SACRAMENTO STATE

CSc 28
Discrete Structures

Chapter 3
Set Theory

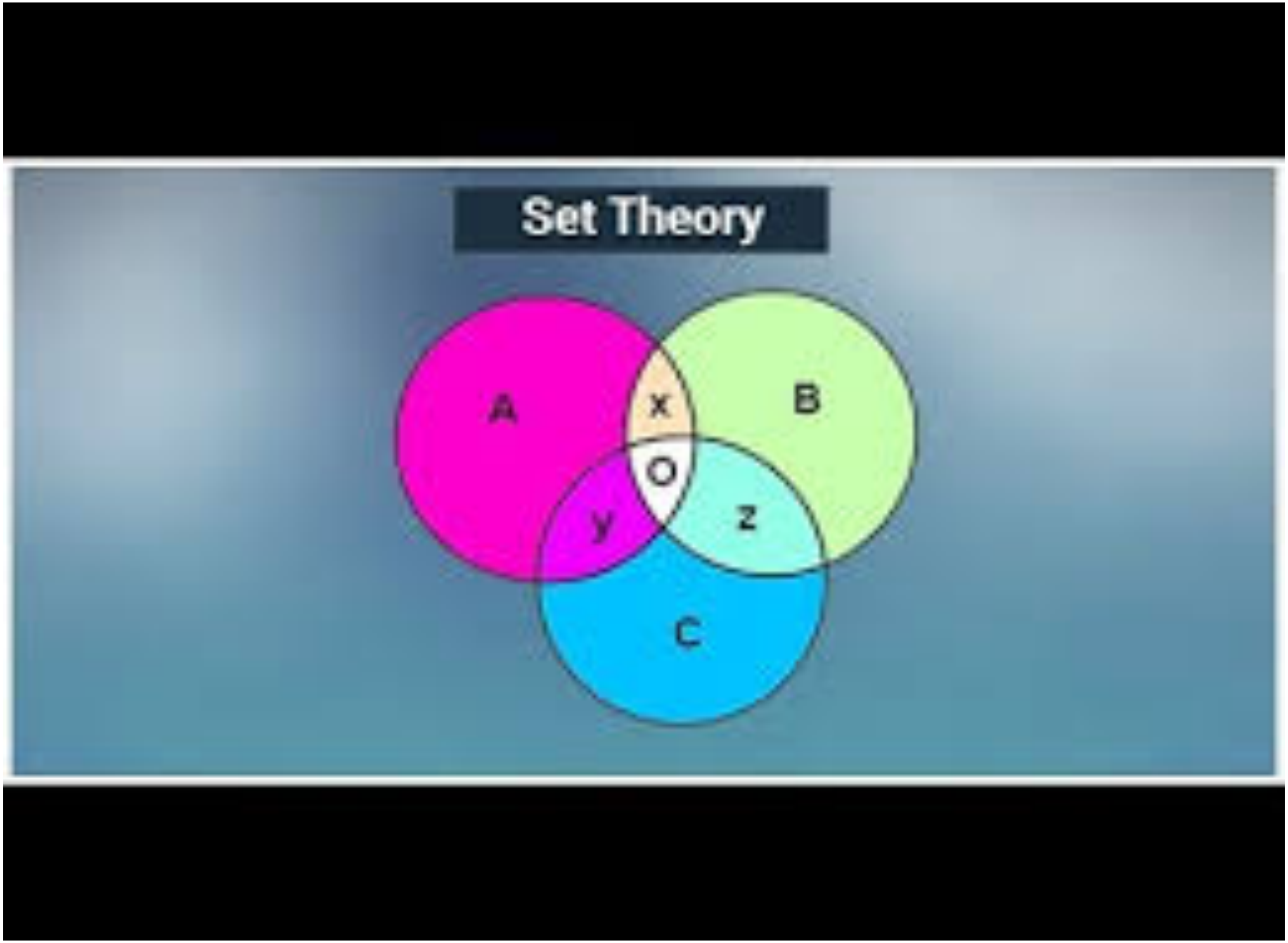
Herbert G. Mayer, CSU CSc

Status 2/1/2021

Syllabus

- Set Theory
- Examples of Sets
- Subsets
- Power Set
- Cartesian Product
- Set Operations
- Functions
- References

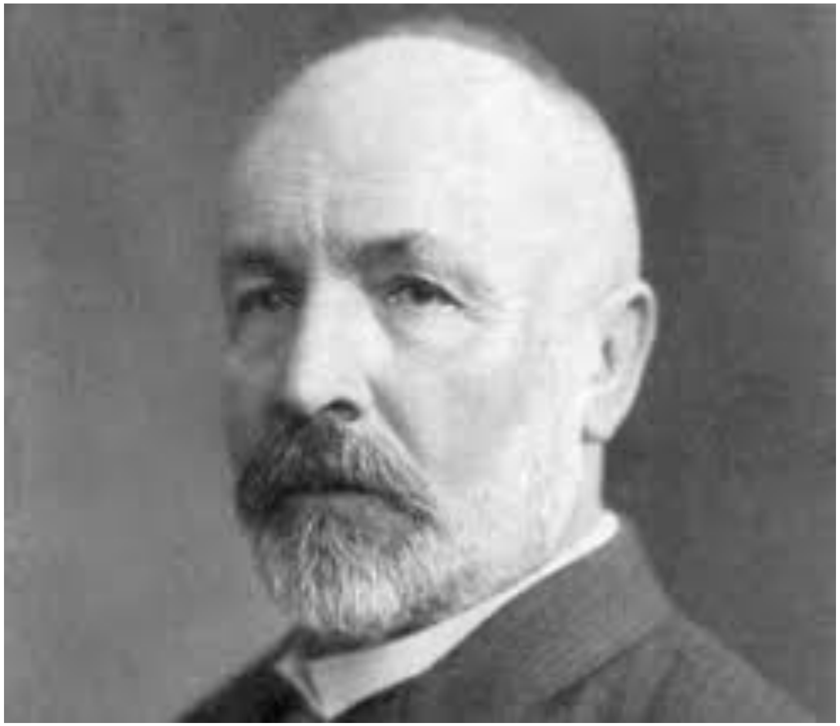
Set Theory



Set Theory

- Set theory: Branch of mathematical logic that studies sets
- Informally: Set is a collection of distinct objects
- Almost any type of object can be collected into a set, including sets
- Set theory is frequently applied to objects relevant to mathematics
- Modern set theory pioneered by Georg Cantor and Richard Dedekind
- After discovery of paradoxes in set theory, such as Russell's Paradox, numerous axiom systems were proposed early twentieth century; common: ZFC
- ZFC for Zermelo-Fraenkel with Axiom of Choice

Set Theory



Georg Cantor 1845 - 1918

Richard Dedekind 1831 - 1916

Set Theory

- Set theory is commonly employed as a foundational system for mathematics, particularly in the form of Zermelo–Fraenkel set theory [2] with the axiom of choice; see [5]
- Contemporary research into set theory includes structure of the real number line, up to consistency of Large Cardinals, a special Math branch, not detailed here; see [4]
- Set theory founded via a single paper in 1874 by Georg Cantor: "On a Property of the Collection of All Real Algebraic Numbers”
- A bit more formally: . . .

Set Theory

Axiom of Choice

- Formulated 1904 by Ernst Zermelo et al.
- To formalize proof of the Well-Ordering Theorem
- Detail see again [5]
- Axiom of choice, or AC, is an axiom of set theory that a Cartesian product of a collection of non-empty sets is non-empty
- I.e. a choice can be made, even if the set is infinite!
- See example:

Set Theory

Axiom of Choice, Cont'd

- Easy example: Sets picked from natural numbers
- From such sets, one may always select "largest" or "smallest" element
- E.g. in { { 4, 5, 6 }, { 13, 10 }, { 44, 1, 617, 80000 } } the set of smallest elements is: { 4, 10, 1 }
- In this case, "select the smallest number" is a Choice Function
- Even if infinitely many sets were collected from natural numbers, it is always possible to choose the smallest unique element from each set

Set Theory

Axiom of Choice, Cont’d

- **That is, the choice function provides the set of chosen elements**
- **However, no choice function is known for the collection of all non-empty subsets of the real numbers**
- **. . . as there are so called non-constructible reals**
- **In that case the Choice Function has to be invoked**
- **Not discussed here**

Set Theory

Ernst Zermelo

1871 - 1953

Set Theory

Non-constructible numbers:

- Origin of constructible numbers inextricably linked with the history of the three impossible compass and straightedge constructions:
  - Duplicating the cube
  - Trisecting an angle
  - Squaring the circle
- The restriction of using only compass and straightedge in geometric constructions is often credited to philosopher Plato
- See: https://en.wikipedia.org/wiki/Constructible_number

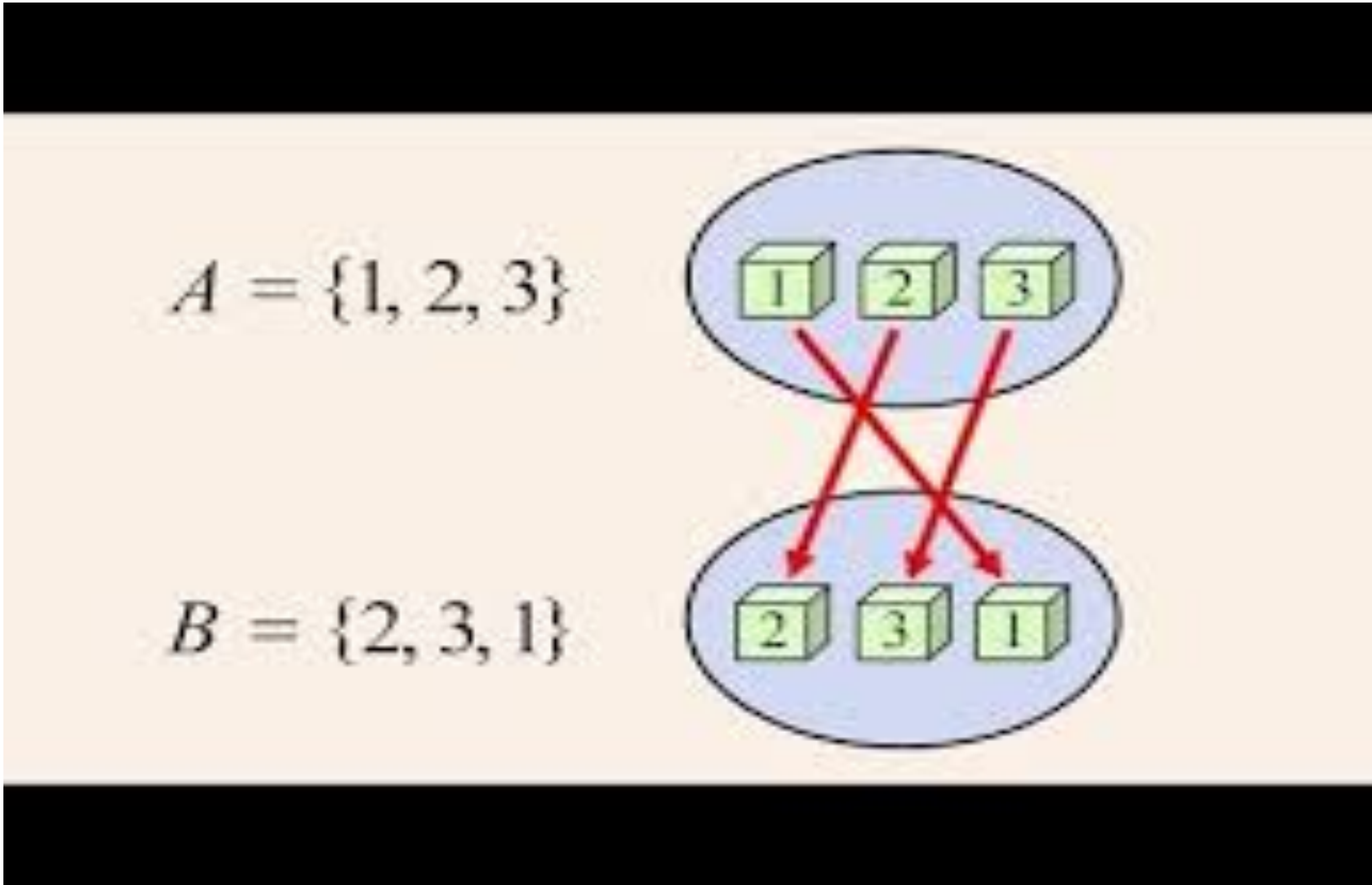
Set Theory

- Set: Collection of objects, these are called elements
- $a \in A$ "a is an element of set A"
  "a is a member of set A"
- $a \notin A$ "a is not an element of A"
- $A = \{ a_1, a_2, \ldots, a_n \}$ "A contains $a_1, \ldots, a_n$"
- Order of elements is insignificant
- It does not matter how often the same element is listed, i.e. repetition doesn't count, thus does not contribute to, or change the set
- Conventional (and efficient) to list each distinct member just once

Set Definition

- **Set Theory** is a branch of mathematical logic that studies sets
- Set is a well-defined **collection of distinct elements**
- Elements of sets are AKA **members**
- Elements can be anything clearly identifiable: such as people, letters of the alphabet, numbers, points in space, etc. and even sets
- It is common for sets to have a name
- Two sets are equal if they contain exactly the same elements
- A set that has no elements is called an empty set

Set Equality



Set Equality

Sets A and B are equal if and only if they contain exactly the same elements

Examples:

- **A = { 9, 2, 7, -3 },**
- **B = { 7, 9, -3, 2 } :** A = B
- **C = { dog, cat, horse },**
- **D = { cat, horse, squirrel, dog } :** C ≠ D
- **E = { dog, cat, horse },**
- **F = { cat, dog, horse, dog } :** E = F

Examples of Sets

Examples of Mathematical Sets

"Standard" Sets, AKA classes of numbers:

- Natural Numbers N = { 0, 1, 2, 3, … }
- Integer Numbers Z = { …, -2, -1, 0, 1, 2, … }
- Positive Integers Z^+ = { 1, 2, 3, 4, … }
- Real Numbers R = { 47.3, -12, π, … }
- Rational Numbers Q = { 1.5, 2.6, -3.8, 15, … }
- Irrational Numbers I = e.g. π, or square root of 2: $\sqrt{2}$

Real numbers: Combination of Rational and Irrationals

Rational number: Can be written as ratio of 2 integers; can locate them as points on the "number line"

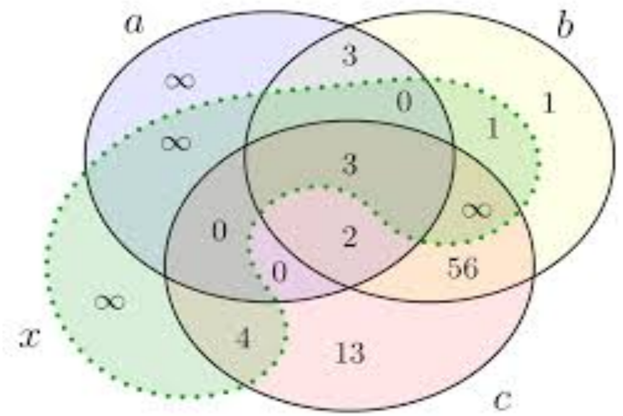
Irrational number: Cannot be expressed as the ratio of 2 integer numbers

Examples of Sets

- **A = ∅** **empty set** **AKA** **null set**, **is a set!**
- **A = { z }** **Note: z ∈ A, but z ≠ { z }**
- **A = { { b,c }, { c,x,d } }** **set of sets**
- **A = { { x, y } }** **Note: { x, y } ∈ A**
- **A = { x | P(x) }** **Set of all x such that P(x) is true**
  P(x) is the ***membership function*** of set **A**
  $\forall x \; (P(x) \rightarrow x \in A)$
- **B = { x | x ∈ N ∧ x > 7 } = { 8, 9, 10, … }**
  "set builder notation"
  Is set B finite or infinite?

Examples of Sets

- **We are now able to define the set of rational numbers Q constructed from integers:**
- **$Q = \{ a / b \mid a \in Z \wedge b \in Z^+ \}$, or**
- **$Q = \{ a / b \mid a \in Z \wedge b \in Z \wedge b \neq 0 \}$**



- **But *how about* the set of Real Numbers R?**
- **R = { r | r is a real number }**

That is the best we can do. The set of **R** can hardly be defined by enumeration, nor by some **builder** function

Subsets

$A \subseteq B$ A is a subset of B

$A \subseteq B$ if and only if every element of A is also an element of B

We can completely formalize this:

$A \subseteq B \Leftrightarrow \forall x\ (x \in A \rightarrow x \in B)$ –note the A, B order!

Examples:

$A = \{3, 9\}$, $B = \{5, 9, 1, 3\}$ $A \subseteq B$? true

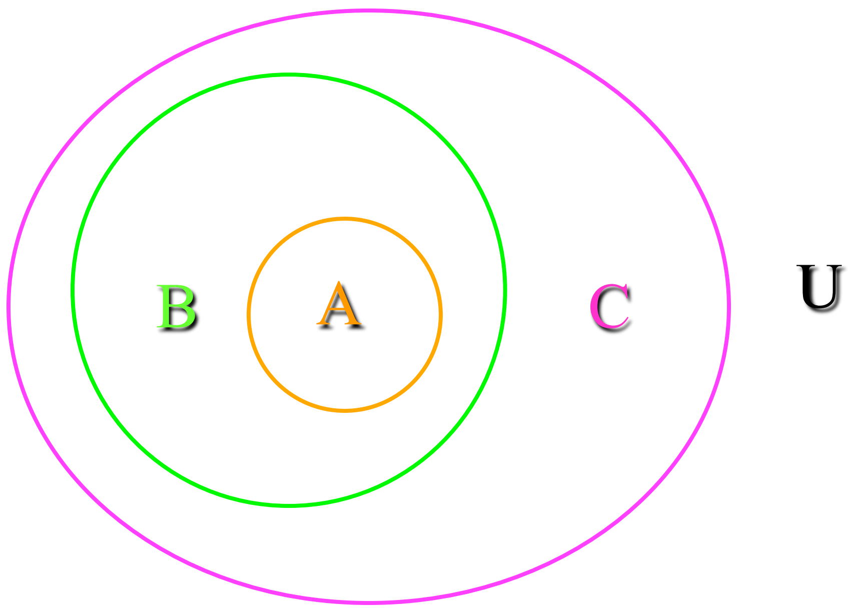
$A = \{3, 3, 3, 9\}$, $B = \{5, 9, 1, 3\}$ $A \subseteq B$? true

$A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$ $A \subseteq B$? false

Subsets

Useful rules:

- $\mathbf{A = B \Leftrightarrow (A \subseteq B) \land (B \subseteq A)}$
- $\mathbf{(A \subseteq B) \land (B \subseteq C) \Rightarrow A \subseteq C}$ (see below **Venn Diagram**)



Subsets

Useful rules:

$\emptyset \subseteq A$ for any set A

$A \subseteq A$ for any set A

Proper subsets:

$A \subset B$ A is a **proper subset** of B

$A \subset B \Leftrightarrow \forall x\, (x \in A \rightarrow x \in B) \wedge \exists x\, (x \in B \wedge x \notin A)$

or

$A \subset B \Leftrightarrow \forall x\, (x \in A \rightarrow x \in B) \wedge \neg \forall x\, (x \in B \rightarrow x \in A)$

Cardinality of Sets

If a set S contains n distinct elements, with n ∈ N, we call S a finite set with cardinality n

Examples below:

A = { Mercedes, BMW, Porsche } **|A| = 3**

B = { { 1 }, { 2, 3 }, { 4, 5 }, { 6 } } **|B| = 4**

C = ∅ **|C| = 0**

D = { x ∈ N | x ≤ 7000 } **|D| = 7001**

E = { x ∈ N | x ≥ 7000 } **|E| = ∞** AKA: infinite

Power Set Review

P(A) define P, the Power Set of set A, as follows:

$P(A) = \{ B \mid B \subseteq A \}$ all possible subsets of set A

Examples:

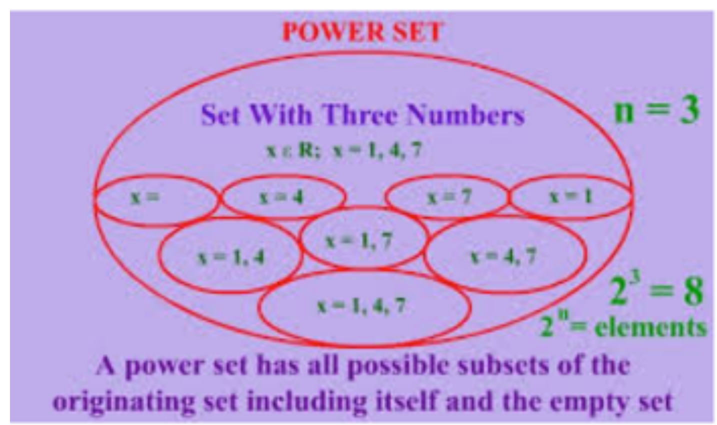
$A = \{ x, y, z \}$ then the Power Set P of A, AKA P(A) is:

$P(A) = \{ \varnothing, \{ x \}, \{ y \}, \{ z \}, \{ x,y \}, \{ x,z \}, \{ y,z \}, \{ x,y,z \} \}$

If: $A = \varnothing$

Then: $P(A) = \{ \varnothing \}$

Note: $|A| = 0$, $|P(A)| = 1$



Power Set Review

Cardinality of power sets: $|P(A)| = 2^{|A|}$

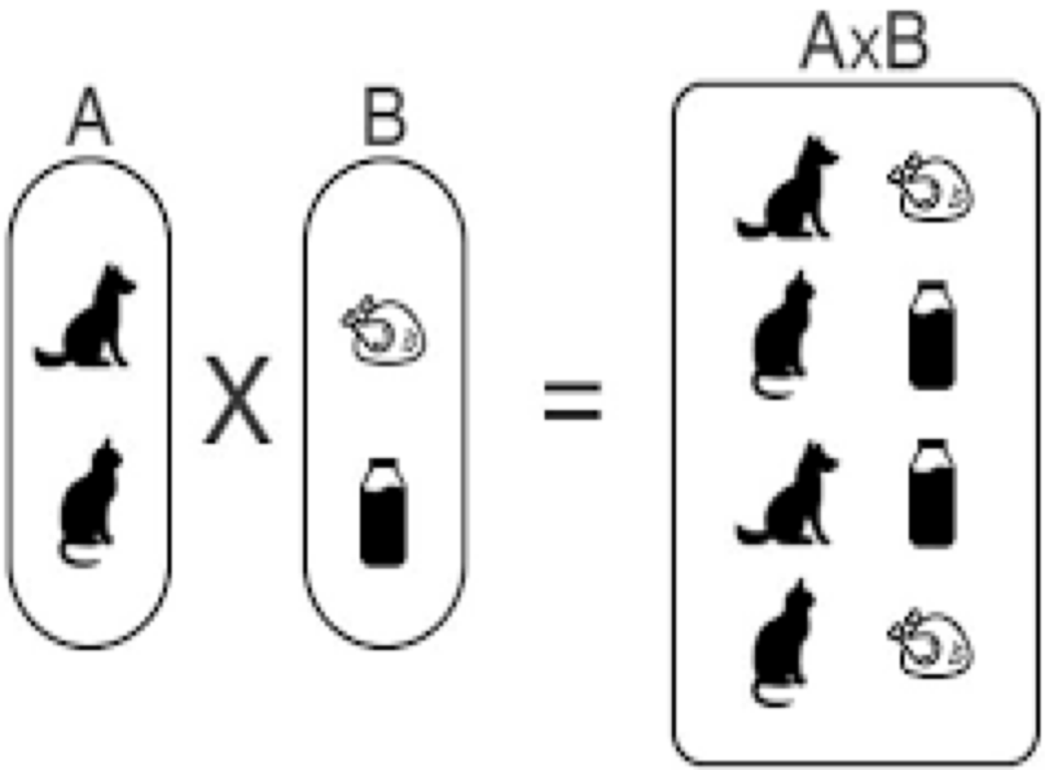
- Imagine each element in A has an "on/off" switch
- Each possible switch configuration in A corresponds to one subset of A, thus to one element in P(A)

A	1	2	3	4	5	6	7	8
X:	x	x	x	x	x	x	x	x
Y:	y	y	y	y	y	y	y	y
Z:	z	z	z	z	z	z	z	z

- With 3 elements X, Y, Z in set A, then there must be $2 \times 2 \times 2 = 2^3 = 8$ elements in the power set P(A)

Cartesian Product of Sets

Cartesian Product



Cartesian Product of Two Sets.

Cartesian Product

- The ordered n-tuple $(a_1, a_2, a_3, \ldots, a_n)$: a systematically arranged collection of n objects into one element
- Careful tuples are not sets, never mind the multiple elements!
- Two ordered n-tuples $(a_1, a_2, a_3, \ldots, a_n)$ and then also $(b_1, b_2, b_3, \ldots, b_n)$ are equal if and only if they contain exactly the same elements and in the same order, i.e. $a_i = b_i$ for $1 \leq i \leq n$
- Cartesian product of two sets $A \times B$ is defined as:
- $A \times B = \{ (a, b) \mid a \in A \land b \in B \}$

Cartesian Product

Example:

A = { good, bad }, B = { student, prof }

A×B = { (good, student), (good, prof), (bad, student), (bad, prof) **}**

B×A = { (student, good), (prof, good), (student, bad), (prof, bad) **}**

Example: A = { x, y }, B = { a, b, c }

A×B = { (x, a), (x, b), (x, c), (y, a), (y, b), (y, c) } Set of tuples

Cartesian Product

- $A \times \emptyset = \emptyset$
- $\emptyset \times A = \emptyset$
- For non-empty sets A and B: $A \neq B \Leftrightarrow A \times B \neq B \times A$
- $|A \times B| = |A| \cdot |B|$ – for any number of sets!
- The Cartesian product of n sets X_i ($i = 1 \,.\,.\, n$) is defined as the ***n*-ary Cartesian Product** C_n over these n sets $X_1, \ldots, X_n$ as:

$$C_n = X_1 \times X_2 \times X_3 \ldots \times X_n$$

Set Operations

Set Operations

- **Union**: $A \cup B = \{ x \mid x \in A \vee x \in B \}$
- Example: $A = \{ a, b \}$, $B = \{ b, c, d \}$

  $A \cup B = \{ a, b, c, d \}$

- **Intersection**: $A \cap B = \{ x \mid x \in A \wedge x \in B \}$
- Example: $A = \{ a, b \}$, $B = \{ b, c, d \}$

  $A \cap B = \{ b \}$

- **Cardinality**: $|A \cup B| = |A| + |B| - |A \cap B| = 4$

Set Operations

- **Two sets are called disjoint if their intersection is empty, that is, they share no elements:**

$$A \cap B = \varnothing$$

- **Difference between two sets A and B contains exactly those elements of A that are not in B:**

$$A\text{-}B = \{\ x \mid x \in A \wedge x \notin B\ \}$$

- **Example: $A = \{ a, b \}$, $B = \{ b, c, d \}$, $A - B = \{ a \}$**
- **Cardinality: $|A\text{-}B| = |A| - |A \cap B|$**

Set Operations

- **The complement of a set A contains exactly those elements under consideration that are not in A**
- **Complement denoted as: A^c**
- **Or $\overline{A}$ in some text books; also shown as $\neg A$**

$$A^c = U - A$$

- **Example: U = N, B = { 250, 251, 252, … ∞ }**
  B^c = { 0, 1, 2, …, 248, 249 } = U - B

Logical Equivalence

Equivalence Law Refresh:

- **Identity law** $P \wedge T \equiv P$
- **Domination law** $P \wedge F \equiv F$
- **Idempotent law** $P \wedge P \equiv P$
- **Double negation law** $\neg(\neg P) \equiv P$
- **Commutative law** $P \wedge Q \equiv Q \wedge P$
- **Associative law** $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$
- **Distributive law** $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
- **De Morgan's law** $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$
- **Implication law** $P \rightarrow Q \equiv \neg P \vee Q$

Set Identity

Key equations

• **Identity law**	$A \cup \varnothing$	$= A, \quad A \cap U = A$
• **Domination law**	$A \cup U$	$= U, \quad A \cap \varnothing = \varnothing$
• **Idempotent law**	$A \cup A$	$= A, \quad A \cap A = A$
• **Double Complement**	$(A^c)^c$	$= A$
• **Commutative law**	$A \cup B$	$= B \cup A, \; A \cap B = B \cap A$
• **Associative law**	$A \cup (B \cup C)$	$= (A \cup B) \cup C, \ldots$
• **Distributive law**	$A \cup (B \cap C)$	$= (A \cup B) \cap (A \cup C)$
• **De Morgan's law**	$(A \cup B)^c$	$= A^c \cap B^c,$
• **Or** De Morgan	$(A \cap B)^c$	$= A^c \cup B^c$
• **Absorption law**	$A \cup (A \cap B)$	$= A, \quad A \cap (A \cup B) = A$
• **Complement law**	$A \cup A^c$	$= U, \quad A \cap A^c = \varnothing$

Set Identity

How to prove $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$?

Method I: logical equivalent

	$x \in A \cup (B \cap C)$	Set
$\Leftrightarrow$	$x \in A \vee x \in (B \cap C)$	
$\Leftrightarrow$	$x \in A \vee (x \in B \wedge x \in C)$	
$\Leftrightarrow$	$(x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$	Logic
$\Leftrightarrow$	$x \in (A \cup B) \wedge x \in (A \cup C)$	
$\Leftrightarrow$	$x \in (A \cup B) \cap (A \cup C)$	Set again

Every logical expression can be transformed into an equivalent expression in set theory and vice versa

Set Identity

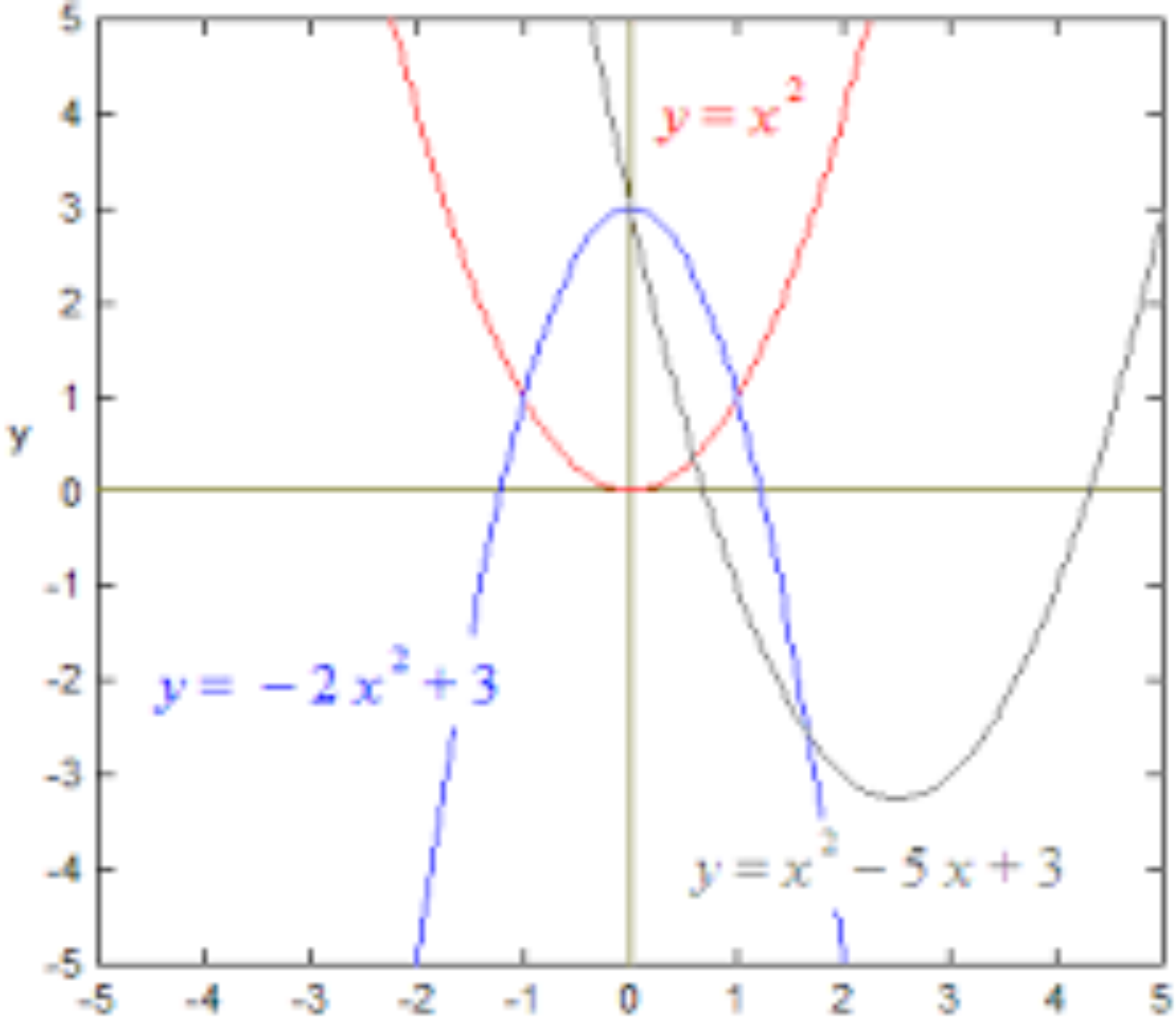
Method II: Membership table

1 means "x **is** an element of this set"
0 means "x is **not** an element of this set"

A	B	C	$B \cap C$	$A \cup (B \cap C)$	$A \cup B$	$A \cup C$	$(A \cup B) \cap (A \cup C)$
0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0
0	1	0	0	0	1	0	0
0	1	1	1	1	1	1	1
1	0	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	1	1	1	1	1	1

Functions

Geometric Functions



Sample Geometric Functions, Our Focus: Logic Functions

Functions

- A function f from set A (which includes a) to set B (which includes b) is an assignment of exactly one element of B to each element of A (e.g. value "a")
- We write: $f(a) = b$
- With b being some unique element of B assigned by function f to the element a of A
- And with f being a function from A to B; we can also write $f: A \rightarrow B$

Functions

- With notation $f: A \rightarrow B$, we say that "A is the domain of f and B is the codomain of f"
- With notation $f(a) = b$, we say that "b is the image of a, and a is the pre-image of b"
- The range of $f: A \rightarrow B$ is the set of all images of all elements of A
- We say that $f: A \rightarrow B$ maps A to B

Functions

Let us view **function f**, with $f: P \rightarrow C$:

- P = { Linda, Max, Kathy, Peter }
- C = { Boston, New York, Hong Kong, Moscow }
- f(Linda) = Moscow
- f(Max) = Boston
- f(Kathy) = Hong Kong
- f(Peter) = New York
- Here, the range of f is C

Functions

Let us re-specify f as follows:

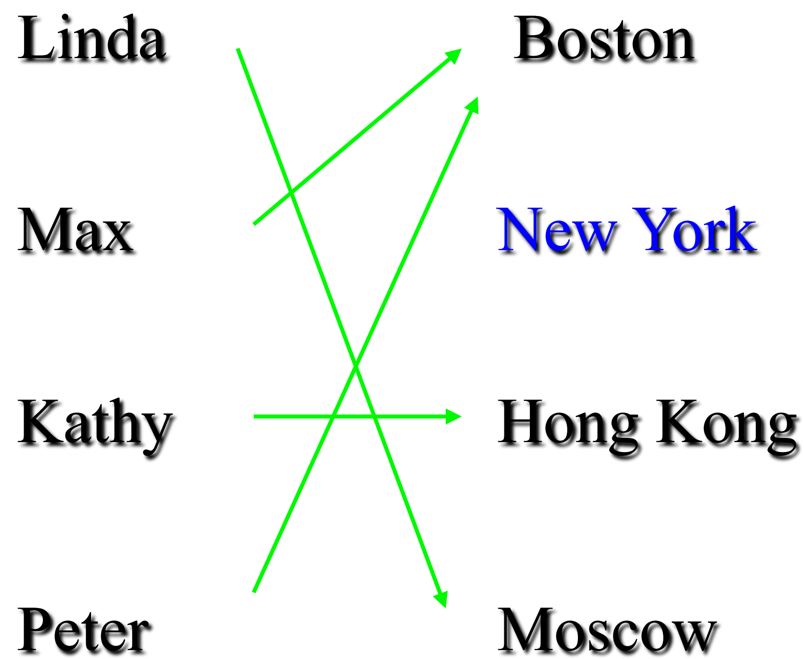
- f(Linda) = Moscow
- f(Max) = Boston
- f(Kathy) = Hong Kong
- f(Peter) = Boston
- Is f still a function? Yes!

What is its range of f? { Moscow, Boston, Hong Kong }

Functions

Other ways to represent f:

x	f(x)
Linda	Moscow
Max	Boston
Kathy	Hong Kong
Peter	Boston



Functions

If the domain of function f is large, it is convenient to specify f with a formula, e.g.:

f: R→R

f(x) = 2 x for example

This leads to:

f(1) = 2

f(3) = 6

f(-3) = -6

…

Functions

- Let f_1 and f_2 be functions from A to R
- Then the sum and the product of f_1 and f_2 are also functions from A to R defined by:
- $(f_1 + f_2)(x) = f_1(x) + f_2(x)$ – function addition
- $(f_1 f_2)(x) = f_1(x) f_2(x)$ – function product

Example:

- $f_1(x) = 3x$, $f_2(x) = x + 5$
- $(f_1 + f_2)(x) = f_1(x) + f_2(x) = 3x + x + 5 = 4x + 5$
- $(f_1 f_2)(x) = f_1(x) f_2(x) = 3x (x + 5) = 3x^2 + 15x$

Functions

- We know the **range** of a function $f: A \rightarrow B$ is the set of all images of elements $a \in A$
- If we only regard a subset $S \subseteq A$, the set of all images of elements $s \in S$ is called the image of S
- We denote the **image of S** by $f(S)$:

$$f(S) = \{ f(s) \mid s \in S \}$$

Functions

Now let's view the following functions:

- **f(Linda) = Moscow**
- **f(Max) = Boston**
- **f(Kathy) = Hong Kong**
- **f(Peter) = Boston**

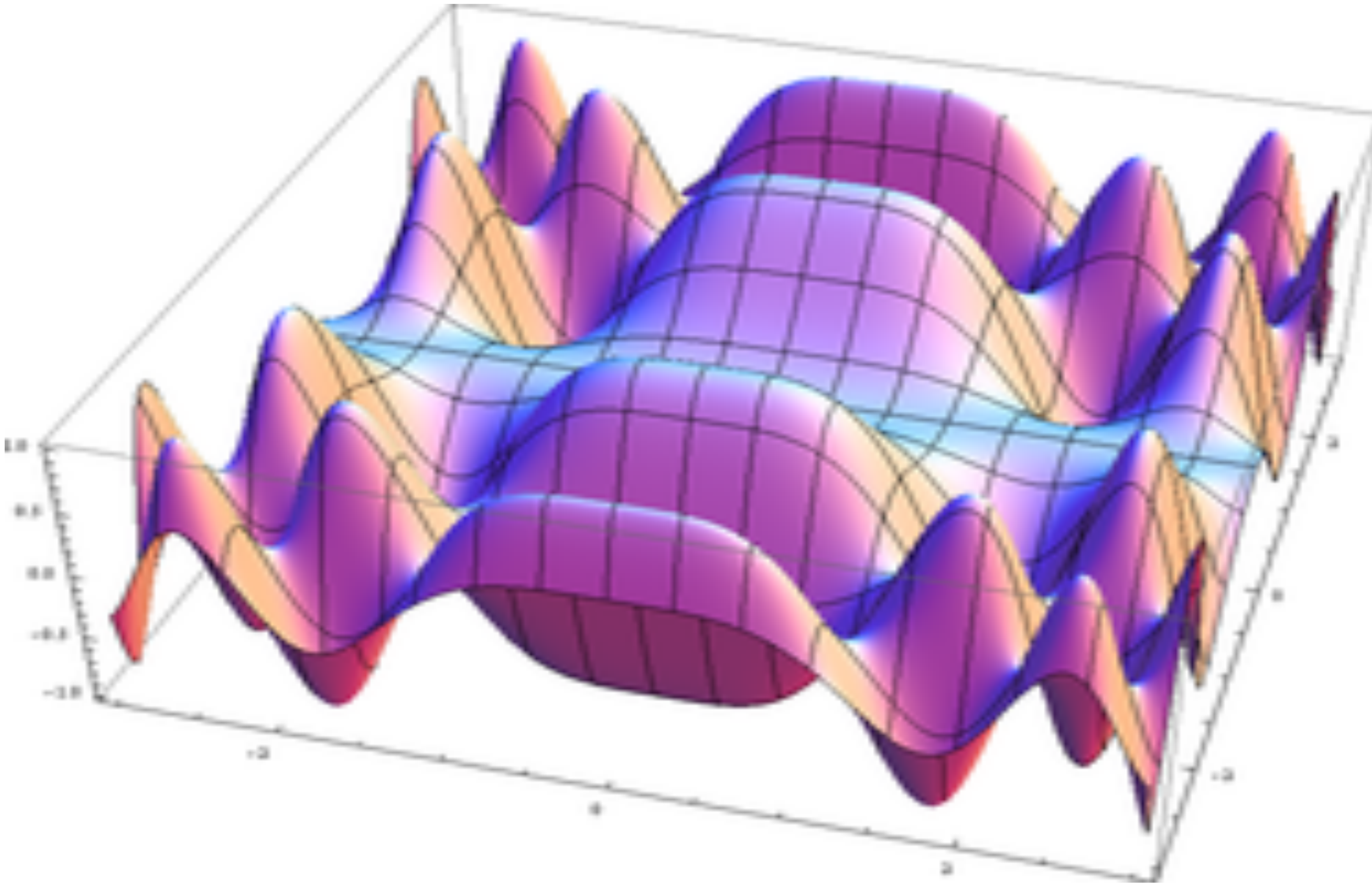
What is the image of S = { Linda, Max } ?

- **f(S) = { Moscow, Boston }**

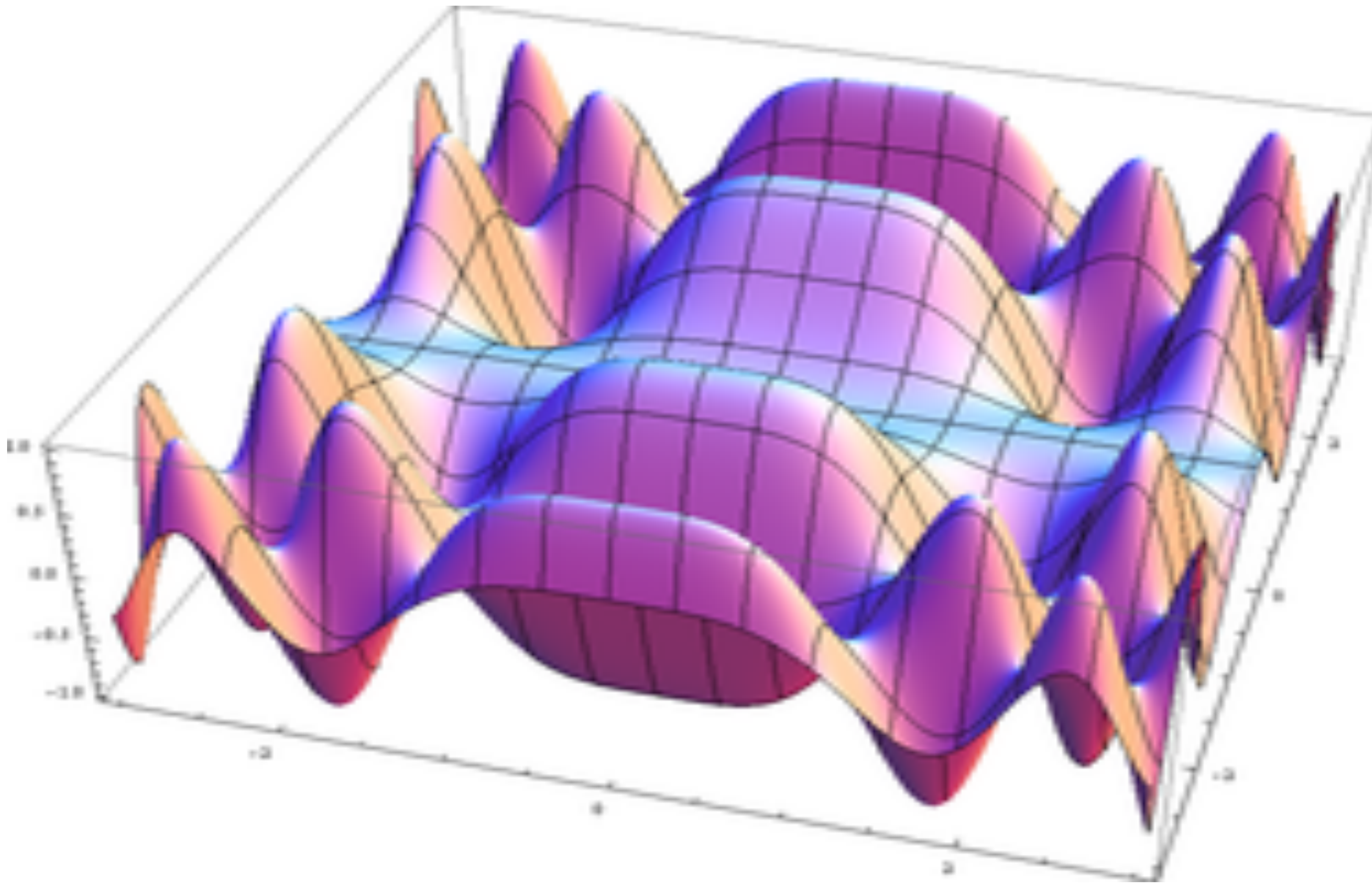
What is the image of S = { Max, Peter } ?

- **f(S) = { Boston }**

Which Function?



That Function!



$f(x, y) = \sin(x^2) * \cos(y^2)$

For Math Majors

Properties of Functions

A function $f: A \rightarrow B$ is said to be one-to-one (or injective), if and only if

$$\forall x, y \in A \; (f(x) = f(y) \rightarrow x = y)$$

In other words: f is one-to-one if and only if it does not map 2 distinct elements of A onto the same element of B

Properties of Functions

And again…

- f(Linda) = Moscow
- f(Max) = Boston
- f(Kathy) = Hong Kong
- f(Peter) = Boston

Is f one-to-one?

No, Max and Peter are mapped onto the same element of the image

- g(Linda) = Moscow
- g(Max) = Boston
- g(Kathy) = Hong Kong
- g(Peter) = New York

Is g one-to-one?

Yes, each element is assigned a unique element of the image

Properties of Functions

How can we prove that a function f is one-to-one?

To prove something, look at the relevant definition:

$$\forall x, y \in A\ (f(x) = f(y) \rightarrow x = y)$$

Example:

$$f: R \rightarrow R$$

$$f(x) = x^2$$

Disproof by counterexample:

$f(3) = f(-3)$, but $3 \neq -3$, so f is not one-to-one

Properties of Functions

Another example:

$$f: R \rightarrow R$$

$$f(x) = 3x$$

One-to-one: $\forall x, y \in A\ (f(x) = f(y) \rightarrow x = y)$

To show: $f(x) \neq f(y)$ whenever $x \neq y$ (indirect proof)

$$x \neq y$$

$$\Leftrightarrow 3x \neq 3y$$

$$\Leftrightarrow f(x) \neq f(y),$$

so if $x \neq y$, then $f(x) \neq f(y)$, that is, **f** is **one-to-one**

Properties of Functions

Function f: $A \rightarrow B$ with $A, B \subseteq R$ is **strictly increasing**, if

$$\forall x, y \in A \, (x < y \rightarrow f(x) < f(y))$$

and strictly decreasing, if

$$\forall x, y \in A \, (x < y \rightarrow f(x) > f(y))$$

Clearly, a function that is either **strictly increasing** or strictly **decreasing** is one-to-one

Properties of Functions

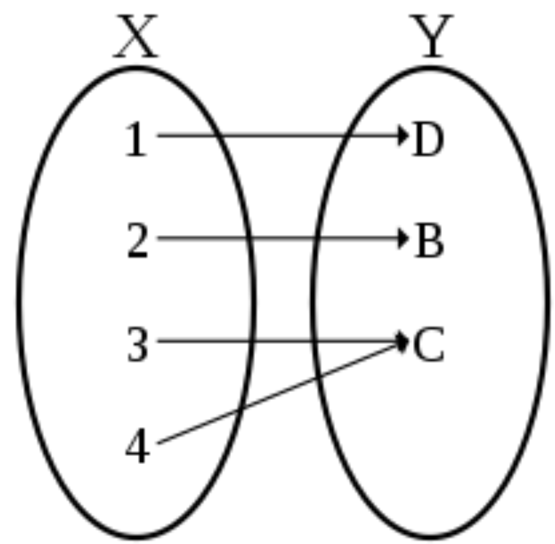
- **A function $f: A \to B$ is called onto, or surjective, if and only if for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$**
- **In other words, f is onto if and only if its range is its entire codomain**
- **A function $f: A \to B$ is a one-to-one correspondence, or a bijection, if and only if it is both one-to-one and onto**
- **Obviously, if f is a bijection and A and B are finite sets, then $|A| = |B|$**

Properties of Functions

Another definition:

In Mathematics a function f from a set X to a set Y is surjective, if for every element y in the codomain Y of f, there is at least one element x in the domain X of f such that f(x) = y.

It is not necessary that x be unique; function f may map one or more elements of X to the same element of Y



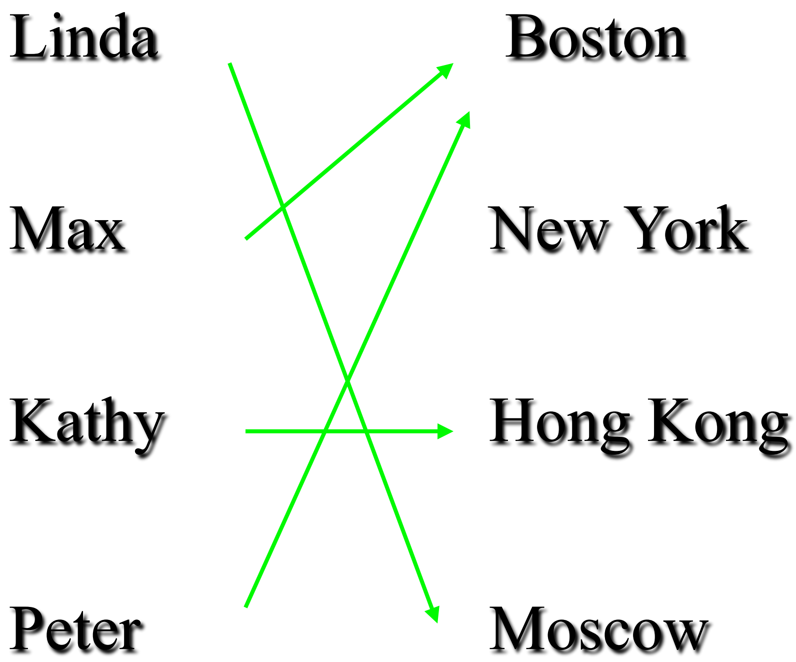
Properties of Functions

Examples:

In the following examples, we use the arrow to represent function mappings f: A→B

Function is a special relation in which each element of the domain A is paired with (mapped onto) exactly one element in the range B. The mapping shows how elements are paired

Properties of Functions



Is f injective?

No

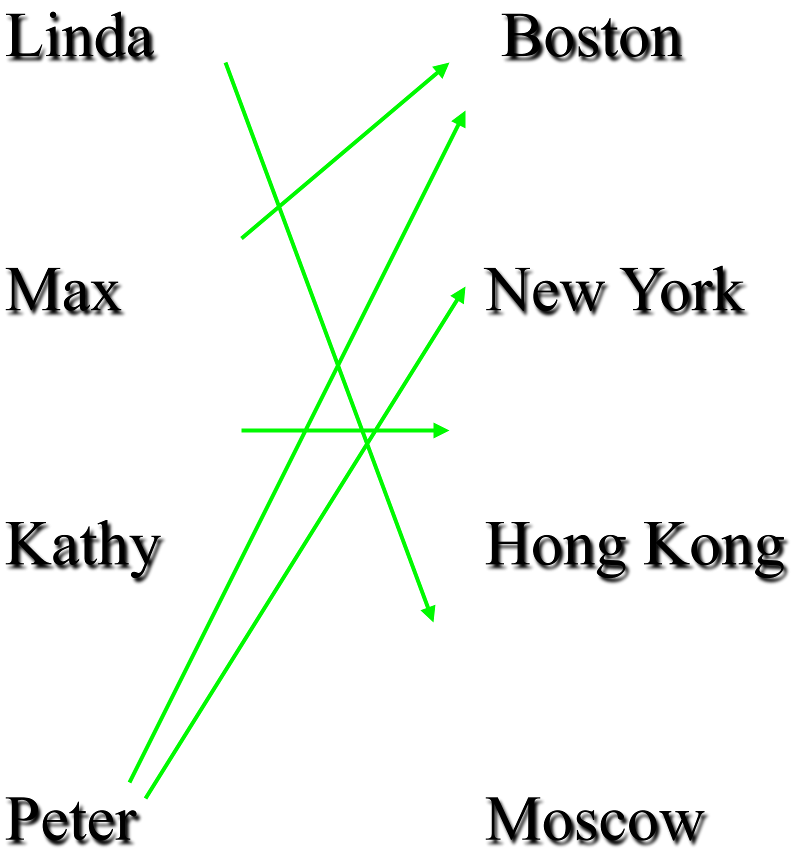
Is f surjective?

No

Is f bijective?

No

Properties of Functions



Is f injective?

No

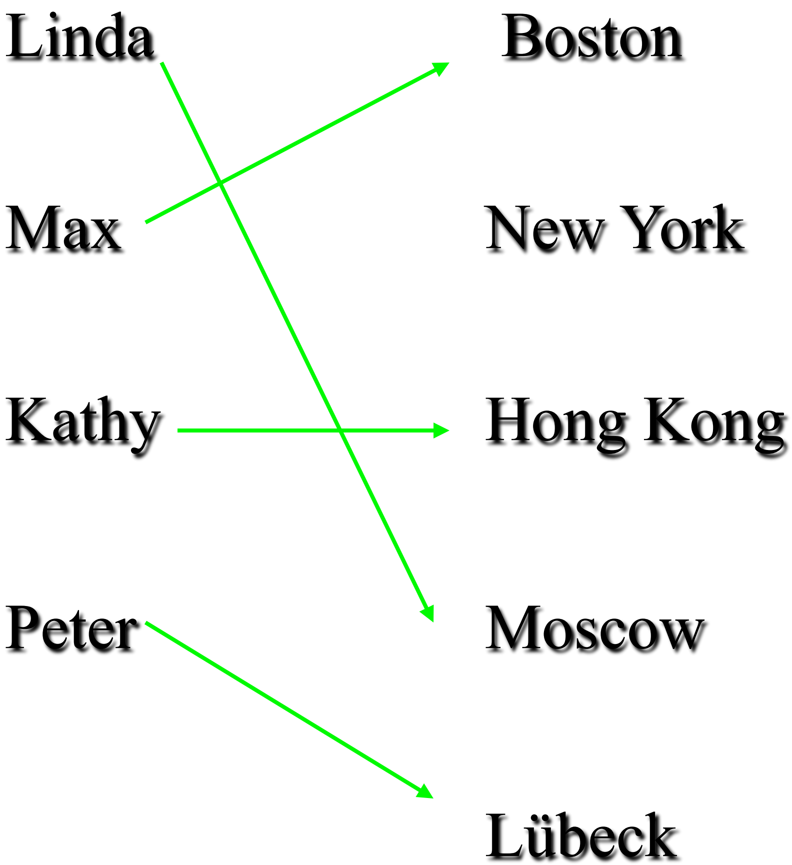
Is f surjective?

Yes

Is f bijective?

No

Properties of Functions



Is f injective?

Yes

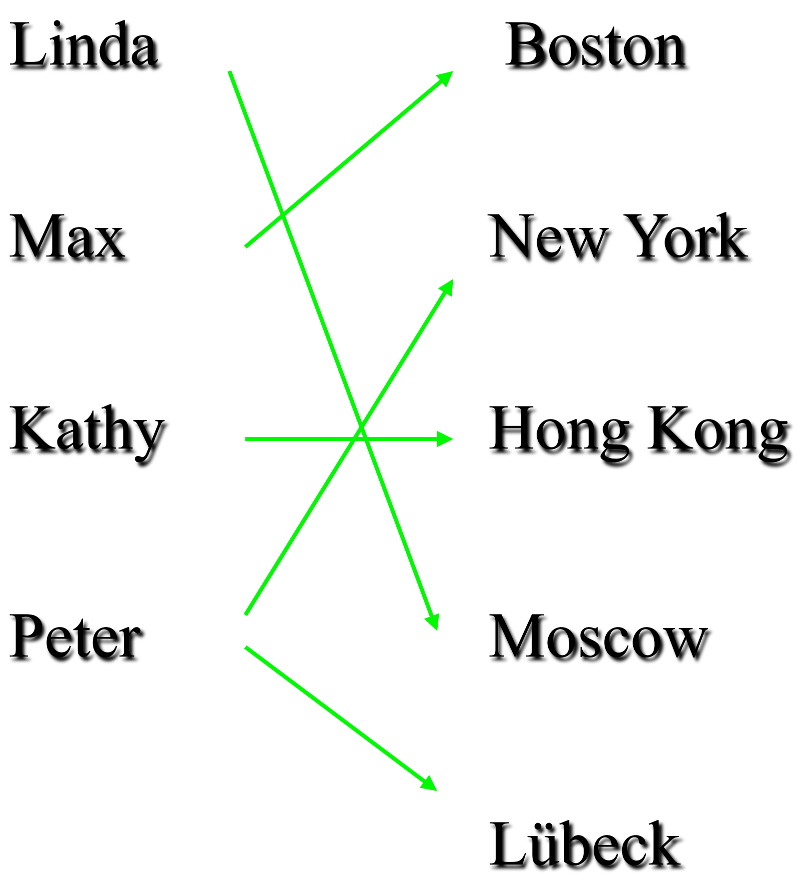
Is f surjective?

No

Is f bijective?

No

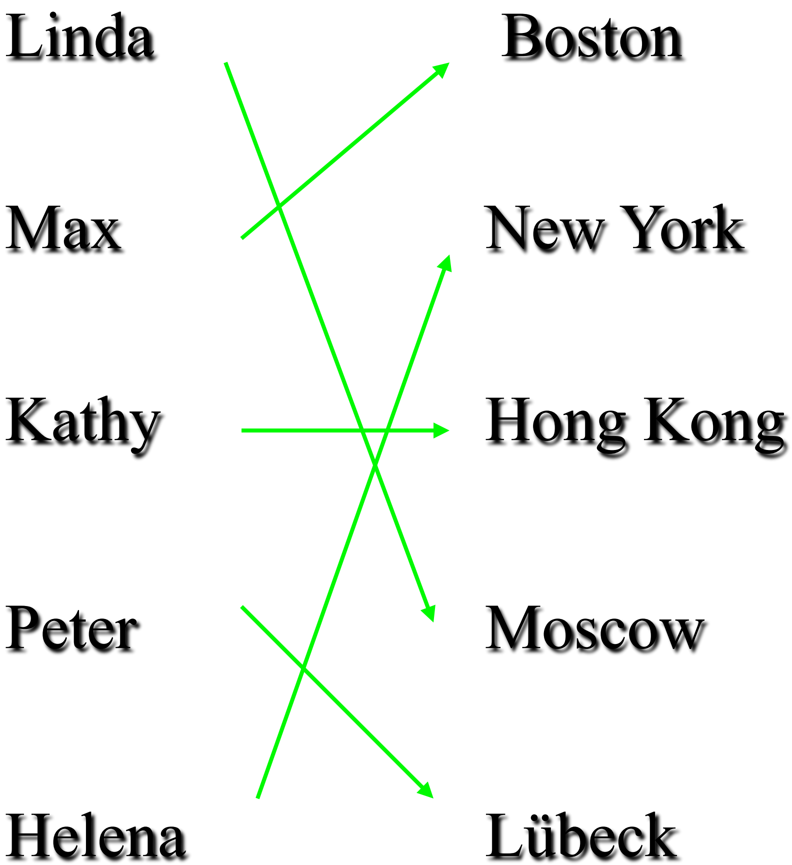
Properties of Functions



Is f injective?

No! f is not even a function!

Properties of Functions



Is f injective?

Yes

Is f surjective?

Yes

Is f bijective?

Yes

Inversion

- **An interesting property of *bijections* is that they have an inverse function**
- **The inverse function of the bijection $f: A \to B$ is the function $f^{-1}: B \to A$ with**

$$f^{-1}(b) = a \text{ whenever } f(a) = b$$

Inversion

Example:

f(Linda) = Moscow
f(Max) = Boston
f(Kathy) = Hong Kong
f(Peter) = Lübeck
f(Helena) = New York

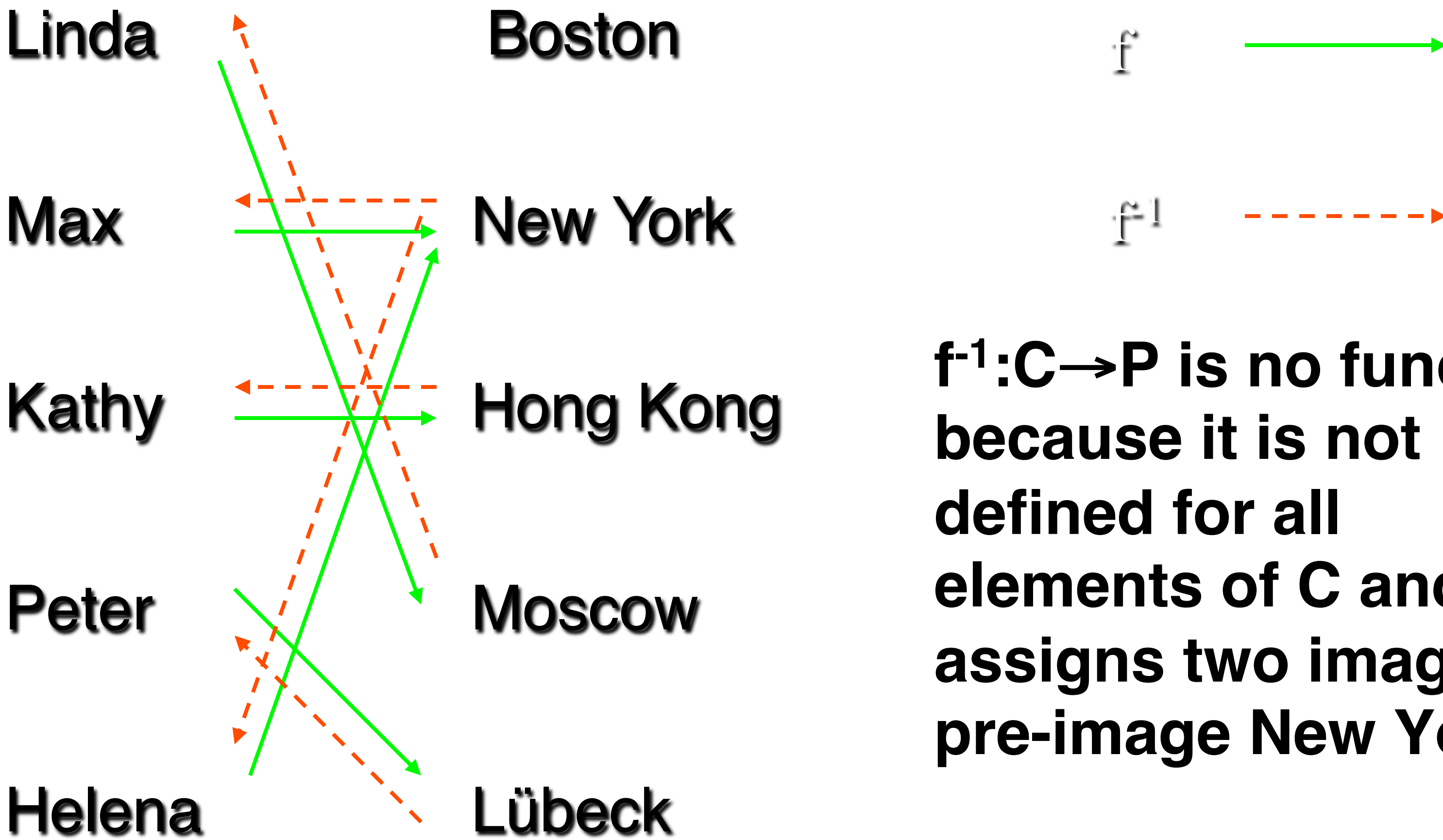
Clearly, f is bijective.

Inverse function f^{-1}:

f^{-1}(Moscow) = Linda
f^{-1}(Boston) = Max
f^{-1}(Hong Kong) = Kathy
f^{-1}(Lübeck) = Peter
f^{-1}(New York) = Helena

Inversion is only possible for bijections = invertible functions

Inversion



f^{-1}:C→P is no function, because it is not defined for all elements of C and assigns two images to pre-image New York

Composition

The composition of two functions $g:A \rightarrow B$ and $f:B \rightarrow C$, denoted by $f \circ g$, is defined by

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

This means that

- first, function g is applied to element $a \in A$, mapping it onto an element of B
- then, function f is applied to this element of B, mapping it onto an element of C
- therefore, the composite function maps from A to C

Composition

Example:

$f(x) = 7x - 4$, $g(x) = 3x$,

$f: R \rightarrow R$, $g: R \rightarrow R$

$(f \circ g)(5) = f(g(5)) = f(15) = 105 - 4 = 101$

$(f \circ g)(x) = f(g(x)) = f(3x) = 21x - 4$

Composition

- **Composition of a function and its inverse:**
- **$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x$**
- **The composition of a function and its inverse is the identity function $i(x) = x$**

Graphs

- The graph of a function $f:A \rightarrow B$ is the set of ordered pairs $\{ (a, b) \mid a \in A \text{ and } f(a) = b \}$
- The graph is a subset of $A \times B$ that can be used to visualize f in a two-dimensional coordinate system

Floor and Ceiling Functions

- The floor and ceiling functions map the real numbers onto the integers ($R \to Z$)
- Floor function assigns to $r \in R$ the largest $z \in Z$ with $z \leq r$, denoted by $\lfloor r \rfloor$
- Examples: $\lfloor 2.3 \rfloor = 2$, $\lfloor 2 \rfloor = 2$, $\lfloor 0.5 \rfloor = 0$, $\lfloor -3.5 \rfloor = -4$
- Ceiling function assigns to $r \in R$ the smallest $z \in Z$ with $z \geq r$, denoted by $\lceil r \rceil$
- Examples: $\lceil 2.3 \rceil = 3$, $\lceil 2 \rceil = 2$, $\lceil 0.5 \rceil = 1$, $\lceil -3.5 \rceil = -3$

Boolean Algebra, Again!

Boolean Algebra

- Boolean algebra provides the operations and the rules for working with the set { 0, 1 }
- These are rules underlying electronic circuits, and methods fundamental to VLSI design
- We are going to focus on the following operations:
  - Boolean complementation
  - Boolean sum
  - Boolean product

Boolean Operations

Note, the Boolean complement is often denoted by a bar -. On the following slides, we'll use that minus bar. Caveat: the -0 is not a "minus zero" ☺

$$-0 = 1 \quad \text{and} \quad -1 = 0$$

The Boolean sum, denoted by + or by OR, has the following values:

$1 + 1 = 1, \quad 1 + 0 = 1, \quad 0 + 1 = 1, \quad 0 + 0 = 0$

The Boolean product, denoted by · or also sometimes by AND, has the following values:

$1 \cdot 1 = 1, \quad 1 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 0 \cdot 0 = 0$

Boolean Functions and Expressions

- Definition: Let B = { 0, 1 }. The variable **x** is called a Boolean variable if it assumes values only from B
- A function from B^n, the set $\{ (x_1, x_2, \ldots, x_n) \mid x_i \in B, 1 \le i \le n \}$, to B is called a Boolean function of **degree n**
- Boolean functions can be represented using expressions made up from variables and Boolean operations

Boolean Functions and Expressions

The Boolean expressions using variables $x_1, x_2, \ldots, x_n$ are defined recursively as follows:

- $0, 1, x_1, x_2, \ldots, x_n$ are Boolean expressions.
- If E_1 and E_2 are Boolean expressions, then $(-E_1)$, (E_1E_2), and $(E_1 + E_2)$ are Boolean expressions

Each Boolean expression represents a Boolean function. The values of this function are obtained by substituting 0 and 1 for the variables in the expression

Boolean Functions and Expressions

- For example, we can create Boolean expression in the variables x, y, and z using the "building blocks" 0, 1, x, y, and z, and the construction rules:
- Since x and y are Boolean expressions, so is xy
- Since z is a Boolean expression, so is -z, AKA not z
- Since xy and (-z) are expressions, so is xy + (-z)

… and so on…

Boolean Functions and Expressions

Example: Give a Boolean expression for the Boolean function F(x, y) as defined by the following table:

x	y	F(x, y)
0	0	0
0	1	1
1	0	0
1	1	0

Possible solution: F(x, y) = (-x) y

Boolean Functions and Expressions

Another Example:

x	y	z	F(x, y, z)
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

Possible solution I:

F(x, y, z) = -(xz + y)

Possible solution II:

F(x, y, z) = (-(xz)) (-y)

Boolean Functions and Expressions

- There is a simple method for deriving a Boolean Expression for a function defined by a table
- This method is based on co-called minterms
- Definition: A literal is some fixed Boolean value or its complement
- A minterm of the Boolean variables $x_1, x_2, \ldots, x_n$ is a Boolean product $y_1 y_2 \ldots y_n$, where $y_i = x_i$ or $y_i = -x_i$
- Hence, a minterm is a product of n literals, with one literal for each variable

Boolean Functions and Expressions

Consider F(x, y, z) again:

x	y	z	F(x, y, z)
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

F(x, y, z) = 1 if and only if:

x = y = z = 0 or

x = y = 0, z = 1 or

x = 1, y = z = 0

Therefore,

F(x, y, z) =

(-x)(-y)(-z) +

(-x)(-y) z +

x (-y)(-z)

Boolean Functions and Expressions

- Definition: The Boolean functions F and G of n variables are equal (trivially visible) if and only if $F(b_1, b_2, \ldots, b_n) = G(b_1, b_2, \ldots, b_n)$ for all b_i
- Two different Boolean expressions that represent the same function are called equivalent
- For example, the Boolean expressions xy, $xy + 0$, and $xy \cdot 1$ are equivalent

Boolean Functions and Expressions

- The complement of Boolean function F is the function $-F$, where $-F(b_1, b_2, \ldots, b_n) = -(F(b_1, b_2, \ldots, b_n))$
- Let F and G be Boolean functions of degree n
- The Boolean sum F+G and Boolean product FG are then defined by

$$(F + G)(b_1, b_2, \ldots, b_n) = F(b_1, b_2, \ldots, b_n) + G(b_1, b_2, \ldots, b_n)$$

$$(FG)(b_1, b_2, \ldots, b_n) = F(b_1, b_2, \ldots, b_n)\, G(b_1, b_2, \ldots, b_n)$$

Boolean Functions and Expressions

- **Question: How many different Boolean functions of degree 1 are there?**
- **Solution: There are four of them, F_1, F_2, F_3, and F_4:**

x	F_1	F_2	F_3	F_4
0	0	0	1	1
1	0	1	0	1

Boolean Functions and Expressions

- **Question: How many different Boolean functions of degree 2 are there?**
- **Solution: There are 16 of them, F_1, F_2, …, F_{16}:**

x	y	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}	F_{11}	F_{12}	F_{13}	F_{14}	F_{15}	F_{16}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Boolean Functions and Expressions

- Question: How many different Boolean functions of degree n are there?
- There are 2^n different n-tuples of 0s and 1s
- A Boolean function is an assignment of 0 or 1 to each of these 2^n different n-tuples
- Therefore, there are 2^{2^n} different Boolean functions

Duality

- There are useful identities of Boolean expressions that can help us to transform an expression A into an equivalent expression B
- We can derive additional identities with the help of the dual of a Boolean expression
- The dual of a Boolean expression is obtained by interchanging Boolean sums and Boolean products and interchanging 0s and 1s

Duality

Examples:

Dual(x(y + z)) = -x + (-y -z) AKA x' + y' z'

Dual(-x + -y + z) = x y -z AKA x y z'

- The dual d() of a Boolean function f() represented by a Boolean expression is the function represented by the dual of this expression
- This dual function, denoted by $f()^d$, does not depend on the particular Boolean expression used to represent f()
- To generate: exchange or with and, and with or, and true with false and false with true, or negated boolean variable

Duality

- Therefore, an identity between functions represented by Boolean expressions remains valid when the duals of both sides of the identity are taken
- We can use this fact, called the duality principle, to derive new identities
- For example, consider the absorption law $x(x + y) = x$
- By taking the duals of both sides of this identity, we obtain the equation $x + xy = x$, also called Absorption Law

A Boolean Algebra

- **All the properties of Boolean functions and expressions that we have discovered also apply to other mathematical structures such as propositions and sets and the operations defined on them**
- **If we can show that a particular structure is a Boolean algebra, then we know that all results established about Boolean algebras apply to this structure**
- **For this purpose, we need an abstract definition of a Boolean algebra**

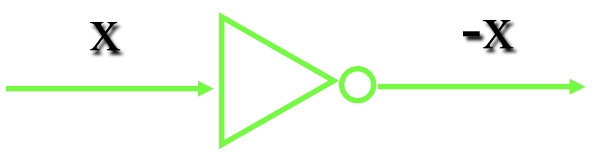
A Boolean Algebra

Definition: A Boolean algebra is a set B with two binary operations $\vee$ and $\wedge$, elements 0 and 1, and a unary operation – such that the following properties hold for all x, y, and z in B:

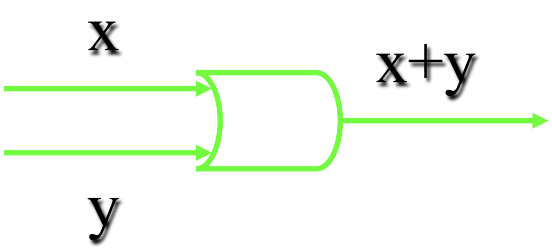
- $x \vee 0 = x$ and $x \wedge 1 = x$ **identity law**
- $x \vee (-x) = 1$ and $x \wedge (-x) = 0$ **domination laws**
- $(x \vee y) \vee z = x \vee (y \vee z)$ and
  $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ **associative laws**
- $x \vee y = y \vee x$ and $x \wedge y = y \wedge x$ **commutative laws**
- $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ and
  $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ **distributive laws**

Logic Gates

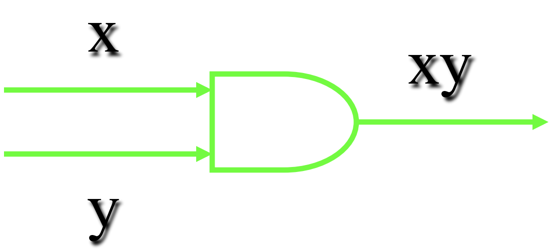
Electronic circuits consist of so-called gates.
There are three basic types of gates:



Inverter



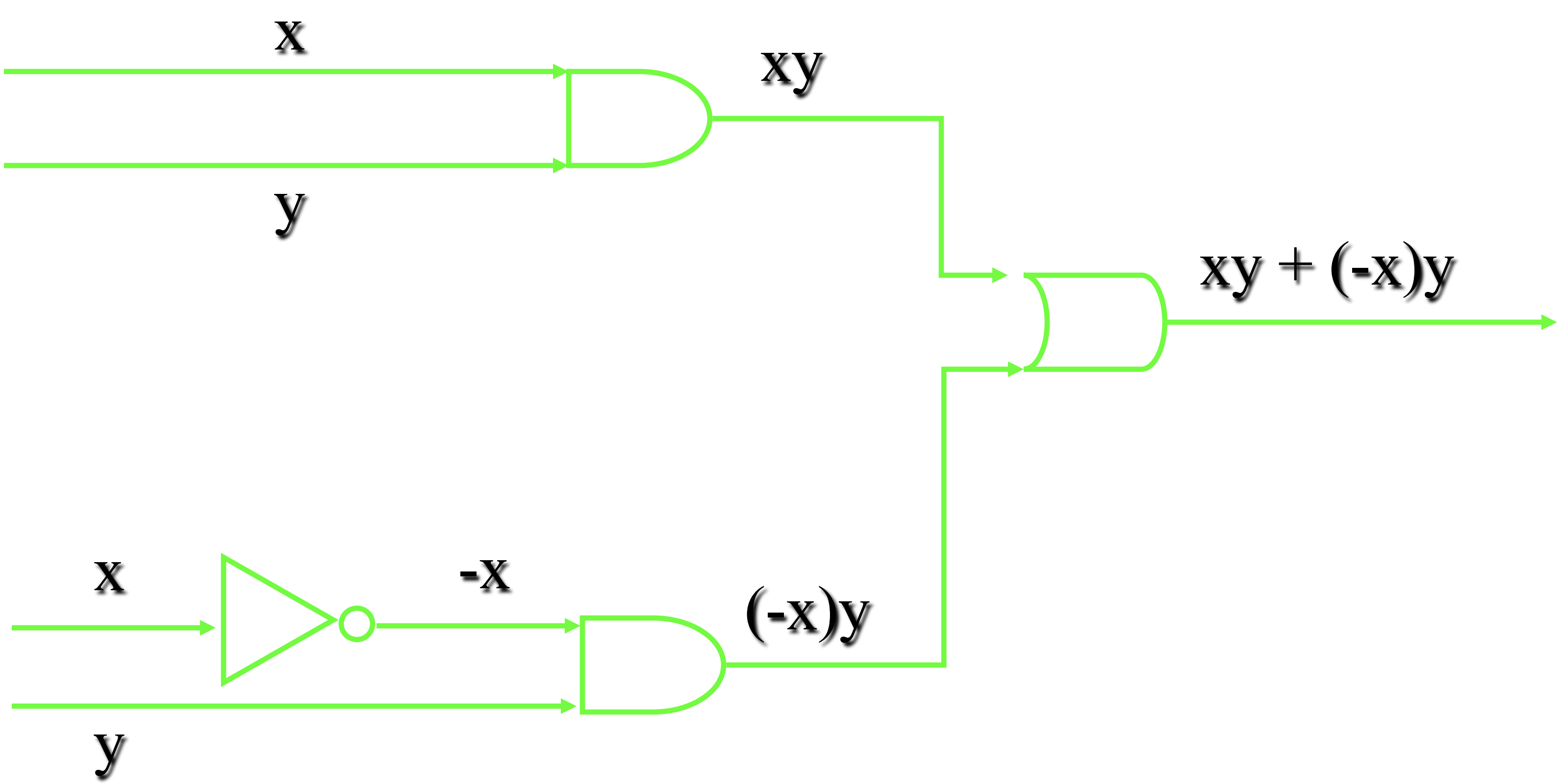
OR gate



AND gate

Logic Gates

Example: How can we build a circuit that computes the function xy + (-x)y ?



Logic, Sets, and Boolean Algebra

<u>Logic</u>	<u>Set</u>	<u>Boolean Algebra</u>
False	$\varnothing$	0
True	U	1
$A \wedge B$	$A \cap B$	$A \cdot B$
$A \vee B$	$A \cup B$	$A+B$
$\neg A$	A^C	not A

Summary

- **Set Theory *branch of mathematics* founded by Georg Cantor**
- **Is a branch of mathematical logic that studies sets**
- **Sets are are collections of objects**
- **Mathematical Logic, Set Theory, Boolean Algebra are equivalent**
- **Duality in Logic Expression often helps in actual circuits to implement by using gates currently at hand**

References

1. Cartesian product: https://en.wikipedia.org/wiki/Cartesian_product
2. Zermelo-Fraenkel set Theory: https://plato.stanford.edu/entries/set-theory/ZF.html
3. Wiki on Set Theory: https://en.wikipedia.org/wiki/Set_theory
4. On large Cardinals: https://en.wikipedia.org/wiki/Large_cardinal
5. Axiom of Choice: https://en.wikipedia.org/wiki/Axiom_of_choice