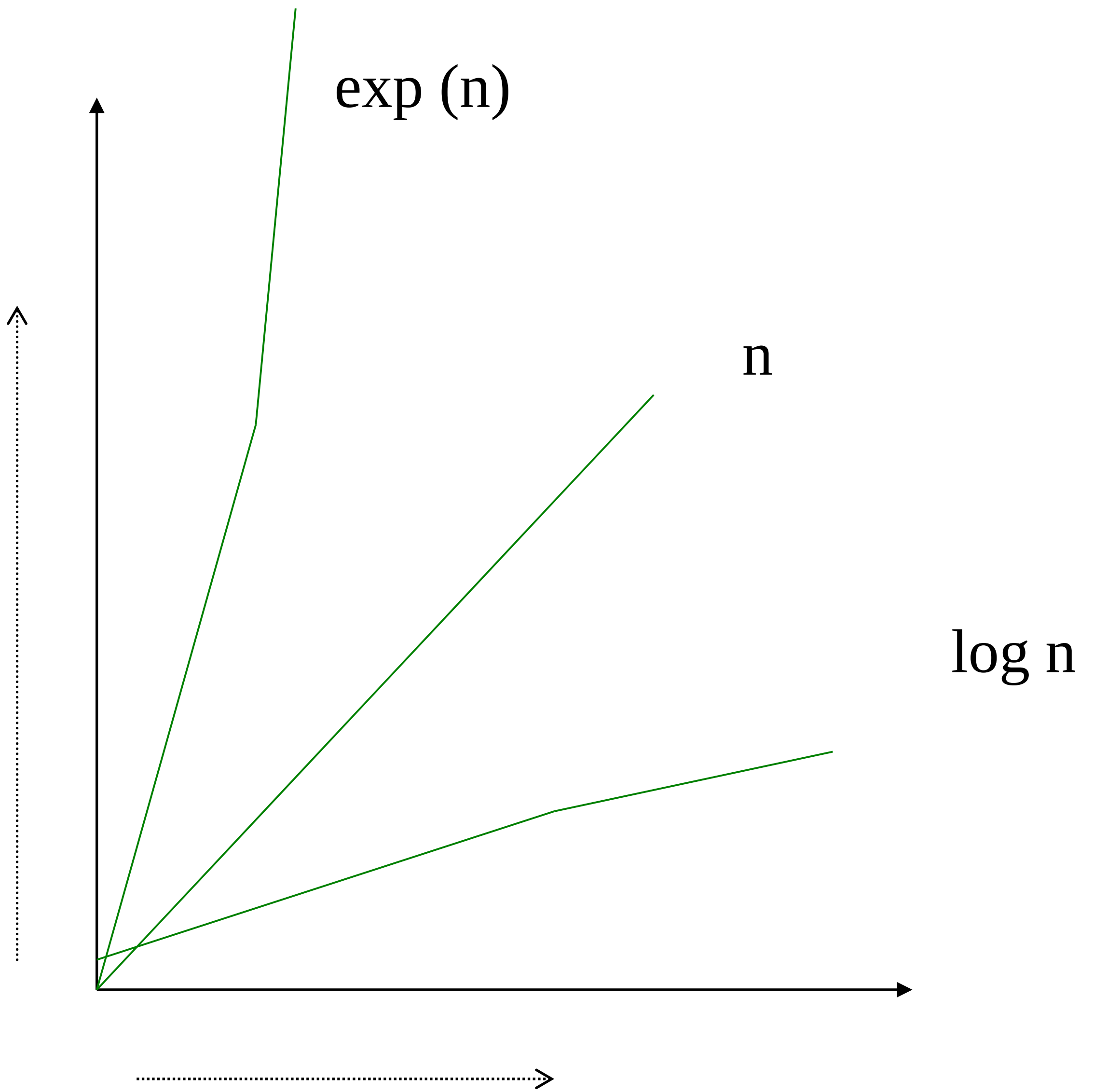
$$n^2-0^2=2\sum_{k=1}^{n}(k)+-n$$

$$n^2+n=2\sum_{k=1}^{n}(k)$$

$$\sum_{k=1}^{n}k=\frac{n^2+n}{2}$$

Big-O Notation

- Let f and g be functions from the set of integers or the set of real numbers to the set of real numbers. We say that f(x) is ***O***(g(x)) if there are constants $C \in \mathbf{R}$ and $k \in \mathbf{R}$ such that $|f(x)| \leq C|g(x)|$ whenever $x > k$.
- We say "f(x) is big-oh of g(x)".
- The intuitive meaning is that as x gets large, the values of f(x) are no larger than a constant time the values of g(x), or f(x) is growing no faster than g(x).
- The supposition is that x gets large, it will approach a simplified limit.


exp (n)
n
log n

Show that $3x^3+2x^2+7x+9$ is $\boldsymbol{O}(x^3)$

Proof: We must show that $\exists$ constants $C \in \mathbf{R}$ and $k \in \mathbf{R}$ such that $|3x^3+2x^2+7x+9| \leq C|x^3|$ whenever $x > k$.

Choose $k = 1$ then

$3x^3+2x^2+7x+9 \leq 3x^3+2x^3+7x^3+9x^3 = 21x^3$

So let $C = 21$.

Then $3x^3+2x^2+7x+9 \leq 21\, x^3$ when $x \geq 1$.

Show that n! is $\boldsymbol{O}(n^n)$

Proof: We must show that $\exists$ constants $C \in \mathbf{R}$ and $k \in \mathbf{R}$ such that $|n!| \leq C|n^n|$ whenever $n > k$.

$$n! = n(n-1)(n-2)(n-3)\ldots(3)(2)(1)$$

$$\leq n(n)(n)(n)\ldots(n)(n)(n) \qquad \textit{n times}$$

$$= n^n$$

So choose $k = 0$ and $C = 1$

General Rules

- Multiplication by a constant does not change the rate of growth. If $f(n) = kg(n)$ where k is a constant, then f is ***O***(g) and g is ***O***(f).
- The above means that there are an infinite number of pairs C, k that satisfy the Big-O definition.
- Addition of smaller terms does not change the rate of growth. If $f(n) = g(n)$ + smaller order terms, then f is ***O***(g) and g is ***O***(f).

Ex.: $f(n) = 4n^6 + 3n^5 + 100n^2 + 2$ is $O(n^6)$.

General Rules (cont.)

- If $f_1(x)$ is $O(g_1(x))$ and $f_2(x)$ is $O(g_2(x))$, then $f_1(x)f_2(x)$ is $O(g_1(x)g_2(x))$.
- Examples:

$10x\log_2 x$ is $O(x\log_2 x)$

$n!6n^3$ is $O(n!n^3)$

$=O(n^{n+3})$

Example: Big-Oh Not Symmetric

- Order matters in big-oh. Sometimes f is $\boldsymbol{O}$(g) and g is $\boldsymbol{O}$(f), but in general big-oh is not symmetric.

Consider $f(n) = 4n$ and $g(n) = n^2$. f is $\boldsymbol{O}$(g).

- Can we prove that g is $\boldsymbol{O}$(f)? Formally, $\exists$ constants $C \in \mathbf{R}$ and $k \in \mathbf{R}$ such that $|n^2| \leq C|4n|$ whenever $n > k$?
- No. To show this, we must prove that negation is true for all C and k. $\forall C \in \mathbf{R}$, $\forall k \in \mathbf{R}$, $\exists n > k$ such that $n^2 > C|4n|$.

$\forall C \in \mathbf{R}, \forall k \in \mathbf{R}, \exists n > k$ such that $n^2 > 4nC$.

- To prove that negation is true, start with arbitrary C and k. Must show/construct an $n>k$ such that $n^2 > 4nC$
- Easy to satisfy $n > k$, then
- To satisfy $n^2>4nC$, divide both sides by n to get $n>4C$. Pick $n = \max(4C+1,k+1)$, which proves the negation.

- If $\lim_{n \to \propto} f(n)/g(n)$ exists and is finite, then $f(n)$ is $O(g(n))$

Example Functions

sqrt(n) , n, 2n, ln n, exp(n), n + sqrt(n) , n + n^2

$\lim_{n \to \propto}$ sqrt(n) /n = 0, sqrt(n) is O(n)

$\lim_{n \to \propto}$ n/sqrt(n) = infinity, n is not O(sqrt(n))

$\lim_{n \to \propto}$ n /2n = 1/2, n is O(2n)

$\lim_{n \to \propto}$ 2n /n = 2, 2n is O(n)

$\lim_{n \to \propto} \ln(n) / n = 0,$ $\ln(n)$ is $O(n)$

$\lim_{n \to \propto} n / \ln(n) = \text{infinity},$ n is not $O(\ln(n))$

$\lim_{n \to \propto} \exp(n) / n = \text{infinity},$ $\exp(n)$ is not $O(n)$

$\lim_{n \to \propto} n / \exp(n) = 0,$ n is $O(\exp(n))$

$\lim_{n \to \propto} (n + \mathrm{sqrt}(n)) / n = 1,$ $n + \mathrm{sqrt}(n)$ is $O(n)$

$\lim_{n \to \propto} n / (\mathrm{sqrt}(n) + n) = 1,$ n is $O(n + \mathrm{sqrt}(n))$

$\lim_{n \to \propto} (n + n^2) / n = \text{infinity},$ $n + n^2$ is not $O(n)$

$\lim_{n \to \propto} n / (n + n^2) = 0,$ n is $O(n + n^2)$

Steps in an Induction Proof

1. Basis step : The proposition is shown to be true for n=1 (or, more generally, the first element in the set)
2. Inductive step: The implication $P(n) \rightarrow P(n+1)$ is shown to be true for every positive integer n.

For $n \in Z^+$

$[P(1) \wedge \forall n(P(n) \rightarrow P(n+1))] \rightarrow \forall n P(n)$

Example 1: If $p(n)$ is the proposition that the sum of the first n positive integers is $n(n+1)/2$, prove $p(n)$ for $n \in Z^+$.

Basis Step: We will show p(1) is true.

$p(1) = 1(1+1)/2 = 2/2 = 1$

Inductive Step:

We want to show that $p(n) \to p(n+1)$

Assume $1+2+3+4+. . . + n = n(n+1)/2$

Then $1+2+3+4+. . . + n + (n+1) = n(n+1)/2 + n+1 = n(n+1)/2 + (n+1)(2/2) =$

$[n(n+1) + 2(n+1)]/2 = [n^2 + 3n +2]/2 = [(n+1)(n+2)]/2$

Since p(1) is true and $p(n) \to p(n+1)$, then p(n) is true for all positive integers n.

Example 2: If p(n) is the proposition that the sum of the first n odd integers is n^2, prove p(n) for $n \in Z^+$

Induction Proof

Basis Step: We will show that p(1) is true.

$1 = 1^2$

Inductive Step

We want to show that $p(n) \to p(n+1)$

Assume $1 + 3 + 5 + 7 + \ldots + (2n-1) = n^2$

Then $1 + 3 + 5 + 7 + \ldots + (2n-1) + (2n + 1) = n^2 + 2n + 1 = (n+1)^2$

Since p(1) is true and $p(n) \to p(n+1)$, then p(n) is true for all positive integers n.

Example 3: If p(n) is the proposition that $\sum_{j=0}^{n} 2^j = 2^{n+1} - 1$ prove p(n) when n is a non-negative integer.

Inductive Proof

Basis Step: We will show p(0) is true.

$2^0 = 1 = 2-1 = 2^{0+1} - 1$

Inductive step: We want to show that $p(n) \rightarrow p(n+1)$

Assume $2^0 + 2^1 + 2^2 + 2^3 + \ldots + 2^n = 2^{n+1} - 1$, then

$2^0 + 2^1 + 2^2 + 2^3 + \ldots + 2^n + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1}$

$= 2(2^{n+1}) - 1 = 2^{n+2} - 1$

Since p(0) is true and $p(n) \rightarrow p(n+1)$, then p(n) is true for all nonnegative integers n.

Example 4: Prove that $\sum_{j=n}^{2n-1}(2j+1) = 3n^2$

whenever n is a positive integer.

Proof:

Basis Case: Let n = 1, then

$$\sum_{j=1}^{2(1)-1}(2j+1) = \sum_{j=1}^{1}\left(2j+1\right) = 3 = 3\left(1\right)^2 = 3$$

Prove that $\sum_{j=n}^{2n-1}(2j+1) = 3n^2$ whenever n is a positive integer.

<u>Inductive Case:</u>

Assume that the expression is true for n, i.e., that

$$\sum_{j=n}^{2n-1}(2j+1) = 3n^2$$

Then we must show that:

$$\sum_{j=n+1}^{2(n+1)-1}(2j+1) = 3(n+1)^2$$

$$\sum_{j=n+1}^{2(n+1)-1} (2j+1) = \sum_{j=n+1}^{2n+1} (2j+1)$$

$$= \sum_{j=n}^{2n-1} (2j+1) - (2n+1) + \left(2(2n)+1\right) + \left(2(2n+1)+1\right)$$

$$= 3n^2 - (2n+1) + (2(2n)+1) + (2(2n+1)+1)$$

$$= 3n^2 - 2n - 1 + 4n + 1 + 4n + 3$$

$$= 3n^2 + 6n + 3 = 3(n^2 + 2n + 1)$$

$$= 3(n+1)^2$$