CS220: Applied Discrete Mathematics

Summer 2022

Instructor: Bang Tran

UMass Boston

1

Summary of Proofs (Theorem)

- Direct proof
- Indirect proof
- Prove by cases
- Proof by contradiction

- A direct proof of $p \rightarrow q$ is true by showing that if p is true, then q must also be true, so that the combination p true and q false never occurs.
  - First step: assuming that p is true
  - Second step: showing that q is also true

UMass Boston

2

Summary of Proofs (Theorem)

- Direct proof
- Indirect proof
- Prove by cases
- Proof by contradiction

An implication p→q is equivalent to its contrapositive ¬q → ¬p.
Therefore, we can prove p→q by showing that whenever q is false, then p is also false.

- Step 1: Introduce ¬q as a premise
- Step 2: attempt to derive ¬p

Is also called proof by contraposition

Summary of Proofs (Theorem)

- Direct proof
- Indirect proof
- Prove by cases
- Proof by contradiction

A proof by cases must cover all possible cases that arise in a theorem.

To prove $(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$
we prove that

$$(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \vee (p_n \rightarrow q)$$

Summary of Proofs (Theorem)

- Direct proof
- Indirect proof
- Prove by cases
- Proof by contradiction

Because the statement $r \wedge \neg r$ is a contradiction whenever r is a proposition, we can prove that p is true if we can show that $\neg p \rightarrow (r \wedge \neg r)$ is true for some proposition r

- Step 1: Introduce $\neg p$ as a premise
- Step 2: attempt to derive a contradiction $\neg r \wedge r$

Boolean Algebra

Chapter 12 in the textbook

Boolean Algebra

- Boolean algebra provides the operations and the rules for working with the set **{0, 1}.**
- These are the rules that underlie **electronic circuits**, and the methods we will discuss are fundamental to **VLSI design**.
- We are going to focus on 3 operations:
  - Boolean complementation,
  - Boolean sum, and
  - Boolean product

Boolean Operations

- The **complement** is denoted by a bar (on the slides, we will use a minus sign). It is defined by

  $\bar{0} = 1$ and $\bar{1} = 0.$

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

Boolean Functions and Expressions

- The **Boolean expressions** in the 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 $\overline{E_1}$, $(E_1 E_2)$, 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 $\bar{z}$.
- Since xy and $\bar{z}$ are Boolean expressions, so is $xy\ +\bar{z}$.
- … 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: $F(x, y)\ = \bar{x} \cdot y$

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:

$$F(x, y, z) = \overline{xz + y}$$

Possible solution II:

$$F(x, y, z) = (\overline{xz})\bar{y}$$

Boolean Functions and Expressions

- There is a simple method for deriving a Boolean expression for a function that is defined by a table. This method is based on **minterms**.
- **Definition:** A **literal** is a Boolean variable 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 $y_i = \bar{x}_i$.
- 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,
$F(x, y, z) = \bar{x}\bar{y}\bar{z} + \bar{x}\bar{y}z + x\bar{y}\bar{z}$

Boolean Functions and Expressions

- **Definition:** The Boolean functions F and G of n variables are **equal** if and only if $F(b_1, b_2, \dots, b_n) = G(b_1, b_2, \dots, b_n)$ whenever $b_1, b_2, \dots, b_n$ belong to $\mathbb{B}$.
- 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 the Boolean function F is the function $\overline{F}$, where $\overline{F}(b_1, b_2, \dots, b_n) = \overline{F(b_1, b_2, \dots, b_n)}$.

- Let F and G be Boolean functions of degree n. The **Boolean sum** $\boldsymbol{F + G}$ and **Boolean product** $\boldsymbol{FG}$ are then defined by

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

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

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, $F_1, F_2, \ldots, F_{16}$:

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?

- **Solution:**
  - 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.

Identities

There are useful identities of Boolean expressions that can help us to transform an expression A into an equivalent expression B, e.g.:

Identity Name	AND Form	OR Form
Identity Law	$1x = x$	$0+x = x$
Null (or Dominance) Law	$0x = 0$	$1+x = 1$
Idempotent Law	$xx = x$	$x+x = x$
Inverse Law	$x\bar{x} = 0$	$x+\bar{x} = 1$
Commutative Law	$xy = yx$	$x+y = y+x$
Associative Law	$(xy)z = x(yz)$	$(x+y)+z = x+(y+z)$
Distributive Law	$x+yz = (x+y)(x+z)$	$x(y+z) = xy+xz$
Absorption Law	$x(x+y) = x$	$x+xy = x$
DeMorgan's Law	$(\overline{xy}) = \bar{x}+\bar{y}$	$(\overline{x+y}) = \bar{x}\bar{y}$
Double Complement Law	$\bar{\bar{x}} = x$	

Definition of 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.

Definition of 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 laws)

$x \vee \bar{x} = 1$ and $x \wedge \bar{x} = 0$ (domination laws)

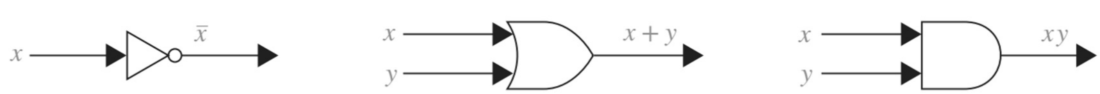
$(x \vee y) \vee z = x \vee (y \vee z)$ and
$(x \wedge y) \wedge z = x \wedge (y \wedge z)$ and (associative laws)

$x \vee y = y \vee x$ 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

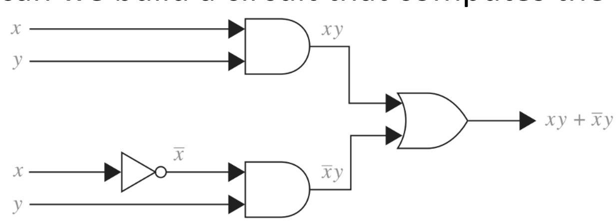
Electronic circuits consist of so-called gates. There are three basic types of gates:

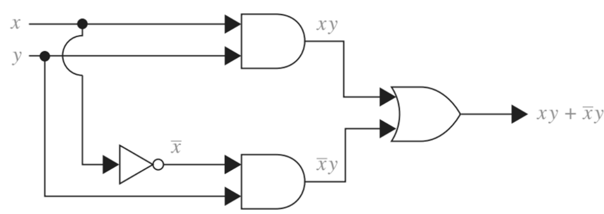


(a) Inverter (b) OR gate (c) AND gate

Logic Gates

- **Example:** How can we build a circuit that computes the function $xy + \bar{x}y$?



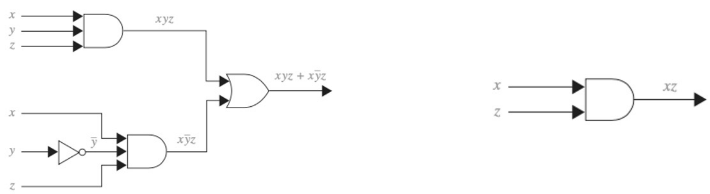


Minimization of Circuits

Chapter 12.4 int the textbook

Minimization of Circuits

- The efficiency of a combinational circuit depends on the number and arrangement of its gates.
- We can always use the sum-of-products expansion of a circuit to find a set of logic gates that will implement this circuit. However, the sum-of-products expansion may contain many more terms than are necessary.



Minimization of Circuits

- Reducing the number of gates on a chip can lead to a more reliable circuit and can reduce the cost to produce the chip.
- Minimization makes it possible to fit more circuits on the same chip.
- Minimization reduces the number of inputs to gates in a circuit. The number of inputs to a gate may be limited because of the particular technology used to build logic gates.
- Reduces the time used by a circuit to compute its output.

Karnaugh Maps (K-Maps)

- Special form of a truth table which enables easier pattern recognition
- Pictorial method of simplifying Boolean expressions
- Good for circuit designs with up to 4 variables

Karnaugh Maps (K-Maps)

Truth Table

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

K-Map

y \ x	0	1
0	0	1
1	1	1

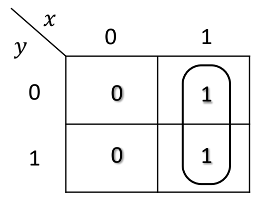
F

Karnaugh Maps (K-Maps)

Truth Table

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

K-Map



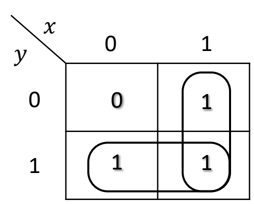
$F = x$

Karnaugh Maps (K-Maps)

Truth Table

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

K-Map



The vertical group shows that the output is independent to y
The horizontal group shows that the ouput is independent to x

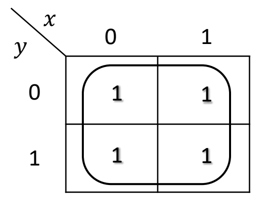
$F = x + y$

Karnaugh Maps (K-Maps)

Truth Table

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

K-Map



The output is independent to all of inputs

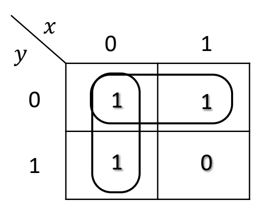
$F = 1$

Karnaugh Maps (K-Maps)

Truth Table

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

K-Map



The 1s in vertical group are always x
The 1s horizontal group are always y

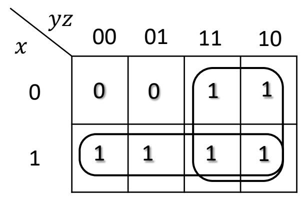
$F = \bar{x} + \bar{y}$

K-Map in three variables

Truth Table

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

K-Map



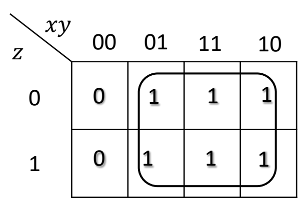
$$F = x + y$$

K-Map in three variables

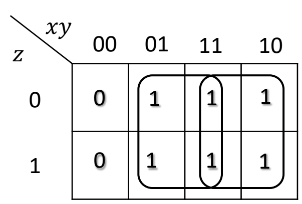
Truth Table

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

K-Map



Wrong! A group of 1s can only contain 2^n of 1s



Correct!

K-Map in three variables

x \ yz	00	01	11	10
0	0	0	1	0
1	0	0	1	0

$F = yz$

x \ yz	00	01	11	10
0	1	0	0	1
1	1	0	0	1

$F = \bar{z}$

x \ yz	00	01	11	10
0	0	0	0	0
1	1	0	0	1

$F = x\bar{z}$

Grouping rules in K-Maps

- A group must only contains 1s, no 0s
- A group can only be horizontal or vertical, not diagonal
- A group must contain 2^n (1, 2, 4, 8, etc.) of 1s
- Each group should be as large as possible
- Groups may overlap
- Groups may wrap around a table
- Every 1 must be in at least one group

K-Map in three variables

- Use K-maps to minimize these sum-of-production expansions.
  a) $xy\bar{z} + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}\bar{y}\bar{z}$
  b) $x\bar{y}z + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z}$
  c) $xyz + xy\bar{z} + x\bar{y}z + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z}$
  d) $xy\bar{z} + x\bar{y}\bar{z} + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z}$

K-Map in three variables

a) $xy\bar{z} + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}\bar{y}\bar{z}$

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x		1	1	
$\bar{x}$	1		1	

$$F = x\bar{z} + \bar{y}\bar{z} + \bar{x}yz$$

K-Map in three variables

b) $x\bar{y}z + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z}$

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x			1	1
$\bar{x}$	1		1	1

$$F = \bar{y} + \bar{x}z$$

K-Map in three variables

c) $xyz + xy\bar{z} + x\bar{y}z + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z}$

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x	1	1	1	1
$\bar{x}$	1		1	1

$$F = x + \bar{y} + z$$

K-Map in three variables

d) $xy\bar{z} + x\bar{y}\bar{z} + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z}$

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x		1	1	
$\bar{x}$			1	1

$$F = x\bar{z} + \bar{y}\bar{z} + \bar{x}\bar{y}$$

The prime implicant $\bar{y}\bar{z}$ is not essential because the cells it covers are covered by other prime implicants.

$$F = x\bar{z} + \bar{x}\bar{y}$$

K-Map in four variables

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
wx				
$w\bar{x}$				
$\bar{w}\bar{x}$				
$\bar{w}x$				

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
wx	1			1
$w\bar{x}$				
$\bar{w}\bar{x}$				
$\bar{w}x$	1			1

K-Map in four variables

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
wx				
$w\bar{x}$				
$\bar{w}\bar{x}$	1	1	1	1
$\bar{w}x$				

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
wx		1	1	
$w\bar{x}$		1	1	
$\bar{w}\bar{x}$		1	1	
$\bar{w}x$		1	1	

K-Map in four variables

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
wx				
$w\bar{x}$				
$\bar{w}\bar{x}$	1			1
$\bar{w}x$				

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
wx		1	1	
$w\bar{x}$				
$\bar{w}\bar{x}$				
$\bar{w}x$		1	1	

47

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
wx	**1**		**1**	**1**
$w\bar{x}$		**1**		**1**
$\bar{w}\bar{x}$				
$\bar{w}x$				

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
wx		**1**		**1**
$w\bar{x}$	**1**			
$\bar{w}\bar{x}$		**1**		**1**
$\bar{w}x$				**1**

48

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
wx	**1**	**1**		**1**
$w\bar{x}$			**1**	**1**
$\bar{w}\bar{x}$		**1**		**1**
$\bar{w}x$				**1**

49

Sets

Chapter 2.1 – 2.2 in the textbook

50

Definition

A set is an unordered collection of objects, called elements or members of the set.

Notation $A = \{a_1, a_2, \dots, a_n\}$

We write $a \in A$ to denote that a is an element of the set A.

The notation $a \notin A$ denotes that a is not an element of the set A

Order of elements is meaningless.

It does not matter how often the same element is listed.

Set Examples

"Standard" Sets:

Natural numbers $\mathbb{N} = \{0, 1, 2, 3, \dots\}$

Integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

Positive Integers $\mathbb{Z}^+ = \{1, 2, 3, 4, \dots\}$

Real Numbers $\mathbb{R} = \{47.3, -12, \pi, \dots\}$

Rational Numbers $\mathbb{Q} = \{1.5, 2.6, -3.8, 15, \dots\}$

(correct definition will follow)

Set Examples

$A = \emptyset$ "empty set/null set"

$A = \{z\}$ Note: $z \in A$, but $z \neq \{z\}$

$A = \{\{b, c\}, \{c, x, d\}\}$

$A = \{\{x, y\}\}$ Note: $\{x, y\} \in A$, but $\{x, y\} \neq \{\{x, y\}\}$

$A = \{x \mid P(x)\}$ "set of all x such that $P(x)$"

$A = \{x \mid x \in \mathbb{N} \wedge x > 7\} = \{8, 9, 10, \dots\}$

Set Examples

We are now able to define the set of rational numbers $\mathbb{Q}$:

$$\mathbb{Q} = \{a/b \mid a \in \mathbb{Z} \wedge b \in \mathbb{Z}^{+}\} \text{ or } \mathbb{Q} = \{a/b \mid a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge b \neq 0\}$$

And how about the set of real numbers $\mathbb{R}$?

$$\mathbb{R} = \{r \mid r\ is\ a\ real\ number\}$$

That is the best we can do.

Set representations

Roster Form

- All elements of the set are listed in-between curly brackets

Statement Form

- The well-defined descriptions of a member of a set
  E.g., "The set of even numbers less than 20"

Set Builder Form

- The general form is $A = \{x : property\}$

Venn Diagram

- The simple and best way for visualized representation of sets.

Set Equality

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

$A = \{9, 2, 7, -3\}$, $B = \{7, 9, -3, 2\}$: $A = B$

Examples:

$A = \{dog, cat, horse\}$,
$B = \{cat, horse, squirrel, dog\}$ $A \neq B$

$A = \{dog, cat, horse\}$, $B = \{cat, horse, dog, dog\}$ $A = B$

Subsets

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

$A \subseteq B$ iff every element of A is also an element of B.

We can completely formalize this: $A \subseteq B \Leftrightarrow \forall x\ (x \in A \rightarrow x \in B)$

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

Examples:

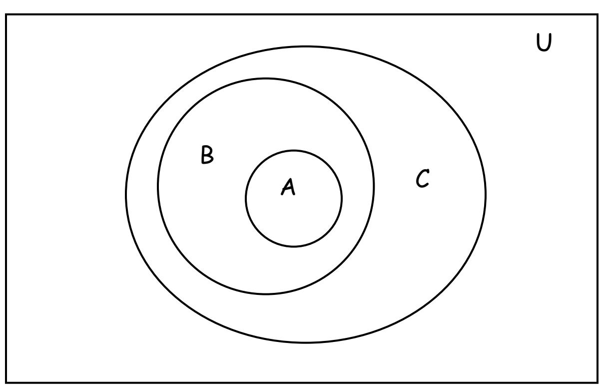
A = {3, 3, 3, 9}, B = {5, 9, 1, 3}, $A \subseteq B$? true

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

Subsets

- Useful rules: $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$; $(A \subseteq B) \wedge (B \subseteq C) \Rightarrow A \subseteq C$

(see 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"

  $A \subset B \Leftrightarrow \forall x\, (x \in A \rightarrow x \in B) \land \exists x\, (x \in B \land x \notin A)$
  or
  $A \subset B \Leftrightarrow \forall x\, (x \in A \rightarrow x \in B) \land \neg \forall x\, (x \in B \rightarrow x \in A)$

Cardinality of Sets

If a set S contains n distinct elements, $n \in \mathbb{N}$,
we call S a **finite set** with **cardinality n**. We write $|S| = n$

Examples:

A = {Mercedes, BMW, Porsche},	$\|A\| = 3$
$B = \{1, \{2, 3\}, \{4, 5\}, 6\}$	$\|B\| = 4$
$C = \emptyset$	$\|C\| = 0$
$D = \{ x \in \mathbb{N} \mid x \leq 7000 \}$	$\|D\| = 7001$
$E = \{ x \in \mathbb{N} \mid x \geq 7000 \}$	E is infinite!

The Power Set

- The power set is the set of all subsets of the given set A.
- We write:

  2^A or $\mathcal{P}(A)$ "power set of A"

  $2^A = \{B \mid B \subseteq A\}$ (contains all subsets of A)

- Examples:

  $A = \{x, y, z\}$

  $2^A = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}$

  $A = \emptyset$

  $2^A = \{\emptyset\}$

  $Note$: $|A| = 0$, $|2^A| = 1$

The Power Set

- Cardinality of power sets:

  $2^A \mid = 2^{|A|}$

  Imagine each element in A has an "on/off" switch

  Each possible switch configuration in A corresponds to one element in 2^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**

For 3 elements in A, there are $2\times2\times2 = 8$ elements in 2^A

Cartesian Product

- The ordered n-tuple $(a_1, a_2, \ldots, a_n)$ is an ordered collection of objects.
- Two ordered n-tuples$(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ are equal if and only if they contain exactly the same elements in the same order, i.e., $a_i = b_i$ for $1 \leq i \leq n$.

The Cartesian product of two sets is defined as:

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

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

$$A{\times}B = \{(x, a), (x, b), (x, c), (y, a), (y, b), (y, c)\}$$

UMass Boston

Cartesian Product

- Note that:
  - $A \times \emptyset = \emptyset$
  - $\emptyset \times A = \emptyset$
  - For non-empty sets A and B: $A{\neq}B \Leftrightarrow A{\times}B \neq B{\times}A$
  - $|A{\times}B| = |A|{\cdot}|B|$
- The Cartesian product of two or more sets is defined as:

$$A_1{\times}A_2{\times} \ldots {\times}An = \{(a_1, a_2, \ldots, an) | a_i \in A_i \; for \; 1 \leq i \leq n\}$$

UMass Boston

Partitions

Definition:
A partition of a set S is a collection of disjoint nonempty subsets of S that have S as their union. In other words, the collection of subsets $Ai, i \in I$, forms a partition of S if and only if:

1) $A_i \neq \emptyset$ for $i \in I$
2) $A_i \cap A_j = \emptyset$ if $i \neq j$
3) $\bigcup_{i \in I} Ai = S$

Partitions

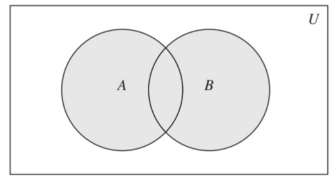
Examples: Let S be the set $\{u, m, b, r, o, c, k, s\}$. Do the following collections of sets partition S ?

$\{\{m, o, c, k\}, \{r, u, b, s\}\}$	yes.
$\{\{c, o, m, b\}, \{u, s\}, \{r\}\}$	no (k is missing).
$\{\{b, r, o, c, k\}, \{m, u, s, t\}\}$	no (t is not in S).
$\{\{u, m, b, r, o, c, k, s\}\}$	yes.
$\{\{b, o, r, k\}, \{r, u, m\}, \{c, s\}\}$	no (r is in two sets).
$\{\{u, m, b\}, \{r, o, c, k, s\}, \emptyset\}$	no (∅ is not allowed).

Set Operations

- Union: A∪B = {x | x∈A ∨ x∈B}

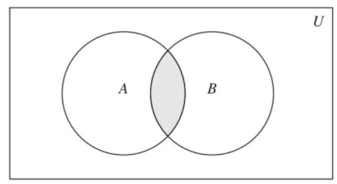
E.g., A = {a, b}, B = {b, c, d} A∪B = {a, b, c, d}



$A \cup B$ is shaded.

- Intersection: A∩B = {x | x∈A ∧ x∈B}

E.g., A = {a, b}, B = {b, c, d} A∩B = {b}



$A \cap B$ is shaded.

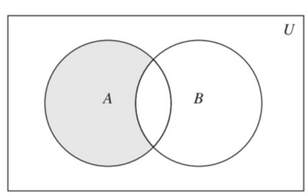
Set Operations

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

  $A \cap B = \varnothing$

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

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



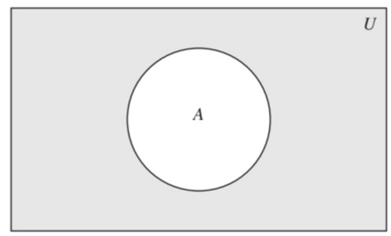
$A - B$ is shaded.

Example: $A = \{1, 2\}$, $B = \{2, 4, 6\}$, $A - B = \{1\}$

Set Operations

- The complement of a set A contains exactly those elements under consideration that are not in A:

  $\bar{A} = U - A$



$\bar{A}$ is shaded.

Example: $U = \mathbb{N},\ B = \{250, 251, 252, \dots\}$

$\bar{B} = \mathbb{N} - B = \{0, 1, 2, \dots, 248, 249\}$

- Table 1 in Section 2.2 (8th edition) shows many useful equations for set identities.

Identity	*Name*
$A \cap U = A$ $A \cup \emptyset = A$	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
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

Set Operations

- **How can we prove** $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$?
- Method 1:

$$x \in A \cup (B \cap C)$$
$$\Leftrightarrow x \in A \vee x \in (B \cap C)$$
$$\Leftrightarrow x \in A \vee (x \in B \wedge x \in C)$$
$$\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$$
(distributive law for logical expressions)
$$\Leftrightarrow x \in (A \cup B) \wedge x \in (A \cup C)$$
$$\Leftrightarrow x \in (A \cup B) \cap (A \cup C)$$

UMass Boston

Set Operations

Method 2: 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∩C	A∪(B∩C)	A∪B	A∪C	(A∪B) ∩(A∪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

UMass Boston

Set Operations

- Method 3: Apply existing Set identities

- Take-Home message:

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

Exercises

- Question 1:
  Given a set A = {x, y, z} and a set B = {1, 2, 3, 4}, what is the value of $| 2^A \times 2^B |$?

- Question 2:
  Is it true for all sets A and B that $(A\times B)\cap(B\times A) = \varnothing$?
  Or do A and B have to meet certain conditions?

- Question 3:
  For any two sets A and B, if $A - B = \varnothing$ and $B - A = \varnothing$, can we conclude that A = B? Why or why not?

Exercises

- Question 1:

  Given a set A = {x, y, z} and a set B = {1, 2, 3, 4}, what is the value of $|2^A \times 2^B|$?

Answer:

$|2^A \times 2^B| = |2^A| \cdot |2^B| = 2^{|A|} \cdot 2^{|B|} = 8 \cdot 16 = 128$

75

Exercises

- Question 2:

  Is it true for all sets A and B that $(A \times B) \cap (B \times A) = \varnothing$? Or do A and B have to meet certain conditions?

Answer:

If A and B share at least one element x, then both $(A \times B)$ and $(B \times A)$ contain the pair (x, x) and thus are not disjoint.

Therefore, for the above equation to be true, it is necessary that $A \cap B = \varnothing$.

76

Exercises

Question 3:

For any two sets A and B, if $A - B = \emptyset$ and $B - A = \emptyset$, can we conclude that $A = B$? Why or why not?

Answer:

Proof by contradiction: Assume that $A \neq B$.

Then there must be either an element x such that $x \in A$ and $x \notin B$ or an element y such that $y \in B$ and $y \notin A$.

If x exists, then $x \in (A - B)$, and thus $A - B \neq \emptyset$.

If y exists, then $y \in (B - A)$, and thus $B - A \neq \emptyset$.

This contradicts the premise $A - B = \emptyset$ and $B - A = \emptyset$, and therefore we can conclude $A = B$.

77

Functions

Chapter 2.3 in the textbook

78

Functions

- A function f from a set A to a set B is an assignment of exactly one element of B to each element of A.
- We write: $f(a) = b$
  if b is the unique element of B assigned by the function f to the element a of A.

  If f is a function from A to B, we write f: $A \rightarrow B$
  (note: Here, "$\rightarrow$" has nothing to do with if… then)

Terminologies

If f: $A \rightarrow B$, we say that A is the domain of f and B is the codomain of f.

If $f(a) = b$, 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 elements of A.

We say that f: $A \rightarrow B$ maps A to B.

Functions

Let us take a look at the function $f: P \rightarrow C$ with

$P = \{Linda, Max, Kathy, Peter\}$

$C = \{Boston, New\ York, Hong\ Kong, Moscow\}$

$f(Linda) = Moscow$

$f(Max) = Boston$

$f(Kathy) = Hong\ Kong$

$f(Peter) = New\ York$

Here, the range of f is C.

Functions

- Let us re-specify f as follows:

$f(Linda) = Moscow$

$f(Max) = Boston$

$f(Kathy) = Hong\ Kong$

$f(Peter) = Boston$

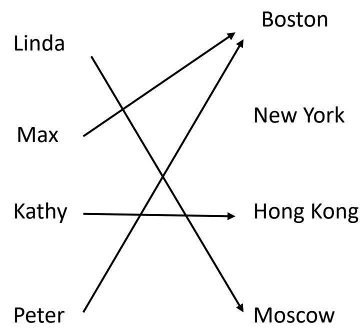
What is its range? {Moscow, Boston, Hong Kong}

- Is f still a function? yes

Functions

- Other ways to represent f:

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



Functions

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

  $f: \mathbb{R} \rightarrow \mathbb{R}$

  $f(x) = 2x$

- This leads to:

  $f(1) = 2$

  $f(3) = 6$

  $f(-3) = -6$

  …

Functions

- Let f_1 and f_2 be functions from A to $\mathbb{R}$.
- Then the sum and the product of f_1 and f_2 are also functions from A to $\mathbb{R}$ defined by:

$$(f_1 + f_2)(x) = f_1(x) + f_2(x)$$
$$(f_1 f_2)(x) = f_1(x) f_2(x)$$

Example:

$f_1(x) = 3x,\ f_2(x) = x + 5$

$(f_1 + f_2)(x) = f_1(x) + f_2(x) = 3x + x + 5 = 4x + 5$

$(f_1 f_2)(x) = f_1(x) f_2(x) = 3x\,(x + 5) = 3x2 + 15x$

Functions

- We already know that the range of a function $f: A \to B$ 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

- Let us look at the following well-known function:
  $f(Linda) = Moscow$
  $f(Max) = Boston$
  $f(Kathy) = Hong\ Kong$
  $f(Peter) = Boston$

- What is the image of $S = \{Linda, Max\}$?
  $f(S) = \{Moscow, Boston\}$

- What is the image of $S = \{Max, Peter\}$?
  $f(S) = \{Boston\}$

UMass Boston

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 two distinct elements of A onto the same element of B.

UMass Boston

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?
- Whenever you want to prove something, first take a look at the relevant definition(s):

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

- Example:

  $f: \mathbb{R} \rightarrow \mathbb{R}$
  $f(x) = x^2$

- Disproof by counterexample:

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

Properties of Functions

- … and yet another example:
  $f: R \to R$
  $f(x) = 3x$

- One-to-one: $\forall x, y \in A\ (f(x) = f(y) \to x = y)$
  To show: $f(x) \neq f(y)$ whenever $x \neq y$
  $x \neq y$
  $\Leftrightarrow 3x \neq 3y$
  $\Leftrightarrow f(x) \neq f(y)$,
- so if $x \neq y$, then $f(x) \neq f(y)$, that is, f is one-to-one.

Properties of Functions

- A function $f: A \to B$ with $A, B \subseteq \mathbb{R}$ is called strictly increasing, if $\forall x, y \in A\ (x < y \to f(x) < f(y))$,
- and strictly decreasing, if $\forall x, y \in A\ (x < y \to f(x) > f(y))$.

- Obviously, a function that is either strictly increasing or strictly decreasing is one-to-one.

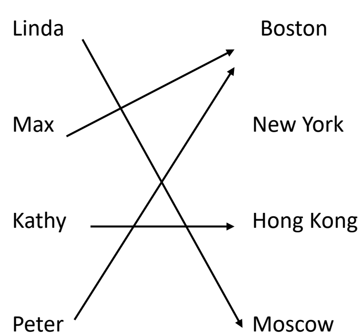
Properties of Functions

- A function $f: A \rightarrow B$ 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 $f: A \rightarrow B$ 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

Examples:

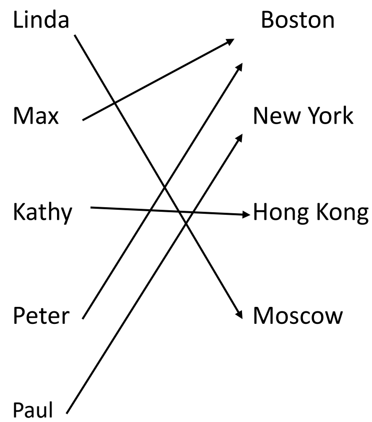
In the following examples, we use the arrow representation to illustrate functions $f: A \rightarrow B$.
In each example, the complete sets A and B are shown.



Is f injective?
No.
Is f surjective?
No.
Is f bijective?
No.

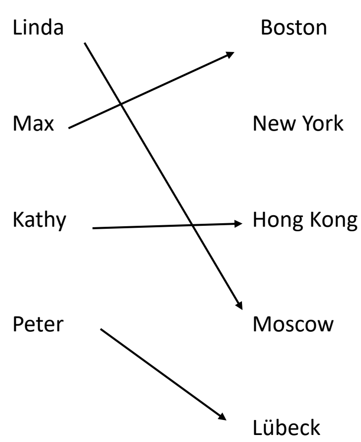
Properties of Functions

- Is f injective?
  - No.
- Is f surjective?
  - Yes.
- Is f bijective?
  - No.



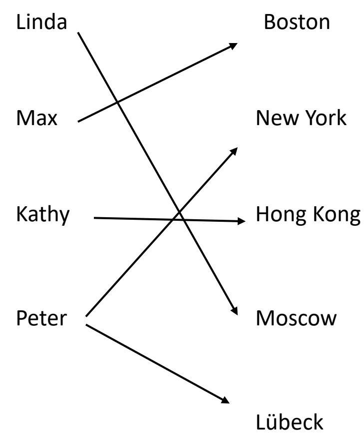
Properties of Functions

- Is f injective?
  - Yes.
- Is f surjective?
  - No.
- Is f bijective?
  - No.



Properties of Functions

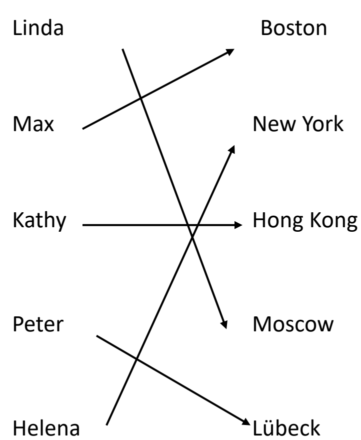
- Is f injective?
  - No! f is not even a function!



97

Properties of Functions

- Is f injective?
  - Yes.
- Is f surjective?
  - Yes.
- Is f bijective?
  - Yes.



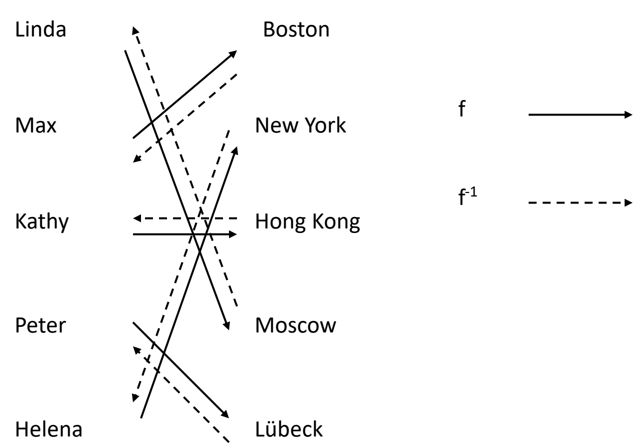
98

Inversion

- An interesting property of bijections is that they have an inverse function.

- The inverse function of the bijection $f: A \rightarrow B$ is the function $f^{-1}: B \rightarrow A$ with $f^{-1}(b) = a$ whenever $f(a) = b$.

Inversion



Inversion

Example:

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

Clearly, f is bijective.

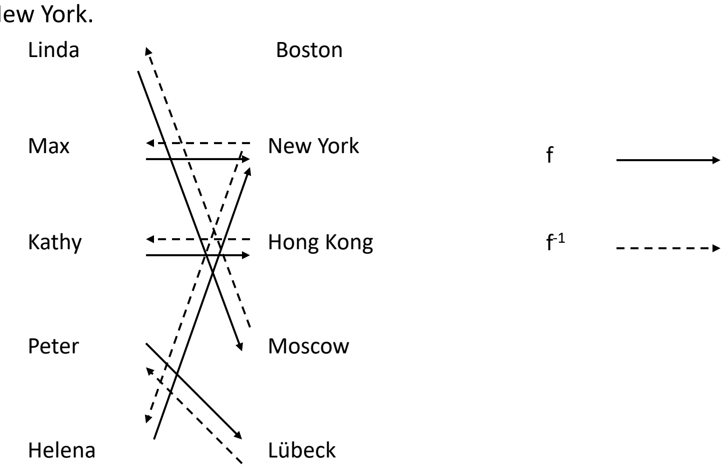
The inverse function f^{-1} is given by:

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}: $C \rightarrow P$ is no function, because it is not defined for all elements of C and assigns two images to the pre-image New York.



Composition

The **composition** of two functions $g: A \to B$ and $f: B \to C$, 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:$\mathbb{R} \to \mathbb{R}$, g: $\mathbb{R} \to \mathbb{R}$

(f ∘ g)(5) = f(g(5)) = f(15) = 105 – 4 = 101

(f ∘ 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 $i(x) = x$.

The Graphs of Functions

- The graph of a function $f: A \to B$ 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.

Example: The graph of the function $f(x) = 2n + 1$ and the function $f(x) = x^2$ when n is an interger

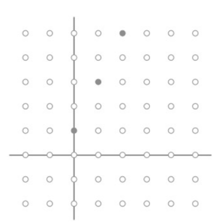


FIGURE 8 **The graph of $f(n) = 2n + 1$ from Z to Z.**

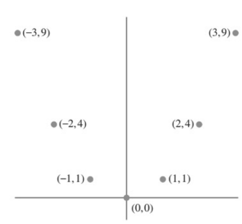


FIGURE 9 **The graph of $f(x) = x^2$ from Z to Z.**

Floor and Ceiling Functions

The floor and ceiling functions map the real numbers onto the integers ($\mathbb{R} \rightarrow \mathbb{Z}$).

The floor function assigns to $r \in \mathbb{R}$ the largest $z \in \mathbb{Z}$ with $z \leq r$, denoted by $\lfloor r \rfloor$.

- Examples: $\lfloor 2.3 \rfloor = 2, \lfloor 2 \rfloor = 2, \lfloor 0.5 \rfloor = 0, \lfloor -3.5 \rfloor = -4$

The ceiling function assigns to $r \in \mathbb{R}$ the smallest $z \in \mathbb{Z}$ with $z \geq r$, denoted by $\lceil r \rceil$.

- Examples: $\lceil 2.3 \rceil = 3, \lceil 2 \rceil = 2, \lceil 0.5 \rceil = 1, \lceil -3.5 \rceil = -3$

Sequences

- Sequences represent ordered lists of elements.
- A sequence is defined as a function from a subset of $\mathbb{N}$ 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.

Example:

subset of $\mathbb{N}$:	1	2	3	4	5	…
S:	2	4	6	8	10	…

Sequences

- We use the notation $\{a_n\}$ to describe a sequence.
- Important: Do not confuse this with the {} used in set notation.
- It is convenient to describe a sequence with an **equation**.
- For example, the sequence on the previous slide can be specified as $\{a_n\}$, where $a_n = 2n$.

The Equation Game

What are the equations that describe the following sequences $a_1, a_2, a_3, \ldots$?

1, 3, 5, 7, 9, …	$a_n = 2n - 1$
-1, 1, -1, 1, -1, …	$a_n = (-1)^n$
2, 5, 10, 17, 26, …	$a_n = n^2 + 1$
0.25, 0.5, 0.75, 1, 1.25 …	$a_n = 0.25n$
3, 9, 27, 81, 243, …	$a_n = 3^n$