INTRODUCTION

Discrete Math I – MTSC 213

Delaware State University

Discrete Math Introduction

- In discrete math we are mainly concerned with integers
- Integer arithmetic, puzzles, games, digital clocks involve discrete math
- Continuous math, calculus, rates of change are not related to discrete math

Discrete Math Introduction

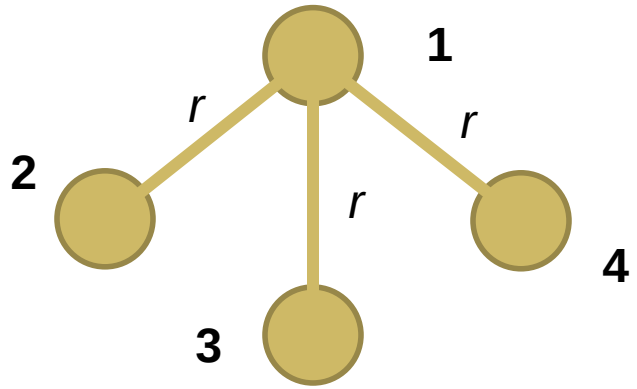
- Topics of interest:
- Series of integers

$$432 = 10^2 + 10^2 + 10^2 + 10^2 + 10^1 + 10^1 + 10^1 + 10^0 + 10^0 = 2^8 + 2^7 + 2^5 + 2^4$$

- Repeated experiments (coin flip)

$$HHHHHTHTHHTTTHHTHTTTHTTT$$

- Sets of elements
- Graph theory (social networks, world wide web)



Discrete Math Significance

- Continuous mathematics serve as the foundation of *physics and engineering*
- Discrete mathematics serve as the foundation of *computer science*
- Discrete mathematics deal with digital logic (true/false, 0/1)

LOGIC

Discrete Math I – MTSC 213

Delaware State University

Introduction

- In discrete math we are mainly concerned with integers
- Calculus deals with real numbers
- Every area of mathematics deals with concepts and topics specific to this area
- Often times, relationships between concepts is the topic of our study
- These relationships are expressed as statements
- Verifying statements is accomplished by using methods of proof
- To understand methods of proof we need to know the concept of sets and logic

Statements

- Statements may be considered the ‘building blocks’ of logic
- In mathematics we encounter and use them very often
- Sometimes we are asked to verify if they are true

Sentences

- In English grammar we have the following types of sentences
  - Declarative, something is being declared or asserted
  - Interrogative, a question is asked
  - Imperative, a command is given
  - Exclamatory, in which an emotion is expressed

Definition: Statement

A statement is a declarative sentence that is either true or false but not both.

Truth Values

- Every statement has a truth value that is either true (T) or false (F)
- Interrogative, imperative or exclamatory statements do not have a truth value

Example: Statements and truth values

Classify the following mathematical sentences as declarative, interrogative, imperative or exclamatory. Which declarative sentences are statements and which statements are true?

1. Is it true that $\frac{-9}{3} + \frac{4}{2} = \frac{-9+4}{3+2}$? Interrogatory sentence.
2. Multiply the numbers 2/3 and 9/10. Imperative sentence.
3. $1.414 \neq \sqrt{2}$. Declarative sentence, statement, true.
4. $\sqrt{(-3)^2} = -3$. Declarative sentence, statement, false.
5. What a difficult calculus exam! Exclamatory sentence.
6. $3x + 1 = 7$. Declarative, but not statement.

Open Sentences

Definition: Open sentence

An open sentence is a declarative sentence containing one or more variables whose truth or falseness depends on the values of these variables.

An open sentence containing a variable x is typically represented by $P(x)$. If x is an object that is a member of a collection of object, then **S** is called the domain of x and $P(x)$ is an open sentence over the domain of **S**.

Example: Open sentence

Consider the open sentence
$P(x) : 3x - 9 = 0$
where the element x represents a real number.
Thus
$P(3) : 3 \cdot 3 - 9 = 0$ is *true* and
$P(-3) : 3 \cdot (-3) - 9 = 0$ is *false*.

Discrete Math I - MTSC 213
Lecture 2

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 31, 2013

1 Negation, Conjuction and Disjunction

This section deals with operations between statements that produce new statements. We also discuss the truth values of the produced statements.

1.1 Truth Tables

A table that contains all possible assigments of truth values for one or more statements is called a *truth table*.
The tables for a single statement P or Q have two rows true (T), or false (F). If we consider both statements at the same time we have 2^2 combinations as seen in the third table.

P
T
F

Q
T
F

P	Q
T	T
T	F
F	T
F	F

1.2 Negation

Definition 1.1. The negation of a statement P is the statement
not P (or **It is not the case that** P)
written in symbols as $\sim P$.

The corresponding truth table is

P	$\sim P$
T	F
F	T

Table 1: Truth table of negation.

Example 1.1. For a real number x, the negation of the open sentence $P(x)$: $(x-2)^2 > 0$ is

$$\sim P(x) : (x-2)^2 \leq 0.$$

$P(x)$ becomes a statement for each specific real number x. $P(3)$ is true and $P(2)$ is false. $\sim P(3)$ is false and $\sim P(4)$ is true.

1.3 Conjunction

Definition 1.2. For two statements P and Q, the conjunction of P and Q is the statement
P **and** Q
denoted by $P \wedge Q$.

The truth table of a conjunction is

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Table 2: Truth table of conjunction.

1.4 Disjunction

Definition 1.3. For two statements P and Q, the disjunction of P and Q is the statement
P **or** Q
denoted by $P \vee Q$.

The truth table of a disjunction is

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Table 3: Truth table of disjunction.

1.5 Inclusive or Exclusive OR

The disjunction $P \vee Q$ is referred to as **inclusive or**. On the other hand the operator that is true when exactly one of P and Q is true, is called **exclusive or**.

Definition 1.4. For two statements P and Q, the **exclusive or** of P and Q is the statement
P **or** Q **but not both**
denoted by $P \oplus Q$.

The truth table of exclusive or is

P	Q	$P \oplus Q$
T	T	F
T	F	T
F	T	T
F	F	F

Table 4: Truth table of exclusive or.

Example 1.2. For an integer n, consider the two open sentences
$P(n) : n^3 + 2n$ is even and $Q(n) : n^2 - 4 < 0$.
The conjunction, disjunction and exclusive or of $P(n)$ and $Q(n)$ are the open sentences:
$P(n) \wedge Q(n) : n^3 + 2n$ is even and $Q(n) : n^2 - 4 < 0$.
$P(n) \vee Q(n) : n^3 + 2n$ is even or $Q(n) : n^2 - 4 < 0$.
$P(n) \oplus Q(n) : n^3 + 2n$ is even and $Q(n) : n^2 - 4 < 0$ but not both.
$P(1) \wedge Q(1)$ is false, while $P(1) \vee Q(1)$ is true. $P(3) \wedge Q(3)$ and $P(3) \vee Q(3)$ are false statements. Also, $P(0) \oplus Q(0)$ is false, while $P(1) \oplus Q(1)$ and $P(2) \oplus Q(2)$ are both true.

1.6 Compound Statements

The operations $\sim$, $\vee$, $\wedge$, $\oplus$ are called logical connectives. A compound statement is a statement constructed from one or more statements, called component statements, and one or more logical connectives. Of special interest are compound statements that have "equal" truth tables.

Definition 1.5 (Logical Equivalence)**.** Two compound statements R and S constructed from the same component statements are **logically equivalent** if R and S have the same truth value for all the combinations of truth values of their component statements. If R and S are logically equivalent then we write $R \equiv S$, while if R and S are not logically equivalent we write $R \not\equiv S$.

Theorem 1.6 (Commutative Laws)**.** *For every two statements P and Q, $P \wedge Q \equiv Q \wedge P$ and $P \vee Q \equiv Q \vee P$.*

P	Q	$P \wedge Q$	$Q \wedge P$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	F

P	Q	$P \vee Q$	$Q \vee P$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

Table 5: Truth table of exclusive or.

1.7 De Morgan's Laws

The De Morgan's Laws involve the logical connectives of negation, conjunction and disjunction.

Theorem 1.7 (De Morgan's Laws)**.** *For every two statements P and Q,*
(a) $\sim(P \vee Q) \equiv (\sim P) \wedge (\sim Q)$,
(b) $\sim(P \wedge Q) \equiv (\sim P) \vee (\sim Q)$.

Example 1.3. For a real number x, let $P(x) : x^2 - 8x + 15 = 0$.
(a) Use the word or to describe those real numbers x for which $P(x)$ is true.
(b) Use De Morgan's Laws to describe those real numbers x for which $P(x)$ is false.
(a) $P(x)$ is true when $x = 3$ or $x = 5$.
(b) $P(x)$ is false when $x \neq 3$ and $x \neq 5$.

Theorem 1.8. *For every statement P,*
$P \equiv \sim(\sim P)$.

This can be verified by use of the truth table.

P	$\sim P$	$\sim (\sim P)$
T	F	T
F	T	F

Table 6: Truth table of $\sim (\sim P)$.

1.8 Associative and Distributive Laws

As we know the associative and distributive laws hold true for the addition and multiplication of real numbers. Here we outline the logical equivalence of statements involving conjunction and disjunction.

Theorem 1.9. *Let P, Q and R be three statements. Then,*
*(a)**Associative Laws***
$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$ *and* $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$
*(b)**Distributive Laws***
$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$ *and* $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$.

These laws can be verified by truth tables (left as homework).

Discrete Math I - MTSC 213
Lecture 3

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 31, 2013

1 Implications

Definition 1.1. For two statements P and Q, the implication $P \to Q$ is commonly written as
If P, **then** Q.
An implication is also sometimes referred to as a **conditional**. The statement P in the implication $P \to Q$ is the **hypothesis** (or premise) of $P \to Q$, while Q is the conclusion (or consequence) of $P \to Q$.

In the truth table below we observe the following for $P \to Q$ between two statements P and Q:

- If the hypothesis P is false, then $P \to Q$ is true regardless of the truth value of Q;
- If the conclusion Q is true, then $P \to Q$ is true regardless of the truth value of P;
- $P \to Q$ is false, only when the hypothesis P is true and the conclusion Q is false.

Example 1.1. Determine the truth value of each of the following implications.
(a)If $2 + 3 = 5$, then $4 + 6 = 10$.

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

Table 1: Truth table of implication.

(b)If $4 + 6 = 10$, then $5 + 7 = 14$.
(c)If $5 + 7 = 14$, then $6 + 9 = 15$.
(d)If $8 + 11 = 21$, then $12 + 14 = 28$.

Answer
(a) if T then T. This is a true implication.
(b) if T then F. This is a false implication.
(c) if F then T. This is a true implication.
(b) if F then F. This is a true implication.■

Example 1.2. For a real number x, consider the two open sentences
$P(x) : x - 2 = 0$. and $Q(x) : x^2 - x - 2 = 0$.
Investigate for all real numbers x, the truth or falseness of the implication $P(x) \to Q(x)$: If $x - 2 = 0,$ then $x^2 - x - 2 = 0$.

Answer
$P(x)$ is true only when $x = 2$, so $P(2)$ is true. $Q(2)$ is also true, so $P(2) \to Q(2)$ is true. For $x \neq 2$ $P(x)$ is false, so $P(x) \to Q(x)$ is true, regardless of the truth value of $Q(x)$. So, $P(x) \to Q(x)$ is true $\forall x \in \mathbb{R}$.■

1.1 Stating implications in words

1.2 Converse of an implication

Definition 1.2. For statements (or open sentences) P and Q, the implication $Q \to P$ is called the converse of $P \to Q$.

$P \to Q$
If P, then Q
Q if P
P **implies** Q
P **only if** Q
P **is sufficient for** Q
Q **is necessary for** P

Table 2: Expressing an implication.

1.3 Contrapositive of an implication

Definition 1.3. For statements (or open sentences) P and Q, the contrapositive of implication $P \to Q$ is $(\sim Q) \to (\sim P)$.

Theorem 1.4. *For every two statements P and Q,*
$P \to Q \equiv (\sim Q) \to (\sim P)$.

Thus, an implication and its contrapositive are logically equivalent.

P	Q	$P \to Q$	$\sim Q$	$\sim P$	$(\sim Q) \to (\sim P)$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Table 3: Logical equivalence of an implication and its contrapositive.

Theorem 1.5. *For every two statements P and Q,*
$P \to Q \equiv (\sim P) \vee Q$.

We can show this using the truth table.

Theorem 1.6. *For every two statements P and Q,*
$\sim(P \to Q) \equiv P \wedge (\sim Q)$.

This can be verified as follows: $\sim(P \to Q) \equiv \sim((\sim P) \vee Q) \equiv (\sim(\sim P)) \wedge (\sim Q) \equiv P \wedge (\sim Q)$.■

P	Q	$P \to Q$	$\sim P$	$\sim P \vee Q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Table 4: $P \to Q \equiv (\sim P) \vee Q$.

Example 1.3. For an integer n, consider the open sentences
$P(n) : n$ is even. $Q(n) : n$ is not the sum of three odd integers.
(a) State $P(n) \to Q(n)$ in words.
(b) State $\sim (P(n) \to Q(n))$ in words using the phrase "it is not the case that".
(c) Use the previous theorem to restate $\sim (P(n) \to Q(n))$ in words.

Answer
(a) If n is even, then n is not the sum of three odd integers.
(b) It is not the case that if n is even, then n is not the sum of three odd integers.
(c) n is even, and n is the sum of three odd integers.■

Discrete Math I - MTSC 213
Lecture 4

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 31, 2013

1 Biconditionals

1.1 If and only if

Definition 1.1. For two statements P and Q, the **biconditional** of P and Q is the conjunction of the implication $P \to Q$ and its converse $Q \to P$. The biconditional of P and Q is denoted by $P \leftrightarrow Q$. So $P \leftrightarrow Q$ is the statement $(P \to Q) \wedge (Q \to P)$.

The biconditional $P \leftrightarrow Q$ is expressed as
P **if and only if** Q
or
P **is necessary and sufficient for** Q.

The truth table of the biconditional statement can be evaluated as follows

P	Q	$P \to Q$	$Q \to P$	$P \leftrightarrow Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Table 1: Truth table of biconditional.

Example 1.1. Consider the statements:
P: I will receive an A on the exam.
Q: I study for at least 10 hours.
The biconditional of P and Q is
$P \leftrightarrow Q$: I will receive an A on the exam **if and only if** I study for at least 10 hours.

Answer The statement $P \leftrightarrow Q$ is true when either
(a) I study for at least 10 hours and receive an A on the exam or
(b) I do not study for at least 10 hours and do not receive an A on the exam.■

The use of the expression **if and only if** for the biconditional can be explained as follows:
The biconditional $P \leftrightarrow Q$ is defined as $(P \to Q) \wedge (Q \to P)$.
By use of the commutative law we have
$(P \to Q) \wedge (Q \to P) \equiv (Q \to P) \wedge (P \to Q)$.
$Q \to P$ can be expressed as P **if** Q.
$P \to Q$ can be expressed as P **only if** Q.

Therefore $(Q \to P) \wedge (P \to Q)$ can be expressed as
P **if** Q **and** P **only if** Q, or
P **if and only if** Q.
Frequently **if and only if** is abbreviated as **iff**.
In addition, $P \leftrightarrow Q$ can be expressed as, P **is necessary and sufficient for** Q.

Example 1.2. For an integer n, consider the open sentences
$P(n) : (n-1)^2 = 0$ and $Q(n) : 7n - 3 = 0$. The biconditional $P \leftrightarrow Q$ is
$P \leftrightarrow Q : (n-1)^2 = 0$ if and only if $7n - 3 = 0$
Investigate the truthness or falseness of the biconditional for various integers.

Answer
$P(n)$ is true only when $n = 1$. $Q(1)$ is false, so $P \leftrightarrow Q$ is false for $n = 1$. For $n \neq 1$, $P(n)$ is false, and $Q(n)$ is also false for all integers, therefore $P \leftrightarrow Q$ is true for $n \neq 1$.■

Example 1.3. Suppose that P and Q are two statements such that $P \to Q$ is true and $Q \to P$ is false. Please investigate the truth value of $P \leftrightarrow Q$.

Answer

The biconditional $P \leftrightarrow Q$ is defined as $(P \rightarrow Q) \wedge (Q \rightarrow P)$. Since $Q \rightarrow P$ is false, $P \leftrightarrow Q$ is false.■

Discrete Math I - MTSC 213
Lecture 5

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 31, 2013

1 Tautologies and Contradictions

Definition 1.1 (Tautology)**.** A compound statement is a **tautology** if it is true for all possible combinations of truth values of its component statements.

Definition 1.2 (Contradiction)**.** A compound statement is a **contradiction** if it is false for all possible combinations of truth values of its component statements.

Therefore, a compound statement S is a tautology if and only if its negation $\sim S$ is a contradiction.

For every statement P, the statement $P \vee (\sim P)$ is a tautology, while $P \wedge (\sim P)$ is a contradiction. This is verified by the following truth table.

P	$\sim P$	$P \vee (\sim P)$	$P \wedge (\sim P)$
T	F	T	F
F	T	T	F

Table 1: Truth table for a tautology and a contradiction.

Example 1.1. Because $P \vee (\sim P)$ is a tautology and $P \wedge (\sim P)$ is a contradiction for every statement P, if we let
$P(n) : P$ is even.
where n is an integer, then

$P \vee (\sim P) : n$ is even or n is odd
is a true statement for every integer n; while
$P \wedge (\sim P) : n$ is even and n is odd
is a false statement for every integer n.

Further, for any two logically equivalent statements R and S, the biconditional $R \leftrightarrow S$ is a tautology.

1.1 Modus Ponens and Modus Tollens

Example 1.2. Let P and Q be two statements. Show that $(P \wedge (P \rightarrow Q)) \rightarrow Q$ is a tautology.

Answer
We use the truth table to verify that $(P \wedge (P \rightarrow Q)) \rightarrow Q$ is a tautology.■

P	Q	$P \rightarrow Q$	$P \wedge (P \rightarrow Q)$	$(P \wedge (P \rightarrow Q)) \rightarrow Q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Table 2: Truth table of modus ponens.

The tautology $(P \wedge (P \rightarrow Q)) \rightarrow Q$ is called **modus ponens** (mode that affirms the hypothesis) in logic.
The tautology $(P \rightarrow Q) \wedge (\sim Q)) \rightarrow (\sim P)$ is called **modus tollens** (mode that denies the conclusion).

Example 1.3. Let P and Q be two statements. Show that $(P \rightarrow Q) \wedge (\sim Q)) \rightarrow (\sim P)$ is a tautology.

Answer
We use the truth table to prove that $(P \rightarrow Q) \wedge (\sim Q)) \rightarrow (\sim P)$ is a tautology.■

P	Q	$P \to Q$	$\sim Q$	$(P \to Q) \wedge (\sim Q))$	$\sim P$	$((P \to Q) \wedge (\sim Q)) \to (\sim P)$
T	T	T	F	F	F	T
T	F	F	T	F	F	T
F	T	T	F	F	T	T
F	F	T	T	T	T	T

Table 3: Truth table of modus tollens.

Discrete Math I - MTSC 213
Lecture 6

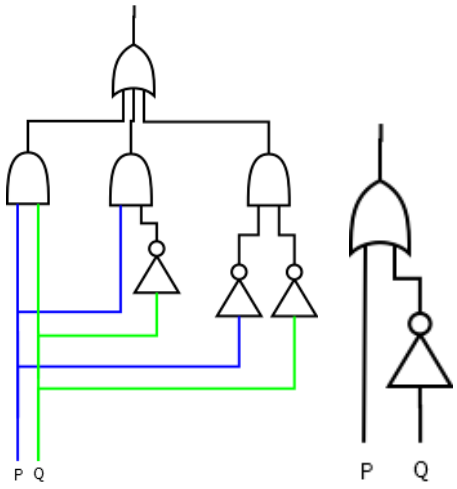
Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 31, 2013

Homework

Exercise 1

Use rules of logic to show that each pair of circuits in 1 have the same input/output table. (Find the Boolean expressions for the circuits and show that they are logically equivalent, when regarded as statement forms.)



a b

Figure 1:

Exercise 2

For the circuits corresponding to the Boolean expressions below there is an equivalent circuit with at most two logic gates. Find such a circuit.

1. $(P \wedge Q) \vee ((\sim P) \wedge Q) \vee ((\sim P) \wedge (\sim Q))$
2. $((\sim P) \wedge (\sim Q)) \vee ((\sim P) \wedge Q) \vee (P \wedge (\sim Q))$

Discrete Math I - MTSC 213
Lecture 6

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 31, 2013

1 Application of Logic: Digital Circuits

1.1 Introduction

One wide-spread application of logic theory can be found in the domain of digital electronics. In the late 1930's Claude Shannon, then a young graduate student of M.I.T. noticed an analogy between the operations of switching devices, such as telephone switching circuits, and the operations of logical connectives. He used this analogy to solve problems of circuit design. This was the subject of his master's thesis, which was published in 1938.

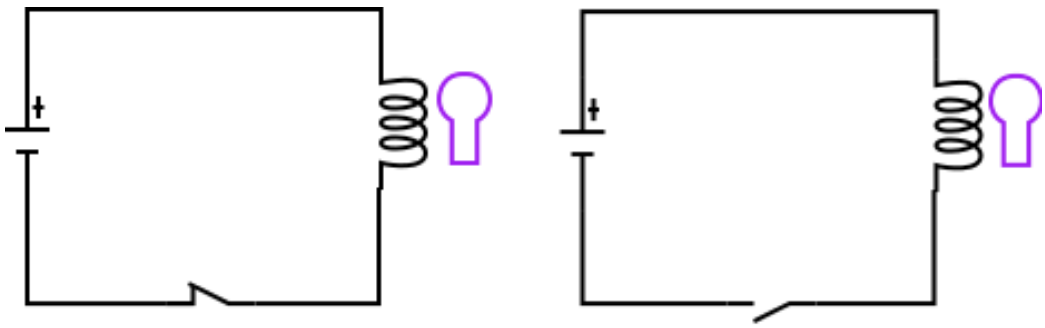


Figure 1: Circuit example with a battery, switch and light bulb. The switch has two states: open (off) and closed (on).

In figure 1, is displayed a simple circuit consisting of a battery, a light bulb and a switch. When the switch is closed, current flows from one terminal to the other. The light bulb turns on, if and only if, current flows through it. This happens, if and only if, the switch is closed.

Now we consider the more complicated circuits of switches connected in series, or in parallel (figure 2).

In the first case -switches in series- current flows, if and only if, both switches P and Q are closed.

In the second case -switches in parallel- the current flows, if and only if, either P, or switch Q is closed.

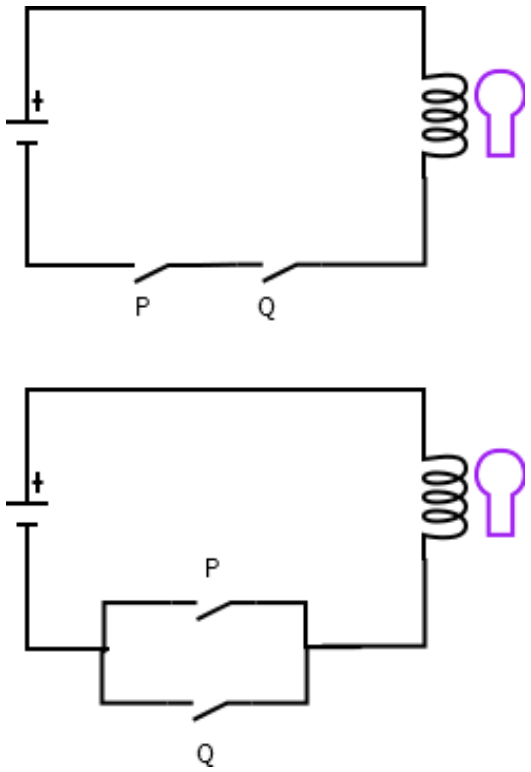


Figure 2: Switches connected in series, and in parallel.

The possible states of the two circuits are described in tables 1 and 2.

We note that, if we replace **closed** and **on** by **T**, and if we replace **open** and **off** by **F**, then our tables become the truth tables for a **conjunction** (table 1), and **disjunction** (table 2).

Table 1: Switches in series.

P	Q	State
closed	closed	on
closed	opened	off
opened	closed	off
opened	opened	off

Table 2: Switches in parallel.

P	Q	State
closed	closed	on
closed	opened	on
opened	closed	on
opened	opened	off

Later on, in the 1940's and 1950's mainly driven by the invention of electronic transistors, the switches were replaced by electronic devices, with the physical states of **closed** and **open** replaced by **high voltage** and **low voltage**. The breakthrough in electronics led to the development of digital systems, such as digital electronic computers, electronic traffic light systems, electronic calculators, etc.

Electronic engineers continue to use the language of logic when they refer to signals. They use symbols 1 and 0 instead of true and false. The symbols 0 and 1 are called, binary digits, or bits. Statistician John Tukey introduced this terminology.

1.2 Black boxes and gates

To simplify the design and analysis of electronic circuits, electronic and computer engineers consider basic circuits as black boxes. The detailed description of the circuit is often ignored and the interest is focused on the input and output signals of this box. In this manner the operation of a black box is summarized by the input/output table that lists all possible input and output signals.

The design of more complicated circuits is accomplished by connecting simple components, known as gates. Three frequently used digital components are the NOT-, AND- and OR- gates (figure 3 and table 3).

A NOT-gate receives one input signal and produces one output signal. Its function corresponds to the logical connective of negation $\sim$.

An AND-gate receives two input signals and produces one output signal. Its function corresponds to the logical connective of conjunction $\wedge$.

An OR-gate receives two input signals and produces one output signal. Its function corresponds to the logical connective of disjunction $\vee$.

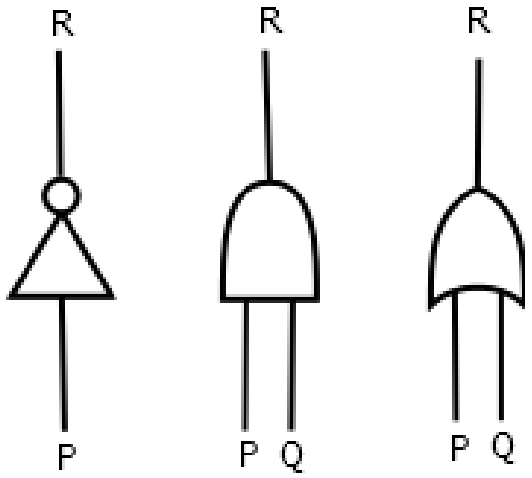


Figure 3: Fundamental NOT-, AND- and OR-gates from left to right.

Table 3: Logic of NOT-, AND-, OR-gates from left to right.

P	R
1	0
0	1

P	Q	R
1	1	1
1	0	0
0	1	0
0	0	0

P	Q	R
1	1	1
1	0	1
0	1	1
0	0	0

Gates can be connected in different ways to create combinatorial circuits whose operation is also described by an input/output table.

1.3 Input/output table for a circuit

For specific input signals we can determine the output signals of digital circuits by tracing the changes of input signals from one gate to the next. Figure 4 produces the input/output table 4.

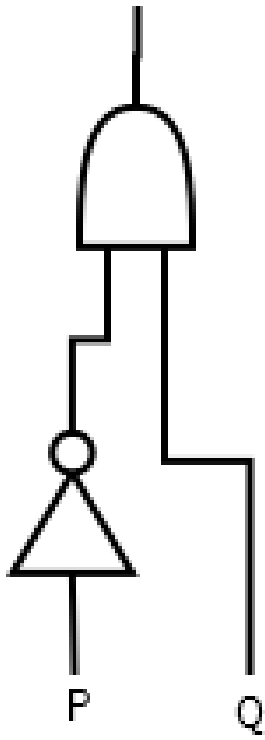


Figure 4: Find the output signals from input signals $\{P, Q\} = \{0, 1\}$ and $\{P, Q\} = \{1, 1\}$.

Similarly we can construct the input/output table for a circuit.

Table 4: Input/output table for circuit in figure 4.

P	Q	R
1	1	0
1	0	0
0	1	1
0	0	0

1.4 The Boolean expression corresponding to a circuit

One of the founders of symbolic logic was George Boole. In his honor, variables and statements that can take one of only two values are called Boolean

variables. Expressions derived from Boolean variables and logical connectives are also Boolean expressions.

So if we are given a circuit consisting of logical gates we can obtain the Boolean expression by tracing the gates operation applied to the input variables.

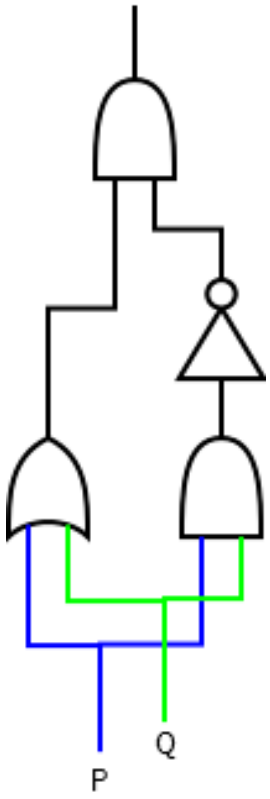


Figure 5: Find the Boolean expression for this circuit.

The Boolean expression of circuit in figure 5 is
$(P \vee Q) \wedge (\sim (P \wedge Q))$.

This is the expression for exclusive OR: P or Q but not both.

1.5 The circuit corresponding to a Boolean expression

Given a Boolean expression, we can design a circuit. Going from inner to outer Boolean terms, corresponds to designing gates from left to right.

For example, given the Boolean expression $(\sim P \wedge Q) \vee (\sim Q)$, we design the circuit of figure 6.

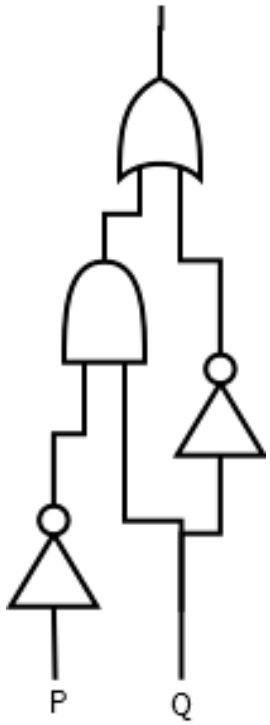


Figure 6: The circuit corresponding to $(\sim P \wedge Q) \vee (\sim Q)$.

1.6 Finding a circuit that corresponds to a given input/output table

We can achieve this by the following steps:

- Identify each row for which the output is 1.
- For each such row, construct an AND expression so that it produces 1 for the exact combination of variables and 0 for all other combinations.
- Connect the previous expressions using OR-operations.

Definition 1.1 (Recognizer)**.** A recognizer is a circuit that outputs 1 for exactly one particular combination of input signals and outputs 0's for all other combinations.

Let's consider the example of the input/output table of figure 6 that is displayed in table 5.

Table 5: Input/output for circuit in figure 6.

P	Q	R
1	1	0
1	0	1
0	1	1
0	0	1

We can connect several recognizers in parallel to produce the input/output table 5, as explained before. The produced circuit is depicted in figure 7.

1.7 Simplifying combinatorial circuits

From the previous example we conclude that the circuits of figure 6 and figure 7 have the same input/output table 5. These two circuits are called equivalent.

Definition 1.2. Two digital logic circuits are equivalent if, and only if, their input/output tables are identical.

In several cases we would like to simplify a combinatorial circuit and use fewer gates. We can achieve this by application of rules of logic.

For example, let's simplify the circuit in figure 8.

We first define the Boolean expression, then apply rules of logic to simplify it. In the end we can design the simplified circuit from the final expression.

The Boolean expression is $((P \wedge (\sim Q)) \vee (P \wedge Q)) \wedge Q$.

So, we have: $((P \wedge (\sim Q)) \vee (P \wedge Q)) \wedge Q \equiv (P \wedge (Q \vee (\sim Q))) \wedge Q \equiv (P \wedge t) \wedge Q \equiv P \wedge Q$.

We conclude that the circuit of figure 8 is logically equivalent to an AND-gate and can be significantly simplified.■

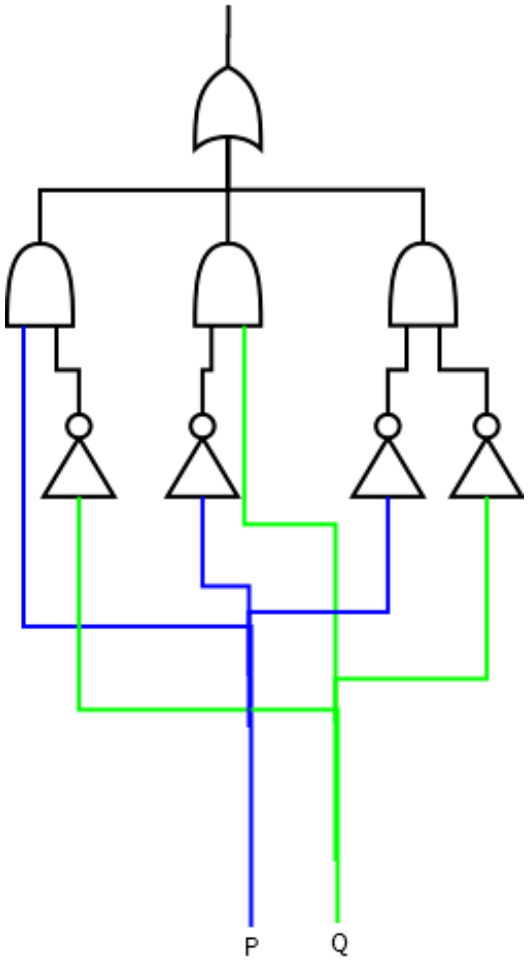


Figure 7: Circuit derived from input/output table.

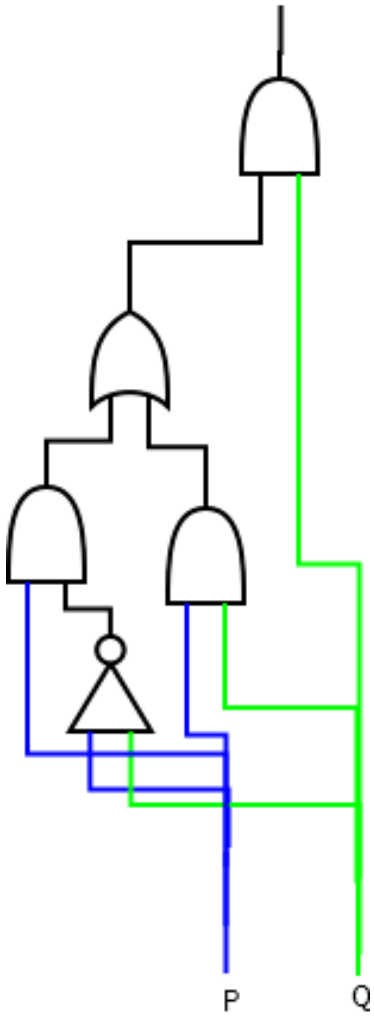


Figure 8: Simplify the circuit.

Discrete Math I - MTSC 213
Lecture 7

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 31, 2013

1 Sets - Sets and Subsets

The concept of a set is fundamental in mathematics. Set theory is called the field of study that deals with sets and their properties.

1.1 Sets and Subsets

A set is a collection of objects. The objects of a set are called the elements of a set. We usually denote sets by capital letters, e.g. A, S, X and the elements by lower case letters, e.g., x, y, z. Sets with relatively few elements can be denoted by roster description, e.g., $S = \{x, y, z\}$. If b is an element of A, we write $b \in A$, otherwise $b \notin A$.

Two sets A and B are equal, denoted by $A = B$, if they consist of exactly the same elements. The order in which the elements are listed does not matter, e.g.,

$S = \{x, y, z\} = \{y, x, z\} = \{y, z, x\}$.

The set $A = \{1, 2, 3, ..., 50\}$ consists of integers from 1 to 50, and the set $S = \{1, 3, 5, ...\}$ consists of positive odd numbers. We use the three dots ..., called an ellipsis to symbolize "and so on (up to)".

If a set contains no elements, it is called the empty set, null set, or void set. The empty set is denoted by $\emptyset$, thus. $\emptyset = \{\}$. A non empty set contains at least one element. For a finite set A, we denote the number of the elements of A by $|A|$, which is called the cardinality of a set.

Example 1.1. Because the sets $\emptyset$ and $\{\emptyset\}$ do not consist of the same elements, $\{\emptyset\} \neq \emptyset$. The set $\{\emptyset\}$ has one element, so $|\{\emptyset\}| = 1$. The set $\emptyset$ has no elements, so $|\emptyset| = 0$.

Example 1.2. The set $A = \{1, \{1, 3\}, \emptyset, \alpha\}$ has four elements. Two of these elements are sets, i.e. $\{1, 3\}$, and $\emptyset$. Because A has 4 elements, the cardinality $|A| = 4$.

1.2 Well-known Sets of Numbers

Some well known infinite sets are:

The set of integers $\{..., -2, -1, 0, 1, 2, ...\}$ is denoted by $\mathbb{Z}$.

The set of positive integers, or natural numbers is denoted by $\mathbb{N}$.

The set of rational number is denoted by $\mathbb{Q}$.

The set of real numbers is denoted by $\mathbb{R}$.

Other useful notations:

For a set S, let $P(x)$ denote an open sentence involving elements $x \in S$. Then

$A = \{x \in S : P(x)\}$

describes the set of those elements of S for which $P(x)$ is true. When S is known we can also use

$A = \{x : P(x)\}$.

The colon in these expressions can be interpreted as "such as". A vertical line can be used for this too. For example,

$A = \{x \in S : P(x)\} = \{x \in S | P(x)\}$.

Example 1.3. List the elements of the following sets:
$A = \{x \in \mathbb{R} : x^2 - x - 6 = 0\}$
$B = \{x \in \mathbb{R} : x^2 + 1 = 0\}$.

Answer The set A represents the set of solutions of $x^2 - x - 6 = 0$. Factorization produces $x^2 - x - 6 = (x + 2)(x - 3)$, so $A = \{-2, 3\}$. On the other hand, $x^2 + 1 = 0$ has no real number solution so $B = \emptyset$.

1.3 Subsets

Definition 1.1 (Subset)**.** A set A is called a subset of a set B written $A \subseteq B$, if every element of A also belongs to B.

According to the above definition, $\mathbb{N} \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{Q}$, and $\mathbb{Q} \subseteq \mathbb{R}$.

Definition 1.2 (Proper subset)**.** A set A is a proper subset of a set B written $A \subset B$, if $A \subseteq B$ but $A \neq B$.

We also observe that $\mathbb{N} \subset \mathbb{Z}$, $\mathbb{Z} \subset \mathbb{Q}$, and $\mathbb{Q} \subset \mathbb{R}$.

Example 1.4. For the sets $A = \{a, b, c\}$ and $C = \{a, b, c, d, e\}$, find all sets B such that $A \subset B \subset C$.

Answer The only subsets that satisfy this condition are $\{a, b, c, d\}$ and $\{a, b, c, e\}$.

1.4 Venn Diagrams

Venn diagrams are used to depict sets, subsets and their relations. A rectangle may represent the universal set and closed curves are drawn to represent the sets. The elements enclosed by the curves belong to the corresponding sets. Figure 1 shows an example of a Venn diagram.

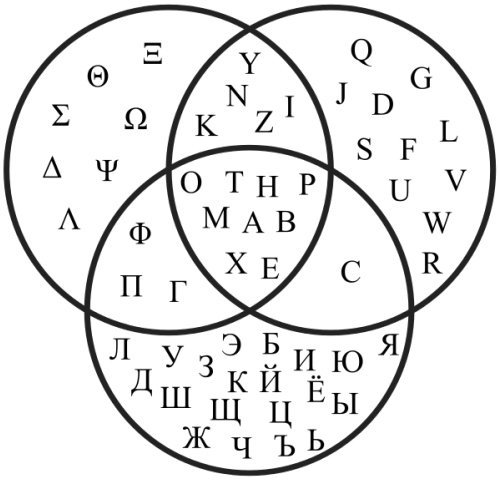


Figure 1: Venn diagram showing Greek, Latin and Cyrillic letters (source: wikipedia).

Example 1.5. Figure 2 displays the Venn diagram of sets A and B.
We note that the elements

- 5, -3, 8, 9, 25 belong to A but not to B

- 3, 17, -12, 19 belong to B but not to A

- 13, 2, -7 belong to both A and B

- -6 belongs to neith A nor B.

So $A = \{-7, -3, 2, 5, 8, 9, 13, 25\}$, $B = \{-12, -7, 2, 3, 13, 17, 19\}$ and the universal set is $U = \{-12, -7, -6, -3, 2, 3, 5, 8, 9, 13, 17, 19, 25\}$.

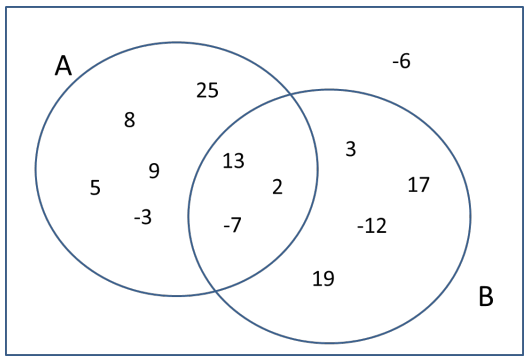


Figure 2:

Example 1.6. Give an example of three sets A, B and C such that $A \in B$, $A \subset B$ and $B \in C$.

Answer
We first choose $A = \{2, 5\}$. Then because $A \in B$ and $A \subset B$, we choose $B = \{A, 2, 5\} = \{\{2, 5\}, 2, 5\}$. We also have to satisfy $B \in C$, so we set $C = \{B, 13\} = \{\{\{2, 5\}, 2, 5\}, 13\}$.

1.5 Power Sets

Definition 1.3 (Power set)**.** The set of all subsets of a set A is called the power set of A and is denoted by $\mathcal{P}(A)$. Thus
$\mathcal{P}(A) = \{B : B \subseteq A\}$.

Theorem 1.4. *If A is a set with $|A| = n$, where n is a nonnegative integer, then*
$|\mathcal{P}(A)| = 2^n$.

Example 1.7. For $A = \{x \in \mathbb{Z} : |x| \leq 3\}$, how many elements are in $\mathcal{P}(A)$?

Answer

Because $A = \{-3, -2, -1, 0, 1, 2, 3\}$, $|A| = 7$. Because of Theorem 1.4, $|\mathcal{P}(a)| = 2^7 = 128$.

Discrete Math I - MTSC 213
Lecture 8

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 14, 2013

1 Set Operations and their Properties

1.1 Intersections and Unions

Definition 1.1 (Intersection)**.** Let A and B be two sets. The intersection $A \cap B$ of A and B is the set of elements belonging to both A and B. Thus $A \cap B = \{x : x \in A \text{ and } x \in B\}$.

Definition 1.2 (Union)**.** Let A and B be two sets. The union $A \cup B$ of A and B is the set of elements belonging to at least one of A and B. Thus $A \cup B = \{x : x \in A \text{ or } x \in B\}$.

Because an element belongs to $A \cup B$ if it belongs to $A \cap B$, it follows that
$A \cap B \subseteq A \cup B$.

Example 1.1. For the sets $C = \{1, 2, 4, 5\}$ and $D = \{1, 3, 5\}$
$C \cap D = \{1, 5\}$ and $C \cup D = \{1, 2, 3, 4, 5\}$.

Theorem 1.3. *For every three sets A, B and C:*

- *Commutative Laws: $A \cap B = B \cap A$ and $A \cup B = B \cup A$*
- *Associative Laws: $(A \cap B) \cap C = A \cap (B \cap C)$ and $(A \cup B) \cup C = A \cup (B \cup C)$*

- *Distributive Laws:* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *and* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Two of the above set properties can be verified by using properties of logic. We can verify $A \cap B = B \cap A$ by showing that $A \cap B$ $B \cup A$ have the same elements.

$x \in A \cap B \equiv x \in A$ and $x \in B$
$\equiv x \in B$ and $x \in A$
$\equiv x \in B \cap A$.

In general, for $n \geq 2$, the intersection of sets $A_1, A_2, ..., A_n$ is
$\cup_{i=1}^{n} A_i = A_1 \cup A_2 \cup ... \cup A_n = x : x \in A_i$ for every i with $1 \leq i \leq n$;
and the union is
$\cap_{i=1}^{n} A_i = A_1 \cap A_2 \cap ... \cap A_n = x : x \in A_i$ for some i with $1 \leq i \leq n$.

Example 1.2. Let $A_1 = \{1, 2\}$, $A_2 = \{2, 3\}$, ..., $A_{10} = \{10, 11\}$. That is, $A_i = \{i, i + 1\}$ for $i = 1, 2, ..., 10$. Then,

$A_1 \cap A_2 \cap ... \cap A_{10} = \emptyset$
and
$A_1 \cup A_2 \cup ... \cup A_{10} = \{1, 2, 3, ..., 11\}$.

Definition 1.4. Two sets A and B are disjoint if they have no elements in common, that is, if $A \cap B = \emptyset$. A collection of sets is set to be pairwise disjoint if every two distinct sets in the collection are disjoint.

Example 1.3. The set of even integers and the set of odd integers are disjoint. The set of negative rational numbers and the sets of irrational numbers are disjoint.

1.2 Difference and Symmetric Difference

Definition 1.5. The difference $A - B$ of two sets A and B is defined as $A - B = \{x : x \in A$ and $x \notin B\}$.

Sometimes, $A - B$ may denoted also as $A \setminus B$

Definition 1.6. The symmetric difference $A \oplus B$ of two sets A and B is defined by:
$A \oplus B = (A - B) \cup (B - A)$.

From this definition it follows that
$x \in A \oplus B = x \in A \oplus x \in B$.

We can interpret the symmetric difference using rules of logic. So, for an element $A \oplus B$ we must have $x \in A - B$ or $x \in B - A$. If $x \in A - B$, then $x \in A$ and $x \notin B$. Also, if $x \in B - A$, then $x \in B$ and $x \notin A$. So, if $x \in A \oplus B$ then x belongs to exactly one of A or B. This is equivalent to the logical connective of exclusive or. This interpretation can be denoted as $x \in A \oplus B \equiv (x \in A) \oplus (x \in B)$. The first $\oplus$ symbol denotes the symmetric difference, while the second $\oplus$ symbol denotes the "exclusive or" between two statements.

We can use Venn diagrams to show that
$A \oplus B = (A \cup B) - (A \cap B)$ (left as an exercise).

It worth noting that even though Venn diagrams may suggest that two sets are equal, this is not a mathematical proof.

Example 1.4. Let A, B, C be sets. Show that:
$(A - B) \cap (A - C) = A - (B \cup C)$.

Answer

We need to show that $(A-B)\cap(A-C) \subseteq A-(B\cup C)$ and $A-(B\cup C) \subseteq (A - B) \cap (A - C)$.

First, we assume that $x \in (A-B)\cap(A-C)$. That is, $x \in (A-B)$ and $x \in (A - C)$. Next, $x \in (A - B)$ means that $x \in A$ and $x \notin B$). Similarly, $x \in (A - C)$ means that $x \in A$ and $x \notin C$). So, $x \notin B$ and $x \notin C$. By definition, $x \notin B \cup C$. So, $x \in A$ and $x \notin B \cup C$, that is $x \in A - (B \cup C)$ and this can be expressed as

$$(A - B) \cap (A - C) \subseteq A - (B \cup C). \tag{1}$$

Now, let's assume that $y \in A - (B \cup C)$. So $y \in A$ and $y \notin (B \cup C)$. $y \notin (B \cup C)$ means that $y \notin B$ and $y \notin C$. It follows that $y \in A - B$ and $y \in A - C$. The last can be expressed as $y \in (A - B) \cap (A - C)$, that is

$$A - (B \cup C) \subseteq (A - B) \cap (A - C). \tag{2}$$

By combining equations 1 and 2 we conclude that
$(A - B) \cap (A - C) = A - (B \cup C)$.■

1.3 Complement of a Set

Definition 1.7. For a set A (that is a subset of the universal set U), the complement $\overline{A}$ of A is the set of elements in the universal set not belonging to A. That is,
$\overline{A} = \{x \in U : x \notin A\} = U - A$

We can use Venn diagrams to show that
$A \cup \overline{A} = U$ and $A \cap \overline{A} = \emptyset$.

Example 1.5. Let $\mathbb{Z}$ be the universal set and let E be the set of odd integers. Then the complement $\overline{E}$ of E is the set of even integers. In addition, $E \cup \overline{E} = \mathbb{Z}$ and $E \cap \overline{E} = \emptyset$.

Theorem 1.8 (De Morgan's Laws)**.** *For two sets A and B,*
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ *and* $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

De Morgan's laws for the complement of the union and intersection of two sets results from De Morgan's laws for the negation of the disjunction and conjunction of two statements. We can show this as follows:

Let A and B be two sets that are subsets of a universal set U. Then,

$x \in \overline{A \cup B} \equiv\sim (x \in A \cup B) \equiv\sim (x \in A \text{ or } x \in B)$
$\equiv\sim ((x \in A) \vee (x \in B)) \equiv (x \notin A) \wedge (x \notin B)$
$\equiv (x \in \overline{A}) \wedge (x \in \overline{B}) \equiv x \in \overline{A} \cap \overline{B}$.
So, $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Similarly, $x \in \overline{A \cap B} \equiv\sim (x \in A \cap B) \equiv\sim (x \in A \text{ and } x \in B)$
$\equiv\sim ((x \in A) \wedge (x \in B)) \equiv (x \notin A) \vee (x \notin B)$
$\equiv (x \in \overline{A}) \vee (x \in \overline{B}) \equiv x \in \overline{A} \cup \overline{B}$.
So, $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Discrete Math I - MTSC 213
Lecture 9

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 14, 2013

1 Cartesian Products of Sets

New sets can be constructed from two given sets A and B by constructing ordered pairs of their elements. For example given two elements a and b we can construct the ordered pair (a, b), where a is the first coordinate of the pair and b is the second coordinate of the pair.

Definition 1.1. For two sets A and B, the Cartesian product $A \times B$ of A and B is the set of all ordered pairs whose first coordinate belongs to A and second coordinate belongs to B. That is

$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$.

Example 1.1. For the sets $A = \{0, 1\}$ and $B = \{\emptyset, \{1\}, 2\}$ determine $A \times B$.

Answer

$A \times B = \{(0, \emptyset), (0, \{1\}), (0, 2), (1, \emptyset), (1, \{1\}), (1, 2)\}$.■

The Cartesian product of $n \geq 2$ sets $A_1, A_2, ..., A_n$ is denoted by $A_1 \times A_2 \times A_3 \times ... \times A_n$ and is defined by

$A_1 \times A_2 \times A_3 \times ... \times A_n = \{(a_1, a_2, ..., a_n) : a_i \in A_i, \text{ for } i = 1 \leq i \leq n\}$.

The elements $(a_1, a_2, ..., a_n)$ are called ordered n-tuples. Ordered 2-tuples are ordered pairs and ordered 3-tuples are ordered triples.

If $A_i = A$, for $i = 1 \leq i \leq n$ then $A_1 \times A_2 \times A_3 \times ... \times A_n$ can also be denoted by A^n.

2 Partitions

In many cases it is useful to divide a nonempty set A into nonempty subsets in such a way that each element of A belongs to exactly one of these subsets.

Definition 2.1. A partition of a nonempty set A is a collection of nonempty subsets of A such that every element of A belongs to exactly one of these subsets.

A partition of a nonempty set A is therefore a collection of pairwise disjoint nonempty subsets of A whose union is A. Thus is $\mathcal{P} = \{S_1, S_2, ..., S_k\}$ is a partition of a nonempty set A, then

1. every subset S_i is nonempty
2. every two different subsets S_i and S_j are disjoint, and
3. the union of all subsets in $\mathcal{P}$ is A.

Example 2.1. Let $A = \{1, 2, ..., 8\}$. Which of the following collections of subsets of A are partitions of A?

1. $\mathcal{P}_1 = \{\{1, 4, 7, 8\}, \{3, 5, 6\}, \{2\}\}$
2. $\mathcal{P}_2 = \{\{1, 4\}, \{2, 8\}, \{3, 5, 7\}\}$
3. $\mathcal{P}_3 = \{\{1, 2, 4\}, \{3, 6, 8\}, \emptyset, \{5, 7\}\}$
4. $\mathcal{P}_4 = \{\{1, 7, 8\}, \{2, 5, 6\}, \{3, 4, 7\}\}$

Answer
Only $\mathcal{P}_1$ is a partition. $\mathcal{P}_2$ misses one element, $\mathcal{P}_3$ includes the empty set as an element, and $\mathcal{P}_4$ contains a common element between two subsets.■

Discrete Math I - MTSC 213
Lecture 10

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 31, 2013

1 Methods of Proof

Familiarity with the fundamentals of Logic and Set prepares us for learning how to read and understand proofs of theorems and be able to write our own proofs.

In theorems we use definitions, assumptions, axioms, and other theorems that have been previously proven.

A proof consists of a series of statements that follow a logical sequence and lead to a conclusion.

2 Quantified Statements

Open sentences involve variableswhos values are taken from a domain.

A statement can be produced from an open sentence by assigning to each variable in the open sentence a value from the domain.

We can also use **quantifiers** to form statements from open sentences.

There are two kinds of quantifiers: **existential** and **universal**.

Example 2.1. For the open sentence

$$R(n)\text{: } n^2 - n \text{ is even}$$

over the domain $\mathbb{Z}$ of integers, the sentence

$$\forall n \in \mathbb{Z},\ R(n)\text{: For every integer } n,\ n^2 - n \text{ is even}$$

is a quantified statement.

2.1 Universal Quantifiers

Let $R(x)$ be an open sentence over the domain S. Then, for each element $a \in S$, $R(a)$ is a statement.

Phrases "for all", "for each", "for every" are referred to as **universal quantifiers** denoted by the symbol $\forall$.

The sentence,
$\forall x \in S, R(x)$
is stated as
for every $x \in S, R(x)$.
This sentence is a statement that is called quantified statement.
Quantified statements are also expressed as implications.

Example 2.2. Let $R(n)$: $5n + 3$ is even , be an open sentence over the domain S of odd integers.

The quantified statement

$$\forall n \in S,\ R(n)$$

can be expressed as

For every odd integer, $5n + 3$ is even,

or

If n is an odd integer, then $5n + 3$ is even.

If $R(x)$ is an implication $P(x) \to Q(x)$ then the quantified statement
$\forall x \in S, P(x) \to Q(x)$
is expressed as follows:

- For every $x \in S$, if $P(x)$ then $Q(x)$.
- If $x \in S$, then $P(x)$ implies $Q(x)$.
- Let $x \in S$. If $P(x)$, then $Q(x)$.

If $R(x)$ is a biconditional statement $P(x) \leftrightarrow Q(x)$, then
$\forall x \in S\ ,\ P(x) \leftrightarrow Q(x)$
is expressed as:

- For every $x \in S$, $P(x)$ if and only if $Q(x)$.
- If $x \in S$, then $P(x)$ if and only if $Q(x)$.
- Let $x \in S$. Then P(x) is necessary and sufficient for $Q(x)$.

Example 2.3. For the open sentences $P(n)$: $n^2 iseven$, $Q(n)$: $niseven$ where n is an integer, the quantified statement

$$\forall n \in \mathbb{Z},\ P(n) \leftrightarrow Q(n)$$

can be expressed as:

- For every integer n, n^2 is even if and only if n is even.
- Let n be an integer. Then n^2 is even if and only if n is even.
- Let $n \in \mathbb{Z}$. Then n^2 is even is a necessary and sufficient condition for n to be even.

2.2 Existential Quantifiers

The phrases "there exists", "there is", "for some", and "for at least one" are referred to as **existential quantifiers**, denoted by $\exists$.

For an open sentence $Q(x)$, the sentence
$\exists x \in S\ ,\ Q(x)$
is a quantified statement expressed as

- There exists $x \in S$, such that $Q(x)$.
- For some $x \in S\ ,\ Q(x)$.
- For at least one $x \in S\ ,\ Q(x)$.

Example 2.4. For the open sentence $Q(x) : x^5 + 55x = 3x^3$, where x is a real number, the quantified statement

$$\exists x \in \mathbb{R},\ Q(x)$$

can be expressed as

- There exists $x \in \mathbb{R}$, such that $x^5 + 55x = 3x^3$.
- For some $x \in \mathbb{R}$, $x^5 + 55x = 3x^3$.
- For at least one $x \in \mathbb{R}$, $x^5 + 55x = 3x^3$.

2.3 Negations of Quantified Statements

For an open sentence $R(x)$ over the domain S, the negation of $\forall x \in S$, $R(x)$ is expressed as

$\sim (\forall x \in S$, $R(x))$: It is not the case that $R(x)$ for every $x \in S$.

This is also stated as:

There exists $x \in S$, such that not $R(x)$,

or,

$$\exists x \in S, \ \sim R(x).$$

Therefore

$$\sim (\forall x \in S \ , \ R(x)) \equiv \exists x \in S, \ \sim R(x).$$

The negation of $\exists x \in S$, $R(x)$ is:

$\sim (\exists x \in S, \ R(x))$: There does not exist $x \in S$, such that $R(x)$.

This is equivalent to:

For every $x \in S$, not $R(x)$.

or

$$\sim (\exists x \in S, \ R(x)) \equiv \forall x \in S, \ \sim R(x).$$

Example 2.5. State the negation of the following statements

(a) Everyone likes the "Wizard of Oz".

(b) There is a city whose population exceeds that of Mexico City.

Answer

The negation of (a) is

There exists someone who does not like the "Wizard of Oz".

The negation of (b) is

The population of every city is does not exceed that of Mexico city.

An equivalent expression is

The population of no city exceeds that of Mexico City.

Discrete Math I - MTSC 213
Lecture 11

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 31, 2013

1 Direct Proof

We previously described universal and existential quantifiers.

- The statement $\forall x \in S$, $R(x)$ is true if $R(x)$ is true for each $x \in S$. Therefore, $\forall x \in S, R(x)$ is false if $R(x)$ is false for at least one element $x \in S$.
- The statement $\exists x \in S$, $R(s)$ is true if there exists at least one element $x \in S$ for which $R(x)$ is true. So, $\exists x \in S$, $R(s)$ is false if $R(x)$ is false for every element $x \in S$.

Example 1.1. Let $S = \{3, 4, 5\}$ and let

$$R(x): \ \frac{x^2+5x+4}{2} \text{ is even.}$$

be an open sentence over the domain S.
(a) State $R(x)$ for each $x \in S$ and determine its truth value.
(b) State $\forall x \in S$, $R(x)$ and determine its truth value.
(c) State $\exists x \in S$, $R(x)$ and determine its truth value.
Answer
(a)

R(3): 14 is even (a true statement).
R(4): 20 is even (a true statement).
R(5): 27 is even (a false statement).

(b) $\forall x \in S$, R(x): For every $x \in S$, $\frac{x^2+5x+4}{2}$ is even.

This is false, because $R(5)$ is false.

(c) $\exists x \in S$, R(x): There is$x \in S$, such that $\frac{x^2+5x+4}{2}$ is even.

This quantified statement is true because there is at least one value of x for which $R(x)$ is true, for example $x = 3$.

Definition 1.1 (Proof)**.** A proof of a statement is a presentation of a logical argument that demonstrates the truth of the statement.

A proof of a statement R consists of a sequence of statements in logical order. The proof leads to a desired conclusion that R is true. In the proof we can use the following:

1. definitions of concepts
2. axioms or principles that have been agreed upon
3. assumptions we may have made
4. previous theorems.

A proof can be written in different ways according to the intended audience. The presentation must be clear, make solid assumptions, and include necessary level of detail to be understood by the reader.

Before writing proofs, one should study and understand proofs by other authors.

Let's begin from the universal quantifier. This is expressed as $\forall x \in S$, $R(x)$, and when $R(x)$ is an implication it becomes $\forall x \in S$, $P(x) \to Q(x)$.

The most common way to verify a statement of the form

$$\forall x \in S,\ P(x) \to Q(x)$$

is to use the method of **direct proof**.

To prove that $\forall x \in S$, $P(x) \to Q(x)$ is true by means of a direct proof, we begin by assuming that $P(x)$ is true for an arbitrary element $x \in S$ and then we show that $Q(x)$ is true.

To generalize, when we want to prove that $\forall x \in S$, $R(x)$ is true using direct proof, we first assume that x is an arbitrary element in S and then show that $R(x)$ is true.

The next sections deal with proofs of mathematical statements that we refer to as results. Some authors call all true mathematical statements theorems, but others call them, observations, facts, results, propositions, or theorems according to their importance. We will use the term theorem for

mathematical statements that are particularly interesting, useful and significant.

For example, we will call the statement Let$x \in \mathbb{R}$. If $x-2 = -$ then $x^2 - x - 2 = 9$ a result, but not a theorem.

1.1 Examples of Direct Proof

We will demonstrate this proof method with simple examples. We often precede the proof with an idea or a plan to be used to construct the proof. This is called proof strategy. In addition, after proving the theorem we may discuss ideas used in the proof, that is called proof analysis.

Result 1.2. *Let x be a real number. If $x - 2 = 0$, then $x^2 - x - 2 = 0$.*

Proof strategy In a direct proof, we first assume that $x - 2 = 0$. We need to show that $x^2 - x - 2 = 0$. We observe that $x^2 - x - 2 = 0$ can be factored as $(x-2)(x+1)$. Given that $x-2 = 0$ we can verify the mathematical statement.

Proof Assume that $x - 2 = 0$. Then $x^2 - x - 2 = (x - 2)(x + 1) = 0 \cdot (x + 1) = 0$.■

Proof Analysis The statement starts with "Let x be a real number." This means that x belongs to the domain of real numbers. We could also prove the statement by assuming $x - 2 = 0$, $x = 2$ because $x^2 - x - 2 = 2^2 - 2 - 2 = 0$.

In the next case we will use the following property of integers

If a and b are integers, then so too are $-a$, $a + b$ and ab.

Also the following definition is useful

Definition 1.3. An integer n is even if $n = 2a$ for some integer a. An integer n is odd if $n = 2b + 1$ for some integer b.

In general we need to prove properties of even and odd integers. Once we have proved these properties, we can use them in other theorems.

Result 1.4. *If n is an even integer, then $n^2 + 4n - 3$ is odd.*

Proof Let n be an even integer. Then $n = 2k$ for some integer k. Then
$n^2 + 4n - 3$
$= (2k)^2 + 4(2k) - 3$
$= 4k^2 + 8k - 3 = (4k^2 + 8k - 4) + 1$

$= 2(2k^2 + 4k - 2) + 1)$.

Because of 1.1, $2k^2 + 4k - 2$ is an integer, so $2(2k^2 + 4k - 2) + 1)$ and $n^2 + 4n - 3$ is odd.■

Proof Analysis We have shown that $n^2 + 4n - 3 = 4k^2 + 8k - 3$ for an even number k. Also, we could seemingly use $4k^2+8k-3 = 2(2k^2+4k-1)-1$ to show that this expression is odd. bu te can't, because we have not shown that an odd integer n can be written as $2k - 1$, where k is an integer.

In other cases we are asked to prove that

$$\text{For } x \in S \text{ and } y \in T,\ P(x, y) \to Q(x, y).$$

is true.

Here, we first assume that $P(x, y)$ is true for arbitrary elements $x \in S$ and $y \in T$, then show that $Q(x, y)$ is true.

Discrete Math I - MTSC 213
Lecture 12

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 31, 2013

1 Proof by Contrapositive

Let P and Q be two statements or open sentences, and an implication $P \to Q$ between P and Q. The contrapositive of $P \to Q$ is $(\sim Q) \to (\sim P)$. We have shown that

$$P \to Q \equiv (\sim Q) \to (\sim P).$$

So if we are asked to prove that $\forall x \in S$, $P(x) \to Q(x)$ is true one method of proof is to verify that

$$\forall x \in S, (\sim Q) \to (\sim P) \text{ is true}$$

using direct proof. This method is called proof by contrapositive.

So, to prove that $\forall x \in S$, $P \to Q$ is true using a proof by contrapositive, we assume that Q(x) is false for an arbitrary element $x \in S$ and show that $P(x)$ is also false.

Result 1.1. *Let n be an integer. If $7n + 3$ is an odd integer, then n is an even integer.*

Proof Assume that n is not an even integer. Then n is an odd integer $n = 2 + 1$, for $k \in \mathbb{Z}$. Then,

$$7n + 3 = 7(2k + 1) + 3 = 14k + 4 = 2(7k + 1).$$

Because $7k + 1$ is an integer, $7n + 3$ is even.

Proof Analysis We first express the contrapositive of our statement and then follow a direct proof method.

Result 1.2. *Let x be a real number. If $x^3 + 3x^2 + 2x + 1 \leq 0$, then $x < 0$.*

Proof
Assume that $x \geq 0$. Then
$x^3 \geq 0$, $3x^2 \geq 0$ and $2x \geq 0$. So,

$$x^3 + 3x^2 + 2x + 1 \geq 0 + 0 + 0 + 1 > 0.\blacksquare$$

1.1 Proofs of Biconditionals

We now consider the biconditional in a quantified statement

$$\forall x \in S,\ P(x) \leftrightarrow Q(x)$$

where $P(x)$, $Q(x)$ are open sentences over a domain S.

The biconditional is defined as

$$P(x) \leftrightarrow Q(x) \equiv (P(x) \rightarrow Q(x)) \wedge (Q(x) \rightarrow P(x)),$$

which is the conjunction of an implication and its converse.

To prove that $\forall x \in S,\ P(x) \leftrightarrow Q(x)$ is true, we must prove that $\forall x \in S,\ P(x) \rightarrow Q(x)$ is true and $\forall x \in S,\ Q(x) \rightarrow P(x)$ is true.

Result 1.3. *Theorem to prove: Let n be an integer. Then n^2 is even if and only if n is even.*

Proof strategy This statement is biconditional, so we need to prove two implications according to the definition.

Let $P(n)$ be the statement $P(n)$: n^2 is even and $Q(n)$: n is even. We can write the theorem to prove as $\forall n \in Z$: $P(n) \leftrightarrow Q(n)$. Therefore we need to prove $\forall n \in Z$: $P(n) \rightarrow Q(n)$ and $\forall n \in Z$: $Q(n) \rightarrow P(n)$. We will prove the latter statement by direct proof and the former statement by contrapositive.

Theorem 1.4. *Let n be an integer. Then n^2 is even if and only if n is even.*

Proof Assume that n is even. Then $n = 2a$ for $a \in \mathbb{Z}$. Then, $n^2 = (2a)^2 = 4a^2 = 2(2a^2)$.

Because $2(2a^2)$ is even, n^2 is even.

Next, we verify the converse. Here we utilize proof by contrapositive. Assume that n is not even that is n is odd and $n = 2b + 1$, $b \in \mathbb{Z}$. Then

$$n^2 = (2b + 1)^2 = 4b^2 + 4b + 1 = 2(2b^2 + 2b) + 1.$$

Based on properties of integers, $2b^2 + 2b$ is an integer, so n^2 is odd.■

We note here that this theorem can be expressed using contrapositives as follows.

Theorem 1.5. *Let n be an integer. Then n^2 is odd iff n is odd.*

Discrete Math I - MTSC 213
Lecture 13

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 31, 2013

1 Proof by Cases

Let's consider the statement $\forall x \in S$, $R(x)$. In some occasions, knowing $x \in S$ does not provide enough information to show that $R(x)$ is true.

In such cases we may divide S into a collection P of subsets of S that is usually a partition of S. The proof is then divided into cases according to subsets.

For example, if we are asked to prove a statement in the domain of integers, it may be helpful to partition $\mathbb{Z}$ into the sets of positive and negative integers. Similarly, when our statement involves an absolute value $|x|$, then it may help to prove the cases of negative and positive integers separately.

Overall, if we wish to prove a statement including an element x in set S, then it may be useful to create a partition P of S. Then the proof can be divided into cases that correspond to the particular subsets of S in P.

Example 1.1. If n is an integer, $n^2 - n$ is an even integer.

Proof Let n be an integer. We consider two cases, (1) n is even, and (2) n is odd.

Case 1. n is even. Then there exists an integer a, such that $n = 2a$. Then,

$$n^2 - n = (2a)^2 - 2a = 4a^2 - 2a = 2(2a^2 - a).$$

Because $2a^2 - a$ is an integer $n^2 - n$ is even.

Case 2. n is odd. Then there exists an integer b, such that $n = 2b + 1$. Then,

$$n^2 - n = (2b + 1)^2 - (2b + 1) = 4b^2 + 4b + 1 - 2b - 1 = 4b^2 + 2b = 2(2b^2 + b).$$

Because $2b^2 + b$ is an integer $n^2 - n$ is even.■

1.1 Parity of Integers

Two integers m and n are said to be of the same parity, if both of them are even or both are odd; otherwise m and n are of opposite parity.

Example 1.2. Result to prove: Let m and n be two integers. Then $3m + n$ is even if and only if m and n are of the same parity.

Proof This is a quantified biconditional statement of the form $\forall, x \in S,\ P \leftrightarrow Q$. Therefore we will need to prove that $\forall, x \in S,\ Q \rightarrow P$ and $\forall, x \in S,\ P \rightarrow Q$. We will solve the former by direct proof and the latter by proof by contrapositive.

We first assume that m and n are of the same parity. We divide this into two cases.

Case 1. m and n are even. Thus, $m = 2a$ and $n = 2b$ for some integers $a, b \in \mathbb{Z}$. Then,

$$3m + n = 3(2a) + 2b = 6a + 2b = 2(3a + b).$$

Because $3a + b$ is an integer, $3m + n$ is even.

Case 2. m and n are odd. Thus, $m = 2a + 1$ and $n = 2b + 1$ for some integers $a, b \in \mathbb{Z}$. Then,

$$3m + n = 3(2a + 1) + (2b + 1) = 6a + 3 + 2b + 1 = 6a + 2b + 2 = 2(3a + b + 1).$$

Because $3a + b + 1$ is an integer, $3m + n$ is even.

We prove $\forall, x \in S,\ P \rightarrow Q$ by contrapositive. Then we have the following statement: Let m and n be two integers. If m and n are of opposite parity, then $3m + n$ is odd. So, let m and n be of opposite parity. We divide this statement into cases.

Case 1. m is even and n is odd. So, $m = 2a$ and $n = 2b + 1$ for some integers $a, b \in \mathbb{Z}$. Then,

$$3m + n = 3(2a) + 2b + 1 = 6a + 2b + 1 = 2(3a + b) + 1.$$

Because $3a + b$ is an integer, $3m + n$ is odd.

Case 2. m is odd and n is even. Then for some integers $a, b \in \mathbb{Z}$, $m = 2a + 1$ and $n = 2b$. Then,
$3m + n = 3(2a + 1) + 2b = 6a + 3 + 2b = 6a + 2b + 2 + 1 = 2(3a + b + 1) + 1.$
Because $3a + b + 1$ is an integer, $3m + n$ is odd. ■

1.2 Without Loss of Generality

Sometimes when we use the proof by cases method, the proofs of two cases are very similar and proving both cases becomes repetitive.

Then we can choose to prove one case only and state that we are doing this without loss of generality.

Example 1.3. Let A, B and C be sets. Then
$$(A - B) \cup (A - C) = A - (B \cap C).$$

Proof Here we need to prove that $(A-B)\cup(A-C) \subseteq A-(B\cap C)$ and $A-(B\cap C) \subseteq (A-B)\cup(A-C)$.

We first show that $(A - B) \cup (A - C) \subseteq A - (B \cap C)$. Let $x \in (A - B) \cup (A - C)$. Then $x \in (A - B)$ or $x \in (A - C)$. We will follow proof by cases.

Case 1. Let $x \in (A - B)$. Then $x \in A$ and $x \notin B$. So $x \notin (B \cap C)$. Because $x \in A$ and $x \notin (B\cap C)$, then $x \in A-(B\cap C)$. So, $(A-B)\cup(A-C) \subseteq A - (B \cap C)$.

Case 2. Let $x \in (A - C)$. Then $x \in A$ and $x \notin C$. So $x \notin (B \cap C)$. Because $x \in A$ and $x \notin (B \cap C)$, then $x \in A - (B \cap C)$. Therefore $(A - B) \cup (A - C) \subseteq A - (B \cap C)$.

Next, we show that $A-(B\cap C) \subseteq (A-B)\cup(A-C)$. Let $x \in A-(B\cap C)$. Then $x \in A$ and $x \notin (B \cap C)$. By DeMorgan's Laws $x \in A$ and $x \notin B$ or $x \notin C$.

Case 1. Let $x \notin B$. Because $x \in A$, $x \in (A - B)$. Therefore, $x \in (A - B) \cup (A - C)$. So, $(A - B) \cup (A - C) \subseteq A - (B \cap C)$.

Case 2. Let $x \notin C$. Because $x \in A$, $x \in (A - C)$. Therefore, $x \in (A - B) \cup (A - C)$. So, $(A - B) \cup (A - C) \subseteq A - (B \cap C)$.■

Discrete Math I - MTSC 213
Lecture 14

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 31, 2013

1 Counterexamples

In the previous sections we dealt with methods of proof for quantified statements of the form $\forall x \in S$, $R(x)$. These statements are true if $R(x)$ is true for all elements in S. We also saw that the negation of this statement is

$$\sim (\forall x \in S,\, R(x)) \equiv \exists x \in S,\ \sim (R(x)).$$

This means that our statement is false, if $R(x)$ is false for at least one element of S.

Now let's consider the statement $\forall x \in S, P(x) \rightarrow Q(x)$. To show that this statement is false we need to find an element $a \in S$ such that $P(a) \rightarrow Q(a)$ is false. The element $a \in S$ is called a **counterexample** for the statement $\forall x \in S$, $P(x) \rightarrow Q(x)$. A counterexample of this statement is an element for which $P(x)$ is **true** and $Q(x)$ is **false**. Such an element is said to **disprove** the statement.

Result 1.1. *Disprove: For every two sets A and B, $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.*

Proof Let $A = \{1\}$ and $B = \{2\}$.
Then, $\mathcal{P}(A) = \{\emptyset, \{1\}\}$ and $\mathcal{P}(B) = \{\emptyset, \{2\}\}$.
$\mathcal{P}(A \cup B) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}$, but $\mathcal{P}(A) \cup \mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}\}$.
Therefore $\mathcal{P}(A \cup B) \neq \mathcal{P}(A) \cup \mathcal{P}(B)$.■

Result 1.2. *Prove or disprove the following:*
(a) Let $S = \{1, 4, 5, 8\}$. If $n \in S$, then $\frac{(n^2-n)}{2}$ is an even integer.

(b) Let $S = \{1, 4, 5, 6, 8\}$. If $n \in S$, then $\frac{(n^2-n)}{2}$ is an even integer.

Proof (a) Let $n \in S$. We have four cases.

Case 1. $n = 1$. Then $\frac{(n^2-n)}{2} = 0$ is even.

Case 2. $n = 4$. Then $\frac{(n^2-n)}{2} = 6$ is even.

Case 3. $n = 5$. Then $\frac{(n^2-n)}{2} = 10$ is even.

Case 4. $n = 8$. Then $\frac{(n^2-n)}{2} = 28$ is even.

Therefore, the statement, If $n \in S$, then $\frac{(n^2-n)}{2}$ is an even integer, is true.■

(b) We test the additional case $n = 6$.

Then, $\frac{(n^2-n)}{2} = 15$ that is false.

So the statement is false and $n = 6$ is a counterexample.■

2 Existence Proofs

In this section we discuss proofs of quantified statements of the form $\exists x \in S$, $R(x)$. We have seen that the statement $\exists x \in S$, $R(x)$ is true if $R(x)$ is true for at least one element of S. Therefore, to prove this statement we need to show that there is some element $a \in S$ for which $R(a)$ is true. This method of proof is called **existence proof**.

Result 2.1. *Disprove the following statement:*

There exists $x \in \mathbb{R}$ such that $x^4 + 2 = 2x^2$.

Proof We are asked to prove that the above statement is false. So we need to show that $x^4 + 2 = 2x^2$ has no solution in the real number domain. Therefore we have to show that

$$\forall x \in \mathbb{R}, x^4 + 2 \neq 2x^2$$

The formula $x^4 + 2 \neq 2x^2$ is equivalent to $x^4 + 2 - 2x^2 \neq 0$. Then

$x^4 + 2 - 2x^2 = x^4 - 2x^2 + 2 = x^4 - 2x^2 + 1 + 1 = (x^2 - 1)^2 + 1$.

Given that $(x^2 - 1)^2 \geq 0$, $(x^2 - 1)^2 + 1 \geq 1$, therefore $(x^2 - 1)^2 + 1 \neq 0$.■

Result 2.2. *Disprove the following statement:*

For every positive integer n, there exists a negative integer m such that $n + m = 1$.

Proof Let $n = 1$.

Then, for every negative number $m < 0$, $n + m < 1 + 0 < 1$.

Therefore the statement is false, or in other words $n = 1$ is a counterexample.■

Proof analysis We are called to disprove a statement of the type $\forall n \in S, \exists m \in T, R(n, m)$.

The negation of this statement is $\exists n \in S, \forall m \in T, \sim (R(n, m))$.

To show that the negation is true, we need to find an element $n \in S$ so that for every element $m \in T$ $R(x, y)$ is false.

Result 2.3. *Prove or disprove the following:*

(a) There exist distinct rational numbers a and b such that $(a-1)(b-1) = 1$.

(b) There exist distinct rational numbers a and b such that $\frac{1}{a} + \frac{1}{b} = 1$.

Proof (a) Let $a = 5$.

Then for $b = 5/4$, $(a - 1)(b - 1) = 1$.■

(b) Let $a = 5$.

Then for $b = 5/4$, $\frac{1}{a} + \frac{1}{b} = 1$.■

Proof Analysis We observe that,

$(a-1)(b-1) = 1 \leftrightarrow ab-a-b+1 = 1 \leftrightarrow ab-a-b = 0 \leftrightarrow \frac{ab}{ab} - \frac{a}{ab} - \frac{b}{ab} = 0 \leftrightarrow 1 - \frac{1}{b} - \frac{1}{a} \leftrightarrow 0$.

We can express this as follows:

For two distinct real numbers a and b,

$(a - 1)(b - 1) = 1$ is true, if and only if,

$ab = a + b$ is true, if and only if,

$\frac{1}{b} + \frac{1}{a} = 1$ is true.

Discrete Math I - MTSC 213
Lecture 15

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 31, 2013

1 Proof by Contradiction

So far, we have learned the methods of direct proof and proof by contrapositive for statements R of the type $\forall x \in S,\ P(x) \to Q(x)$.

This section deals with a third method of proof. Here we assume that $R(x)$ is false. Suppose that this assumption leads to a statement that contradicts an assumption we made in the proof. If the fact or assumption is P then the contradiction we have deduced is $C \equiv P \wedge (\sim P)$. So in this case we have shown that the logical statement $(\sim R) \to C$ is true. Because C is false, $(\sim R)$ must be false, therefore our original statement R is true.

To verify that a statement R is true by proof by contradiction, we first assume that R is false and then conclude with a contradiction. When R is $\forall x \in S,\ P(x) \to Q(x)$, then we assume that there is some $x \in S$, such that $P(x)$ is true and $Q(x)$ is false. Then we attempt to reach a contradiction that will verify our original statement.

Result 1.1. *The sum of a rational number and an irrational number is an irrational.*

Proof Assume that there is a rational number a and an irrational number b, such that $a + b = c$ is rational.

Then, $a = \frac{m}{n}$ and $c = \frac{p}{r}$ where $m, n, p, r \in \mathbb{Z}$ and $r \neq 0, n \neq 0$.

So, $a + b = c$ is equivalent to $\frac{m}{n} + b = \frac{p}{r}$.

Then, $b = \frac{p}{r} - \frac{m}{n}$ and $b = \frac{pn-mr}{rn}$.

Because $m, n, p, r \in \mathbb{Z}$ and $r \neq 0, n \neq 0$ b is a rational number, which contradicts our assumption that b is irrational.■

Result 1.2. *Prove that $\sqrt{2} + \sqrt{3}$ is an irrational number.*

Proof Let $\sqrt{2} + \sqrt{3}$ be rational. Then, $\exists a, b \in \mathbb{Z}, b \neq 0 : \sqrt{2} + \sqrt{3} = \frac{a}{b}$.

Then, $\left(\sqrt{2} + \sqrt{3}\right)^2 = \frac{a^2}{b^2} \leftrightarrow 2 + 3 + 2\sqrt{6} = \frac{a^2}{b^2} \leftrightarrow b^2(2 + 3 + 2\sqrt{6}) = a^2 \leftrightarrow 2b^2 + 3b^2 + 2\sqrt{6}b^2 = a^2 \leftrightarrow 5b^2 + 2\sqrt{6}b^2 = a^2 \leftrightarrow 2\sqrt{6}b^2 = a^2 - 5b^2 \leftrightarrow \sqrt{6} = \frac{a^2-5b^2}{2b^2}$.■

Because $a, b \in \mathbb{Z}$, $a^2 - 5b^2 \in \mathbb{Z}$ and $2b^2 \in \mathbb{Z}$. Therefore, $\sqrt{6}$ is a rational, which is a contradiction.■

Result 1.3. *Prove that there is no smallest positive irrational number.*

Proof Let s be the smallest positive irrational number, $s > 0$.

Also, assume that $\exists r \in \mathbb{Q} : r = s/2$.

Then $r = a/b$, $a, b \in \mathbb{Z}$ and $b \neq 0$.

It follows that $s = 2r = 2(a/b)$.

Because $r \in \mathbb{Q}$, then $s \in \mathbb{Q}$, which contradicts our assumption that $s \in \mathbb{R} - \mathbb{Q}$.■

Result 1.4. *Prove that there do not exist three distinct positive real numbers a, b and c such that two of the three numbers $\sqrt{a+b}$, $\sqrt{b+c}$ and $\sqrt{a+c}$ are equal.*

Proof Assume that there exist three distinct positive real numbers a, b and c such that $\sqrt{a+b} = \sqrt{b+c}$.

Then, $(\sqrt{a+b})^2 = (\sqrt{b+c})^2 \leftrightarrow a + b = b + c \leftrightarrow a = c$.

The latter equality contradicts our assumption that a, b and c are distinct.■

Result 1.5. *Use proof by contradiction to prove the following: Assume that n is an integer. If $3n + 14$ is even, then n is even.*

Proof Let n be an integer, $3n + 14$ be even, and n be odd. Then,

$n = 2k + 1$ for some integer k.

Therefore $3n+14 = 3(2k+1)+14 = 6k+17 = 6k+16+1 = 2(3k+8)+1$.

This means that $3n + 14$ is odd that contradicts our assumption that $3n + 14$ is even.■

Discrete Math I - MTSC 213
Lecture 18

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 9, 2013

1 Mathematical Induction

We have reviewed three methods of proving the quantified statement of the form

$$\forall x \in S,\ R(x),$$

where $R(x)$ is an open sentence over a domain S. These three proof techniques are direct proof, proof by contrapositive, and proof by contradiction.

If $S = \mathbb{N}$, then there is another method of proof that we can use the method of mathematical induction to prove that $\forall n \in \mathbb{N},\ R(n)$.

2 The Principle of Mathematical Induction

Given a statement $\forall n \in \mathbb{N},\ P(n)$, the main idea of mathematical induction is to verify that $P(n)$ is true for $n = 1$ and to establish the truth of a specific implication.

The Principle of Mathematical Induction The statement

$$\forall n \in \mathbb{N},\ P(n)$$

is true if

(1) $P(1)$ is true and

(2) the statement $\forall k \in \mathbb{N},\ P(k) \to P(k+1)$ is true.

A proof using the Principle of Mathematical Induction is called an induction proof, a proof by mathematical induction, or a proof by induction.

The first step is called the base, basis step, or anchor.

The second step is called the inductive step.

$P(k)$ is called the inductive hypothesis or induction hypothesis.

The statement $\forall k \in \mathbb{N}$, $P(k) \rightarrow P(k+1)$ is usually verified using proof by hypothesis.

Result 2.1. *For every positive integer n,*

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + ... + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}.$$

Proof

We proceed by induction.

Basis step: we verify that the statement is true for $n = 1$.

We observe that $\frac{1}{1\cdot 2} = \frac{1}{1+1}$.

Inductive step: Let

$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + ... + \frac{1}{k\cdot(k+1)} = \frac{k}{k+1}$.

where k is a positive integer.

We show that

$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + ... + \frac{1}{(k+1)\cdot(k+2)} = \frac{k+1}{k+2}$.

We observe that

$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + ... + \frac{1}{(k+1)\cdot(k+2)}$

$= \left[\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + ... + \frac{1}{k\cdot(k+1)}\right] + \frac{1}{(k+1)\cdot(k+2)}$

$= \frac{k}{k+1} + \frac{1}{(k+1)\cdot(k+2)}$

$= \frac{k\cdot(k+2)+1}{(k+1)\cdot(k+2)}$

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

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

$= \frac{(k+1)}{(k+2)}$.

By the principle of Mathematical Induction, it then follows that

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + ... + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$$

for every positive n.■

Result 2.2. *For every positive integer n,*

$$1 + 2 + ... + n = \frac{n \cdot (n+1)}{2}$$

Proof We use induction.
Basis step: For $n = 1$ we observe that $1 = \frac{1 \cdot (1+1)}{2}$.
Inductive step: Let
$1 + 2 + ... + k = \frac{k \cdot (k+1)}{2}$
for a positive integer k. We show that
$1 + 2 + ... + (k + 1) = \frac{(k+1) \cdot (k+2)}{2}$ We observe that
$1 + 2 + ... + (k + 1) = (1 + 2 + ... + k) + (k + 1)$
$= \frac{k \cdot (k+1)}{2} + (k + 1)$
$= \frac{(k \cdot (k+1)) + (2 \cdot (k+1))}{2}$
$= \frac{(k+2) \cdot (k+1)}{2}$.
By the principle of Mathematical Induction, it follows that

$$1 + 2 + ... + n = \frac{n \cdot (n+1)}{2}$$

for every positive n.■

Result 2.3. *For every positive integer n,*

$$1 + 2 + 2^2 + ... + 2^n = 2^{n+1} - 1$$

Proof We use proof by induction.
Basis step: For $n = 1$ we observe that $1 + 2^1 = 2^2 - 1$
Inductive step: Let
$1 + 2 + 2^2 + ... + 2^k = 2^{k+1} - 1$
for a positive integer k.
Now we show that
$1 + 2 + 2^2 + ... + 2^{k+1} = 2^{k+2} - 1$.
We observe that
$1 + 2 + 2^2 + ... + 2^{k+1} = \left(1 + 2 + 2^2 + ... + 2^k\right) + 2^{k+1}$
$= 2^{k+1} - 1 + 2^{k+1}$
$= 2 \cdot 2^{k+1} - 1$
$= 2^{k+2} - 1$.
By the principle of Mathematical Induction, it follows that

$$1 + 2 + 2^2 + ... + 2^n = 2^{n+1} - 1$$

for every positive n.■

Result 2.4. *Let $r \geq 2$ be an integer. Prove that $1+r+r^2+...+r^n = \frac{r^{n+1}-1}{r-1}$ for every positive integer n.*

Proof

We utilize proof by induction.

Basis step: For $n = 1$ we observe that

$1 + r^1 = \frac{r^2-1}{r-1}$

$1 + r = \frac{(r+1)(r-1)}{r-1}$

$r + 1 = r + 1$

$1 = 1$

so the equation is true.

Inductive step: Let

$1 + r + r^2 + ... + r^k = \frac{r^{k+1}-1}{r-1}$

for a positive integer k.

We show that $1 + r + r^2 + ... + r^{k+1} = \frac{r^{k+2}-1}{r-1}$.

$1 + r + r^2 + ... + r^{k+1}$

$= \left(1 + r + r^2 + ... + r^k\right) + r^{k+1}$

$= \frac{r^{k+1}-1}{r-1} + r^{k+1}$

$= \frac{r^{k+1}-1+r^{k+1}(r-1)}{r-1}$

$= \frac{r^{k+1}-1+r^{k+2}-r^{k+1}}{r-1}$

$= \frac{r^{k+2}-1}{r-1}$.

By the Principle of Mathematical induction, the formula $1+r+r^2+...+r^n = \frac{r^{n+1}-1}{r-1}$ holds for every positive integer n.■

Discrete Math I - MTSC 213
Lecture 19

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 11, 2013

1 Additional Examples of Induction Proofs

In this section we will use variations and generalizatin of the Principle of Mathematical Induction to solve various types of statements.

In several cases $\mathbb{N}$ is not the appropriate domain, but we need to show that an examine the truth of an open sentence $P(n)$ in the set $S = \{i \in \mathbb{Z}\colon\ i \geq m\} = \{m, m+1, m+2, ...\}$. In these cases we utilize a generalized form of the Principle of Mathematical Induction, that is usually referred to by the same name.

The Principle of Mathematical Induction For a fixed integer m, let $S = \{i \in \mathbb{Z}\colon\ i \geq m\}$.

Then the statement

$$\forall n \in S,\ P(n)\colon \text{ For every integer } n \geq m, P(n)$$

is true if

(1) $P(m)$ is true and

(2) the statement $\forall k \in S,\ P(k) \rightarrow P(k+1)$ is true.

When $m = 1$ this principle becomes the Principle of Mathematical Induction that was originally described in the previous section.

Result 1.1. *For every integer $n \geq 4$, $n! > 2^n$. (Please solve)*

We now consider other applications of the Principle of Mathematical Induction. We can use this method of proof to prove that known properties of two objects of a certain types hold for more objects of the same type. For example, we know the following fundamental property of real numbers:

If a and b are real numbers such that $ab = 0$, then either $a = 0$ or $b = 0$.

Let's now verify the following result:

Result 1.2. *If $a_1, a_2, ..., a_n$ are $n \geq 2$ real numbers such that $a_1a_2...a_n = 0$, then $a_i = 0$ for some integer i with $1 \leq i \leq n$.*

Proof

We proceed by induction.

For n=2, it follows from the fundamental property of real numbers that if $a_1a_2 = 0$, then $a_1 = 0$, or $a_2 = 0$.

Now we assume the following statement:

If $a_1, a_2, ..., a_k$ are $k \geq 2$ real numbers such that $a_1a_2...a_k = 0$, then $a_i = 0$ for some integer i with $1 \leq i \leq k$.

We will show that if $a_1, a_2, ..., a_{k+1}$ are real numbers such that $a_1a_2...a_{k+1} = 0$, then $a_i = 0$ for some integer i with $1 \leq i \leq k + 1$.

Let $a_1, a_2, ..., a_{k+1}$ be real numbers such that $a_1a_2...a_{k+1} = 0$.

Then $a_1a_2...a_{k+1} = (a_1a_2...a_k)a_{k+1} = 0$. Therefore fundamental property of real numbers it follows that either $(a_1a_2...a_k) = 0$ or $a_{k+1} = 0$.

If $a_{k+1} = 0$ then we found the solution.

Otherwise if $(a_1a_2...a_k) = 0$, it follows by the inductive hypothesis that $a_i = 0$ for some integer i with $1 \leq i \leq k$.

In either case, $a_i = 0$ for some integer i with $1 \leq i \leq k + 1$.

By the Principle of Mathematical Induction the result is true.

Theorem 1.3. *Let n be a nonnegative integer. If A is a set with $|A| = n$, then the cardinality of its power set is $|\mathcal{P}(A)| = 2^n$.*

Proof

We proceed by induction.

For $n = 0$, we observe that $|A| = 0$ is the cardinality of the empty set. Then we observe that $|\mathcal{P}(\emptyset)| = 1 = 2^0$.

Next, we assume that if S is a set with $|S| = k$, then the cardinality of its power set is $|\mathcal{P}(S)| = 2^k$, for a nonnegative integer k.

We show that the following statement is true: If A is a set with $|A| = k+1$, then the cardinality of its power set is $|\mathcal{P}(A)| = 2^{k+1}$.

Let $A = \{a_1, a_2, a_3, ..., a_{k+1}\}$ and $B = \{a_1, a_2, a_3, ..., a_k\}$. By inductive hypothesis it follows that $|B| = k$ and $|\mathcal{P}(B)| = 2^k$. These are equal to the subsets of A that do not contain a_{k+1}.

Now the subsets of A that contain a_{k+1} can be produced by the union of elements of $\mathcal{P}(B)$ and $\{a_{k+1}\}$. Therefore, the cardinality of remaining sets is 2^k.

It follows that the cardinality of all subsets of A is $|\mathcal{P}(A)| = 2^k + 2^k = 2(2^k) = 2^{k+1}$.

The result then follows by the Principle of Mathematical Induction.

Discrete Math I - MTSC 213
Lecture 20

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 16, 2013

1 Sequences

The concept of sequences frequently occurs in discrete mathematics. Here a sequence is a listing of elements of a set. A sequence can be finite or infinite. We are more interested in infinite sequences. The elements of a sequence typically belong to $\mathbb{Z}$ or to $\mathbb{R}$.

An infinite sequence is denoted by $a_1, a_2, a_3, ...$ or by $\{a_n\}$. The element a_1 is called the first term of the sequence, a_2 is the second term, and a_n is called the nth term.

Example 1.1. (a) 1,2,3,4,... is a sequence whose nth term is n.

(b) 1,4,9,16,... is a sequence whose nth terms is n^2.

(c) 1,8,27,64,... is a sequence whose nth term is n^3.

Sequences (a)-(c) are polynomial sequences of the form $\{n^k\}$ for a fixed integer k.

(d) 2,4,8,16,... is a sequence whose nth term is 2^n.

(3) 4,7,10,13,... is a sequence whose nth term is $3n + 1$.

Definition 1.1 (Geometric sequence)**.** A geometric sequence is a sequence in which the ratio of every two elements a_n and a_{n+1} is a constant r, i.e. $a_{n+1}/a_n = r$ for each $n \in \mathbb{N}$.

Definition 1.2 (Arithmetic sequence)**.** An arithmetic sequence is a sequence in which the difference between consecutive elements a_n and a_{n+1} is a constant r. This means that $a_{n+1} - a_n = r$ for each $n \in \mathbb{N}$.

Example 1.2. Determine the nth term of the sequence $\{a_n\}$ who first four terms are:

$$a_0 = -\frac{1}{3}, a_1 = \frac{2}{5}, a_2 = -\frac{4}{7}, a_3 = \frac{8}{9}.$$

Answer

We check the sign, the numerator and denominator. A sequence generating these terms is

$$a_n = (-1)^{n+1}\frac{2^n}{2n+3}.$$

1.1 Binary Strings

We now consider finite sequences. A finite sequence may also be called a string. The number of terms of a string is called the string's length. We can denote a string of length n by $a_1, a_2, ..., a_n$, or by $(a_1, a_2, ..., a_n)$, or by $a_1a_2...a_n$, where a_i belongs to a set S and $1 \leq i \leq n$.

A specific type of strings contain binary digits. A binary digit, or bit, is an element with values 0 or 1, so $S = \{0, 1\}$. The corresponding string is called a binary string or a bit string. An n-bit string is a bit string of length n. The 6-bit string $(0, 1, 0, 0, 1, 0)$ can also be written as $0, 1, 0, 0, 1, 0$, or 010010). Bit strings are ubiquitous in digital logic and computer science in general.

Example 1.3. There are $2^4 = 16$ subsets of a set S with 4 elements. These subsets can be represented by bit-strings of length 4. We first order the elements so that $S = \{a_1, a_2, a_3, a_4\}$. Each subset can be represented by a bit string whose i-th term is 1 if a_i belongs to the subset. On the other hand a_i is 0 if a_i does not belong to the subset.

For example $A = \{a_1, a_4\}$ is represented by 1001, and $B = \emptyset$ is represented by 0000.

1.2 Recursively Defined Sequences

An alternative definition of sequences uses a recursive description. In this definition, one or more terms are initially defined and subsequent terms are defined according to the initial terms.

Definition 1.3 (Recursively Defined Sequence)**.** A sequence $a_1, a_2, ..., a_n$ of real numbers is said to be recursively defined if:

(1) For some fixed positive integer t, the terms $a_1, a_2, ..., a_t$ are given.

(2) For each integer $n > t$ a_n is defined in terms of one or more of $a_1, a_2, ..., a_n$.

Here $a_1, a_2, ..., a_t$ are called the initial values of $\{a_n\}$. The relation between a_n and $a_1, a_2, ..., a_t$ for $n > t$ is the recurrence relation for $\{a_n\}$.

Example 1.4 (please solve)**.** For $X = \{x_1, x_2, x_3, x_4, x_5\}$ determine

(a) which 5-bit string corresponds to each of the subsets below:
$X + 1 = \{x_1, x_4\}, X_2 = \{x_2, x_4, x_5\}, X_3 = \{x_3, x_5\}$.

(b) which subset of X corresponds to each of the 5-bit strings below:
$s_1 = 00000, s_2 = 01001, s_3 = 11111$.

Example 1.5 (please solve)**.** A sequence $A_1, A_2, A_3, ...$ of sets is defined recursively by $A_1 = \{1\}$ and $A_n = ((A_1 \cup A_2 \cup A_3 \cup ... \cup A_{n-1}) - A_{n-1}) \cup \{n\}$ for $n \geq 2$. Determine the sets A_2, A_3, A_4, A_5, A_6.

Discrete Math I - MTSC 213
Lecture 21

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 16, 2013

1 Sequences

1.1 Fibonacci Numbers

A popular recursively defined sequence results from certain positive integer numbers is known as the Fibonacci numbers.

Example 1.1. The Fibonacci sequence $F_1, F_2, F_3, ...$ is defined recursively by

$$F_n = \begin{cases} 1 & \text{if } n = 1, 2 \\ F_{n-2} + F_{n-1} & \text{if } n \geq 3 \end{cases}$$

The numbers $F_1, F_2, F_3, ...$ are called Fibonacci numbers.
We observe that
$F_1 = 1$
$F_2 = 1$
$F_3 = 2$
$F_4 = 3$
$F_5 = 5$
$F_6 = 8$.
The Finbonacci numbers appear in some unexpected applications.

Example 1.2. For every integer $n \geq 2$,
$F_{n-1}F_{n+1} = F_n^2 + (-1)^n$

Answer
We proceed by induction.
For $n = 2$, $F_1F_3 = 1 \cdot 2 = 1^2 + 1 = F_2^2 + (-1)^2$.
We assume that for $k \geq 2$, $F_{k-1}F_{k+1} = F_k^2 + (-1)^k$.
So, $F_k^2 = F_{k-1}F_{k+1} - (-1)^k$.
We show that $F_kF_{k+2} = F_{k+1}^2 + (-1)^{k+1}$

$$\begin{aligned} F_kF_{k+2} &= F_k(F_k + F_{k+1}) \\ &= F_k^2 + F_kF_{k+1} \\ &= F_{k-1}F_{k+1} - (-1)^k + F_kF_{k+1} \\ &= (F_{k-1} + F_k)F_{k+1} - (-1)^k \\ &= F_{k+1}F_{k+1} - (-1)^k \\ &= F_{k+1}^2 + (-1)^{k+1}. \end{aligned}$$

Therefore by the Principle of Mathematical Induction it follows that $F_{n-1}F_{n+1} = F_n^2 + (-1)^n$.

The Fibonacci numbers where introduced in the middle ages by Leonardo da Pisa who was known for the leaning tower of Pisa. Leonardo da Pisa called himself Fibonacci. He wrote the book Liber Abaci that introduced the decimal number system to the Latin-speaking world.

The solution of the following problem stated in Liber Abaci led to the introduction of Fibonacci numbers.

"A certain man had one pair of rabbits together in a certain enclosed place and one wishes to know how many are created from the pair in one year when it is the nature of them in a single month to bear a single pair and in the second month those born to bear also."

Example 1.3 (Please solve)**.** For a nonnegative n, let s_n be the number of subsets of an n-element set.
(a) What are s_0, s_1, s_2?
(b) Give a recursive definition of s_n for $n \geq 0$.

Example 1.4. For a positive integer n, let s_n be the number of n-bit strings having no three consecutive 0s.

(a) Determine s_1, s_2, s_3.

(b) Give a recursive definition of s_n, for $n \geq 1$.

Answer

(a) s_1: number of 1-bit strings with no three consecutive 0s.

These bit-strings are 0 and 1. All have no three consecutive 0s, so $s_1 = 2$.

s_2: number of 2-bit strings with no three consecutive 0s.

These strings are 00, 01, 10, and 11. All have no three consecutive 0s, so $s_2 = 4$.

s_3: number of 3-bit strings with no three consecutive 0s.

These strings are 000, 001, 010, 011, 100, 101, 110, 111. 7 out of 8 have no three consecutive 0s, so $s_3 = 7$.

(b) For $n > 3$, the n-bit strings with no three consecutive 0s will end with either a) 1, or b) 10, or c) 100.

So, $s_n = s_{n-1} + s_{n-2} + s_{n-3}$.

Example 1.5. Use induction to show the following for Fibonacci numbers: $F_1 + F_2 + F_3 + ... + F_n = F_{n+2} - 1$ for every positive integer n.

Answer

We proceed by induction.

For $n = 1$, we observe that $F_1 = 1$ and $F_3 - 1 = F_1 + F_2 - 1 = 1 + 1 - 1 = 1$, so $F_1 = F_3 - 1$.

We assume that $F_1 + F_2 + F_3 + ... + F_k = F_{k+2} - 1$ for $k \geq 1$.

We show that $F_1 + F_2 + F_3 + ... + F_{k+1} = F_{k+3} - 1$.

$$\begin{aligned} F_1 + F_2 + F_3 + ... + F_{k+1} &= F_1 + F_2 + F_3 + ... + F_k + F_{k+1} \\ &= F_{k+2} - 1 + F_{k+1} \\ &= (F_{k+1} + F_{k+2}) - 1 \\ &= F_{k+3} - 1. \end{aligned}$$

By the Mathematical Principle of Induction it follows that $F_1 + F_2 + F_3 + ... + F_n = F_{n+2} - 1$ for every positive integer n.

Discrete Math I - MTSC 213
Lecture 22

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 22, 2013

1 The Strong Principle of Mathematical Induction

As we mentioned there are several variations of the Principle of Mathematical Induction.

A very useful variation is the Strong Principle of Mathematical Induction.

Definition 1.1 (Strong Principle of Mathematical Induction)**.** The statement

$$\forall n \in \mathbb{N}, P(n) : \text{For every positive integer } n,\ P(n)$$

is true if
(1) $P(1)$ is true and
(2) the statement $\forall k \in \mathbb{N}, P(1) \wedge P(2) \wedge ... \wedge P(k) \Rightarrow P(k+1)$ is true.

The Strong Principle of Mathematical Induction then states that all of the statements $P(1), P(2), P(3), ...$ are true if we can verify that the basis step (1) and the inductive step (2) are true.

If we use a direct proof for the inductive step, we then assume that for an arbitrary positive integer k, the statement $P(i)$ is true for $1 \leq i \leq k$, which we call the induction hypothesis, and show that $P(k+1)$ is a true statement.

So when using the Strong Principle of Mathematical Induction, we can assume that all of the statements $P(1), P(2), ..., P(k)$ are true. We need to show that $P(k+1)$ is true in each situation.

The Strong Principle of Mathematical Induction can be used to verify that the nth term of a recursively defined sequence can be expressed in a closed form (i.e. by a formula).

Example 1.1. A sequence $a_1, a_2, a_3, ...$ is defined recursively by
$a_1 = 1$, $a_2 = 4$ and $a_n = 2a_{n-1} - a_{n-2} + 2$ for $n \geq 3$.
(a) Determine a_3, a_4 and a_5.
(b) Conjecture a formula for a_n for each positive integer n.

Answer
(a) Using the recurrence relation,
$a_3 = 2a_2 - a_1 + 2 = 8 - 1 + 2 = 9$
$a_4 = 2a_3 - a_2 + 2 = 18 - 4 + 2 = 16$
$a_5 = 2a_4 - a_3 + 2 = 32 - 9 + 2 = 25$.
(b) Based on the initial values a_1 and a_2 and the evaluated a_3, a_4 and a_5, we conjecture that a formula for this sequence is $a_n = n^2$ for a positive integer n.

We show next that the above conjecture is correct.

Result 1.2. *A sequence $a_1, a_2, a_3, ...$ is defined recursively by*
$a_1 = 1$, $a_2 = 4$ *and* $a_n = 2a_{n-1} - a_{n-2} + 2$ *for* $n \geq 3$.
Then $a_n = n^2$ for every positive integer n.

Proof
We employ the Strong Principle of Mathematical Induction.

For $n = 1$ we observe that $a_1 = 1 = 1^2$ so the formula holds for $n = 1$.

We assume that for an integer $k \geq 1$, $a_i = i^2$ for $1 \leq i \leq k$.

We now show that $a_{k+1} = (k + 1)^2$.
For $k = 1$, $a_2 = 4 = 2^2$ so the formula is true.
For $k \geq 2$, $k + 1 \geq 3$, so the recurrence relation becomes
$a_{k+1} = 2a_k - a_{k-1} + 2$.
By the inductive hypothesis it follows that

$$\begin{aligned} a_{k+1} &= 2.k^2 - k - 1^2 + 2 \\ &= 2.k^2 - k^2 + 2k - 1 + 2 \\ &= k^2 + 2k + 1 \\ &= (k+1)^2. \end{aligned}$$

By the Strong Principle of Mathematical Induction it follows that the above statement is true.■

Example 1.2. Prove that the nth Fibonacci number is $F_n = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n]$ for $n \geq 1$.

Proof

We proceed by induction.

For $n = 1$, $\frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^1 - (\frac{1-\sqrt{5}}{2})^1] = \frac{1}{\sqrt{5}}(\frac{2\sqrt{5}}{2}) = 1 = F(1)$. Therefore, the statement is true.

We assume that $F_i = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^i - (\frac{1-\sqrt{5}}{2})^i]$ for $1 \leq i \leq k$, $k \geq 1$, $i, k \in \mathbb{Z}$.

We show that $F_{k+1} = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^{k+1} - (\frac{1-\sqrt{5}}{2})^{k+1}]$.

When $k = 1$,

$$\begin{aligned}
&\frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^2 - (\frac{1-\sqrt{5}}{2})^2] \\
&= \frac{1}{\sqrt{5}}[(\frac{1+2\sqrt{5}+5}{2}) - (\frac{1-2\sqrt{5}+5}{4})] \\
&= \frac{1}{\sqrt{5}}(\frac{1+2\sqrt{5}+5-1+2\sqrt{5}-5}{4}) \\
&= \frac{1}{\sqrt{5}}(\frac{4\sqrt{5}}{4}) \\
&= 1 \\
&= F(2).
\end{aligned}$$

When $k \geq 2$,

$$
\begin{aligned}
F_{k+1} &= F_k + F_{k-1} \\
&= \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^k - (\frac{1-\sqrt{5}}{2})^k] + \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-1}] \\
&= \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^k + (\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^k - (\frac{1-\sqrt{5}}{2})^{k-1}] \\
&= \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^k + (\frac{1+\sqrt{5}}{2})^{k-1} - ((\frac{1-\sqrt{5}}{2})^k + (\frac{1-\sqrt{5}}{2})^{k-1})] \\
&= \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^{k-1}(\frac{1+\sqrt{5}}{2}+1) - (\frac{1-\sqrt{5}}{2})^{k-1}(\frac{1-\sqrt{5}}{2}+1)] \\
&= \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^{k-1}(\frac{1+\sqrt{5}}{2})^2 - (\frac{1-\sqrt{5}}{2})^{k-1}(\frac{1-\sqrt{5}}{2})^2] \\
&= \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^{k+1} - (\frac{1-\sqrt{5}}{2})^{k+1}].
\end{aligned}
$$

By the Strong Principle of Mathematical Induction it follows that the formula is true.■

1.1 The Strong Principle of Mathematical Induction (general form)

Definition 1.3 (Strong Principle of Mathematical Induction)**.** For a fixed integer m, let

$$S = \{i \in \mathbb{Z}\} : i \geq m.$$

The statement

$$\forall n \in S, P(n) : \text{For every } n \text{ in } S,\ P(n)$$

is true if

(1) $P(m)$ is true and

(2) the statement $\forall k \in S, P(m) \wedge P(m+1) \wedge ... \wedge P(k) \Rightarrow P(k+1)$ is true.

Result 1.4. *For every integer $n \geq 2$, $F_n \leq 2F_{n-1}$.*

Proof We utilize induction.

For $n = 2$, $F_2 = 1 \leq 2 = 2.F_1$, so the formula is correct.

We assume that $F_i \leq 2.F_{i-1}$ for integer i, $1 \leq i \leq k$ and $k \geq 2, k \in \mathbb{Z}$.

We show that $F_{k+1} \leq 2.F_k$.
$F_{k+1} = F_k + F_{k-1}$, because $k + 1 \geq 3$.
Based on the inductive hypothesis $F_k \leq 2.F_{k-1}$ and $F_{k-1} \leq 2.F_{k-2}$. So,

$$\begin{aligned} F_{k+1} \leq 2.F_{k-1} + 2.F_{k-2} &= 2.(F_{k-1} + F_{k-2}) \\ &= 2.F_k \end{aligned}$$

Therefore $F_{k+1} \leq 2.F_k$.

By the Strong Principle of Mathematical Induction it follows that For every integer $n \geq 2$, $F_n \leq 2F_{n-1}$.■

Corollary 1.5. *For every positive integer n, $F_n \leq 2^n$.*

Proof

We proceed by induction.

For $n = 1$, $F_1 = 1 \leq 2^1 = 2$, so the statement is true.

We assume that $F_k \leq 2^k$ for an integer k with $k \geq 1$.

We show that $F_{k+1} \leq 2^{k+1}$. Based on the previous result
$F_{k+1} \leq 2.F_k \leq 2.2^k = 2^{k+1}$.

By the Principle of Mathematical Induction it follows that for every positive integer n, $F_n \leq 2^n$.■

Discrete Math I - MTSC 213
Lecture 23

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 24, 2013

1 Relations and Functions

This chapter deals with connections between elements of two sets A and B. Depending on the requirements of these connections we will come across the concepts of relations and functions.

1.1 Relations

An object in one set can be related to an object in another set in several ways. For example, an integer a can be related to an integer b if $a+b$ is even, or if a and b have the same parity.

We have also defined the Cartesian product $A \times B$ of two sets A and B to be the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$.

Definition 1.1 (Relation)**.** A relation R from a set A to a set B is a subset of $A \times B$. In addition, R is said to be s relation on $A \times B$. If $(a, b) \in R$, then a is said to be related to b. If $(a, b) \notin R$ then a is not related to b. If $(a, b) \in R$, then we can write $a \ R \ b$, whereas if $(a, b) \notin R$, we write $a \not R \ b$.

Example 1.1. For the sets $A = \{0, 1\}$ and $B = \{1, 2, 3\}$, suppose that

$$R = \{(0, 2), (0, 3), (1, 2)\}$$

is a relation from A to B. Thus, $0 \ R \ 2$, $0 \ R \ 3$ and $1 \ R \ 2$. Since 1 is not related 3 and 0 is not related to 1, we can write $1 \not R 3$ and $0 \not R 1$.

Example 1.2. Let $\mathbb{N}$ be the set of natural numbers and let $\mathbb{N}^-$ be the set of negative integers. A relation R from $\mathbb{N}$ to $\mathbb{N}^-$ is defined by $a\ R\ b$ if $a+b \in \mathbb{N}$. Let's examine some examples of ordered pairs to see if they are related by R.

Answer
$5\ R$ -1 because $5 + (-1) = 4 \in \mathbb{N}$
$18\ R$ -5 because $18 + (-5) = 13 \in \mathbb{N}$
$15\ \not R$ -15 because $15 + (-15) = 0 \notin \mathbb{N}$
$7\ R$ -25 because $7 + (-25) = -18 \notin \mathbb{N}$

Definition 1.2. A relation R on a set S is a relation from S to S. That is, R is a relation on a set S if R is a subset of $S \times S$.

Example 1.3. We know that if a set A has n elements, then there exist 2^n subsets of A. So if a set A has 3 elements, then $A \times A$ has 9 elements and there are $2^9 = 512$ possible subsets of $A \times A$ therefore 512 possible relations on S.

We list 5 out of the possible 512 relations on the set $A = \{x, y, z\}$
$R_1 = \{(x, y), (x, z), (z, z)\}$
$R_2 = \{(x, y), (y, y), (y, z)\}$
$R_3 = \{(x, x), (y, y), (z, z)\}$
$R_4 = \emptyset$

Definition 1.3. Let R be a relation defined on a nonempty set S. Then R is

(1) reflexive if $a\ R\ a$ for all $a \in S$; that is, if $a \in S$, then $(a, a) \in R$;

(2) symmetric if whenever $a\ R\ b$, then $b\ R\ a$ for all $a, b \in S$; that is, if $(a, b) \in R$ then $(b, a) \in R$;

(3) transitive if whenever $a\ R\ b$ and $b\ R\ c$, then $a\ R\ c$ for all $a, b, c \in S$; that is, if $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

We have seen that for a false statement P and any statement Q, the implication $P \to Q$ is always true. We note here that if we have an empty relation R, defined on a nonempty set S, then R is symmetric, because for all $a, b \in S$ $(a, b) \in R$ is false. Also, the empty relation is transitive because for all $a, b, c \in S$ $(a, b) \in R$ is false and $(b, c) \in R$ is false. But, the empty relation is not reflexive because for all $a \in S$, $(a, a) \in R$ is false.

Example 1.4. A relation R is defined on the set $\mathbb{Z}$ of integers by $a\ R\ b$ if $a.b \geq 0$. Please examine if R possesses the reflexivity, symmetry and transitivity properties.

Answer

Let $a \in \mathbb{Z}$. Because $a \cdot a \geq 0$, it follows that $a\ R\ a$ for all $a \in \mathbb{Z}$ so the relation is reflexive.

Now let $a, b \in \mathbb{Z}$. Assume that $a \cdot b \geq 0$. Because $a \cdot b = b \cdot a$, $b \cdot b \geq 0$. Therefore the relation R is symmetric.

Finally, let $a, b, c \in \mathbb{Z}$. For example, $a = 3$, $b = 0$ and $c = -5$. Then $a \cdot b \geq 0$ and $b \cdot c \geq 0$, but $a \cdot b < 0$, so R is not transitive.

Discrete Math I - MTSC 213
Lecture 24

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 25, 2013

1 Equivalence Relations

Definition 1.1 (Equivalence Relation)**.** A relation R on a nonempty set is an equivalence relation if R is reflexive, symmetric and transitive.

Example 1.1. A relation R is defined on $\mathbb{N} \times \mathbb{N}$ by $(a, b)\ R\ (c, d)$ if $ad = bc$. Show that R is an equivalence relation.

Proof
Let $(a, b) \in \mathbb{N} \times \mathbb{N}$. Because $ab = ba$, $(a, b)\ R\ (a, b)$, so R is reflexive.

Let $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ and $(a, b)\ R\ (c, d)$. Therefore $ad = bc$.
Because $ad = da$ and $bc = cb$, it follows that $cb = da$.
Therefore $(c, d)\ R\ (a, b)$, which implies that R is symmetric.

Let $(a, b), (c, d), (e, f) \in \mathbb{N} \times \mathbb{N}$ such that $(a, b)\ R\ (c, d)$ and $(c, d)\ R\ (e, f)$. This means that $ad = bc$ and $cf = de$.
Because $ad = bc$ we have that $c = \frac{ad}{b}$ and $cf = de$ becomes $\frac{ad}{b} f = de \Rightarrow af = be$.

This means that $(a, b)\ R\ (e, f)$, therefore R is transitive.
Because R is reflexive, symmetric and transitive it follows that R is an equivalence relation.■

1.1 Equivalence Classes

Definition 1.2 (Equivalence Class)**.** Let R be an equivalence relation on set A. For $a \in A$, the equivalence class $[a]$ is defined by

$$[a] = \{x \in A : x \ R \ a\}.$$

So for an equivalence relation R on a set A and an element $a \in A$, the equivalence class is the set of all elements of A that are related to a by R.

Example 1.2. A relation R is defined on the Cartesian product $\mathbb{N} \times \mathbb{N}$ such that $(a, b) \ R \ (c, d)$ if $ad = bc$. Since R is an equivalence relation, there is an equivalence class associated with each element of $\mathbb{N} \times \mathbb{N}$. For example

$$\begin{aligned}[(2,3)] &= \{(x,y) \in \mathbb{N} \times \mathbb{N} : (x,y)R(2,3)\} \\ &= \{(x,y) \in \mathbb{N} \times \mathbb{N} : 3x = 2y\} \\ &= \{(4,6),(6,9),(8,12),(10,15),...\}\end{aligned}$$

We can generalize this as follows: the equivalence class of $[a, b]$ is the set of all ordered pairs (c, d) such that $\frac{c}{d} = \frac{a}{b}$.

Example 1.3. A relation R is defined on $\mathbb{Z}$ by $a \ R \ b$ if $a + b$ is even.

(a) Show that R is an equivalence relation.

(b) Describe the equivalence classes [0], [1], $[-7]$, 6.

(a) **Proof**

Let $a \in \mathbb{Z}$. Then $a+a = 2a$, which is an even integer. Therefore $(a, a) \in R$ and R is reflexive.

Let $a, b \in \mathbb{Z}$ and $(a, b) \in R$. This means that $a + b$ is even. Because $a + b = b + a$, $b + a$ is even. Therefore, $(b, a) \in R$ and R is symmetric.

We assume that $a, b, c \in \mathbb{Z}$ and $(a, b) \in R$ and $(b, c) \in R$. This means that $a + b$ is even and $b + c$ is even.

Therefore, there exist $x, y \in \mathbb{Z}$ such that $a + b = 2x$ and $b + c = 2y$.

We have that $a + b + b + c = 2x + 2y \Rightarrow a + c = 2x + 2y - 2b \Rightarrow a + c = 2(x + y - b)$.

Because of fundamental integer properties $x + y - b$ is an integer, so $a + c$ is even. This means that $(a, c) \in R$, so R is transitive.

Because R is reflexive, symmetric and transitive, R is an equivalence relation.■

(b) The resulting equivalence classes are

$$\begin{aligned}[0] &= \{k \in \mathbb{Z} : (k,0) \in R\} \\ &= \{k \in \mathbb{Z} : k+0 \text{ is even}\} \\ &= \{..., -4, -2, 0, 2, 4, ...\}\end{aligned}$$

$$\begin{aligned}[1] &= \{k \in \mathbb{Z} : (k,1) \in R\} \\ &= \{k \in \mathbb{Z} : k+1 \text{ is even}\} \\ &= \{..., -3, -1, 1, 3, ...\}\end{aligned}$$

$$\begin{aligned}[-7] &= \{k \in \mathbb{Z} : (k,-7) \in R\} \\ &= \{k \in \mathbb{Z} : k-7 \text{ is even}\} \\ &= \{..., -3, -1, 1, 3, ...\}\end{aligned}$$

$$\begin{aligned}[6] &= \{k \in \mathbb{Z} : (k,6) \in R\} \\ &= \{k \in \mathbb{Z} : k+6 \text{ is even}\} \\ &= \{..., -4, -2, 0, 2, 4, ...\}\end{aligned}$$

We observe that $[0] = [6]$ and $[1] = [-7]$.

Theorem 1.3. *Let R be an equivalence relation on a nonempty set A and let a and b be elements of A. Then*

$$[a] = [b] \text{ if and only if } a \ R \ b.$$

Proof This is a biconditional so we will prove that i) if $a \ R \ b$, then $[a] = [b]$ and ii) if $[a] = [b]$, then $a \ R \ b$.

i) Let $a \ R \ b$. To verify that $[a] = [b]$ we need to show that $[a] \subseteq [b]$ and $[b] \subseteq [a]$.

First let $x \in [a]$. Then $(x, a) \in R$.

Because $a \ R \ b$, $(a, b) \in R$.

So, $(x, a) \in R$ and $(a, b) \in R$, and by the transitivity property it follows that $(x, b) \in R$, which means that $x \in [b]$.

Therefore $[a] \subseteq [b]$.

Now we assume that $x \in [b]$ so $(x, b) \in R$.

Because $a \ R \ b$, $(a, b) \in R$ and $(b, a) \in R$.

Therefore $(x, b) \in R$ and $(b, a) \in R$, so by the transitivity property it follows that $(x, a) \in R$.

This means that $x \in [a]$ and because we assume that $x \in [b]$, then $[b] \subseteq [a]$.

Because $[a] \subseteq [b]$ and $[b] \subseteq [a]$, we have that $[a] = [b]$.

ii) Let $[a] = [b]$. If $x \in [a]$, then $x \in [b]$, which means that $(x, a) \in R$ and $(x, b) \in R$. Because R is symmetric $(a, x) \in R$ and by the transitivity property it follows that $(a, b) \in R$, that is $a \ R \ b$.■

Theorem 1.4. *Let R be an equivalence relation defined on a nonempty set A. If $\mathcal{P}$ is the set of all distinct equivalence classes of A resulting from R, then $\mathcal{P}$ is a partition of A.*

Proof We have seen that each equivalence class is nonempty, and that each element of A belongs to an equivalence class. We need to show that the equivalence classes are disjoint, that is distinct equivalence classes have no common elements.

We use proof by contradiction. We assume two distinct equivalence classes $[a]$ and $[b]$ that have a common element x. So, $(x, a) \in R$ and $(x, b) \in R$. By the symmetry property we have that $(a, x) \in R$. Because $(a, x) \in R$ and $(x, b) \in R$, by the transitivity property it follows that $(a, b) \in R$. By the previous theorem it follows that $[a] = [b]$, which is a contradiction. Therefore $[a]$ and $[b]$ are disjoint and $\mathcal{P}$ is a partition of A.■

Corollary 1.5. *Let R be an equivalence relation defined on a nonepty set A. If $[a]$ and $[b]$ are equivalence classes of A resulting from R, then either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.*

Based on the previous result, if $a \ R \ b$, then $[a] = [b]$. On the contrary, if $a \not R \ b$, then $[a] \cap [b] = \emptyset$. Also, if $[a] \cap [b] \neq \emptyset$, then $[a] = [b]$.

Example 1.4. A relation R is defined on $\mathbb{Z}$ by $a \ R \ b$ if $3a - 7b$ is even.

(a) Prove that R is an equivalence relation.

(b) Describe the distinct equivalence classes resulting from R and show that the set of all equivalent classes forms a partition of $\mathbb{Z}$.

(a) **Proof**.

Let $x \in \mathbb{Z}$.

We observe that $3x - 7x = -4x = 2(-2x)$, which is an even number, so $(x, x) \in R$. Hence R is reflexive.

Now let $x, y \in \mathbb{Z}$ and $(x, y) \in R$.

Then $3x - 7y$ is even, so

$3x - 7y = 2k \Rightarrow 3x = 7y + 2k$, $k \in \mathbb{Z}$.

Then $3y - 7x = 3y - 4x - 3x = 3y - 4x - 7y - 2k = 4x - 4y - 2k = 2(2x - 2y - k)$. Because $2x - 2y - k$ is an integer, $3y - 7x = 2k$ is even, hence $(y, x) \in R$ and R is symmetric.

Finally let $x, y, z \in \mathbb{Z}$ such that $(x, y) \in R$ and $(y, z) \in R$.

This means that $3x - 7y$ is even and $3y - 7z$ is even. So, $3x - 7y = 2k$ and $3y - 7z = 2l$ for some $k, l \in \mathbb{Z}$.

Then, $3x - 7y + 3y - 7z = 2k + 2l \Rightarrow 3x - 7z = 2k + 2l + 4y \Rightarrow 3x - 7z = 2(k + l + 2y)$.

Because $k + l + 2y$ is an integer, $3x - 7z$ is even. Hence, $(x, z) \in R$ and the transitivity property holds true.

Because of the reflexivity, symmetry and transitivity properties it follows that R is an equivalence relation.■

(b) Let's begin with the class [0].

$$\begin{aligned}[0] &= \{a \in \mathbb{Z} : 3a \text{ is even}\} \\ &= \{..., -4, -2, 0, 2, 4, ...\}.\end{aligned}$$

Because the equivalence classes form a partition of $\mathbb{Z}$, then we expect to generate another class by selecting an element that does not belong to [0]. So we choose [1].

$$\begin{aligned}[1] &= \{b \in \mathbb{Z} : 3b - 7 \text{ is even}\} \\ &= \{..., -3, -1, 1, 3, ...\}.\end{aligned}$$

We observe that $\{[0], [1]\}$ is a partition of $\mathbb{Z}$.■

Discrete Math I - MTSC 213
Lecture 25

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 28, 2013

1 Functions

Definition 1.1 (Function)**.** Let A and B be two nonempty sets. A function from A to B is a relation from A to B that associates with each element of A a unique element of B. A function f from A to B is denoted by $f : A \to B$.

A function $f : A \to B$ can be described as a subset of $A \times B$ such that for every element a of A there is exactly one ordered pair in f in which a is the first coordinate.

Therefore, if g is a relation from set A to set B and either

(a) there is an element a' of A that is not the first coordinate of any ordered pair in g or

(b) there are more than one ordered pairs in g of which an element a'' is the first coordinate

then g is not a function from A to B.

Example 1.1. Let f be a function from a set $A = \{a_1, a_2, a_3, a_4\}$ to a set $B = \{b_1, b_2, b_3\}$ that assigns

- to a_1 element b_3
- to a_2 element b_1
- to a_3 element b_2
- to a_4 element b_1

Therefore f consists of the following ordered pairs:

$$f = \{(a_1, b_3), (a_2, b_1), (a_3, b_2), (a_4, b_1)\}.\blacksquare$$

Now we introduce some function terminology. Let $f : A \to B$ and $b \in B$ a unique element assigned to $a \in A$. Then we write $b = f(a)$ and say that b is f of a and that b is the image of a under f. In the previous example b_3 is the image of a_1 under f.

Definition 1.2. If $f : A \to B$ is a function from a set A to a set B, then A is called the domain of f and B is the codomain of f. The range $f(A)$ is the set of images of the elements of A, namely

$$f(A) = \{f(a) : a \in A\}.$$

For the function f of the previous example the domain of f is $A = \{a_1, a_2, a_3, a_4\}$ and the codomain of f is $B = \{b_1, b_2, b_3\}$. The range of f is $\{b_1, b_2, b_3\}$.

Definition 1.3 (image)**.** For a function f from a set A to a set B and a subset X of A, the image of X under f is the set

$$f(X) = \{f(x) : x \in X\}.$$

If a set X is $X \subseteq A$, then $f(X) \subseteq B$. Also, if $X = A$ then $f(X) = f(A)$ that is the range of f. If $X = \{a_2, a_4\}$, then $f(X) = \{b_1\}$.

1.1 Representations of Functions

We often use diagrams to represent functions. Arrows connect the elements between A and B.

Example 1.2. For each real number x, let $f(x)$ denote any real number y such that (x, y) lies on the circle $x^2 + y^2 = 25$. Is f a function from $\mathbb{R}$ to $\mathbb{R}$?

Answer f is not a function from R to R. First let's consider $x = 7$. Then there is no coordinate y such that $7^2 + y^2 = 25$.

Also, let $x = 3$. Then $3^2 + y^2 = 25$, $y^2 = 25 - 9$, $y^2 = 16$, so $y = \pm 4$ and f is not a function because for a single x we have two images.■

Example 1.3. Let $A = \{a, b\}$ and $B = \{1, 3\}$. Determine all functions from A to B.

Answer The functions are
$f_1 = \{(a, 1), (b, 1)\}$
$f_2 = \{(a, 1), (b, 3)\}$
$f_3 = \{(a, 3), (b, 1)\}$
$f_4 = \{(a, 3), (b, 3)\}$

For two nonempty sets A and B of real numbers and a function $f : A \to B$ the graph of f is the set of points (x, y) such that $y = f(x)$ when $x \in A$ and $y \in B$.

1.2 Common Functions

1.2.1 Identity Function

For a nonempty set A, the function $f : A \to A$ defined by $f(a) = a, \forall a \in A$ is called the identity function.

For example, given the set $A = \{1, 2\}$, the range of the identity function is $f(A) = \{(1, 1), (2, 2)\}$.

1.2.2 Absolute Value Function

The absolute value function is defined as the function $f : A \to A$ where

$$f(x) = |x| \begin{cases} x, \text{ if } x \geq 0 \\ -x, \text{ if } x < 0. \end{cases}$$

1.2.3 Ceiling Function

For a real number r the ceiling of r is the nearest integer $\lceil r \rceil$ that is greater than or equal to r.

The function $f : \mathbb{R} \to \mathbb{Z}$ defined by $f(x) = \lceil x \rceil$ is the ceiling function.

1.2.4 Floor Function

For a real number r the floor of r is the nearest integer $\lfloor r \rfloor$ that is greater than or equal to r.

The function $f : \mathbb{R} \to \mathbb{Z}$ defined by $f(x) = \lfloor x \rfloor$ is the floor function.

1.2.5 Logarithmic and Exponential Functions

Let $a \in \mathbb{R}^+$, such that $a \neq 1$. If $b \in \mathbb{R}$ and $a^b = c$ then $\log_a c = b$. Therefore,

$$\log_a c = b \text{ iff } a^b = c.$$

We note that $c \in \mathbb{R}^+$. Also, a is called the base.

Well known functions in calculus and computer science are

$$y = \log_e x = \text{iff } x = e^y.$$
$$y = \log_2 x = b \text{ iff } x = 2^y.$$

Example 1.4. The function $f : \mathbb{R} \to \mathbb{R}^+$ defined by $f(x) = 2^x$ is an exponential function.

The function $f : \mathbb{R}^+ \to \mathbb{R}$ defined by $f(x) = \log_e(x) = \ln(x)$ is the natural logarithmic function.

1.3 Composition of Functions

Definition 1.4 (Composition)**.** Let A, B and C be sets and suppose that $f : A \to B$ and $g : B \to C$ are two functions. The composition $g \circ f$ of f and g is the function from A to C defined by

$$(g \circ f)(a) = g(f(a)) \text{ for } a \in A.$$

Example 1.5. Let $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$, where $f(x) = \sin x$ and $g(x) = x^2$. Determine $(f \circ g)(x)$ and $(g \circ f)(x)$.

Answer Because the domain and codomain are the same set, both $(f \circ g)(x)$ and $(g \circ f)(x)$ are defined. So for $x \in \mathbb{R}$ we have

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

Example 1.6. Let $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$ and $C = \{x, y, z\}$ and let $f : A \to B$ and $g : B \to C$ be functions where

$$f = \{(1, c), (2, a), (3, b)\} \text{ and } g = \{(a, x), (b, z), (c, x), (d, z)\}.$$

Find $g \circ f$.

Answer We have to find the ordered pairs $(a, g(f(a))), \forall a \in A$. Therefore
$(g \circ f)(1) = g(f(1)) = g(c) = x$
$(g \circ f)(2) = g(f(2)) = g(a) = x$
$(g \circ f)(3) = g(f(3)) = g(b) = z.$
So $g \circ f = \{(1, x), (2, x), (3, z)\}$.■

Discrete Math I - MTSC 213
Lecture 26

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

October 30, 2013

1 Surjective, Injective, Bijective and Inverse Functions

This section deals with functions from a set A to a set B that satisfy one or both of the following properties

- each element of B is the image of at most one element of A
- each element of B is the image of at least one element of A

These properties are encountered often so it is useful to become familiar with such functions.

1.1 One-to-one Functions

Definition 1.1. For two nonempty sets A and B, a function $f : A \to B$ is said to be one-to-one if every two distinct elements of A have distinct images in B, that is, if $a, b \in A$ and $a \neq b$, then $f(a) \neq f(b)$.

An one-to-one function is referred to as an injective function.

Example 1.1. For two nonempty finite sets A and B , let $f : A \to B$ be the identity function, that is, $f(a) = a$ for every element $a \in A$.

The function f is one-to-one because by definition if $a \neq b$, $a, b \in A$, then $f(a) \neq f(b)$.

Let f be a function $f : A \to B$, where A and B are finite sets and f is an one-to-one function.

Then different elements in A will have different images in B. Therefore, if A has N elements, $|A| = N$, then B has to have at least N elements, $|B| \geq N$. Then we have,

If $f : A \to B$ is one-to-one, then we must have $|B| \geq |A|$.

The contrapositive of this is

If $|B| < |A|$, then there is no one-to-one function f, $f : A \to B$.

Sometimes, it is more straightforward to show that a function is one-to-one using the contrapositive of the definition, that is,

A function $f : A \to B$ is one-to-one, if for $a, b \in A$ and $f(a) = f(b)$, then $a = b$.

Result 1.2. *Let $f : \mathbb{R} \to \mathbb{R}$ be a function defined by $f(x) = 5x - 3$ for $x \in \mathbb{R}$. Then f is one-to-one.*

Proof. Let $a, b \in A$ and $f(a) = f(b)$. Then

$5a - 3 = 5b - 3$

$5a = 5b$

$a = b$.

Based on the previous technique, we can show that a function is not one-to-one by finding distinct elements a and b such that $a \neq b$, for which $f(a) = f(b)$. □

Example 1.2. Show that the functions are not one-to-one:

(a) $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x^2 + 1$ for $x \in \mathbb{R}$

(b) $g : \mathbb{Z} \to \mathbb{Z}$ such that $g(x) = \lceil n/2 \rceil$ for $n \in \mathbb{Z}$.

Answer

(a) For $a = -3$ and $b = 3$, that is $a \neq b$, $f(a) = 10$ and $f(b) = 10$, $f(a) = f(b)$. So f is not one-to-one.

(b) For $c = 3$ and $d = 4$, that is $c \neq d$, $f(c) = 2$ and $f(d) = 2$, that is $f(c) = f(d)$, therefore g is not one-to-one.

1.2 Onto Functions

Definition 1.3. Let A and B be two nonempty sets. A function $f : A \to B$ is called onto if every element of B is the image of some element of A.

So, a function $f : A \to B$ is onto, if every element $b \in B$ is an image of an element $a \in A$, that is, $b = f(a)$. Therefore, the codomain B is equal to the range of A, $B = f(A)$. This type of function is also called a surjective function.

So, a function $f : A \to B$ is onto if every element $b \in B$ is an image of an element $a \in A$. Therefore if A has N elements, then B has at most N elements. It follows that

$$\text{If } f : A \to B \text{ is onto, then } |B| \leq |A|.$$

The contrapositive of this is

$$\text{If } |B| > |A| \text{ , then there is no onto function } f : A \to B.$$

Result 1.4. *The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 4x - 9$ for $x \in \mathbb{R}$ is onto.*

Proof. We begin with an arbitrary number $r \in \mathbb{R}$. We need to show that r is the image of a real number x under f. To find this number we solve for x

$$\begin{aligned} 4x - 9 &= r \\ 4x &= r + 9 \\ x &= \frac{r+9}{4} \end{aligned}$$

Next, we evaluate $f(\frac{r+9}{4})$

$$\begin{aligned} f(\frac{r+9}{4}) &= 4(\frac{r+9}{4}) - 9 \\ &= r + 9 - 9 \\ &= r \end{aligned}$$

Therefore r is the image of $\frac{r+9}{4}$ and f is onto. □

1.3 Bijective Functions

Definition 1.5. A function that is one-to-one and onto is called a bijective function, or one-to-one correspondence.

Result 1.6. *The function* $f : \mathbb{R}^+ \to \mathbb{R}^+$ *defined by* $f(x) = \sqrt{x}$ *is bijective.*

Proof. We need to show that f is one-to-one and onto.

First, we show that f is one-to-one. Let $a, b \in \mathbb{R}^+$ such that $f(a) = f(b)$. Then $\sqrt{a} = \sqrt{b}$, $(\sqrt{a})^2 = (\sqrt{b})^2$, $a = b$. Therefore, f is one-to-one.

Next, we show that f is onto. Let r be an arbitrary number $r \in \mathbb{R}^+$. Then, let $x = r^2$, so $x \in \mathbb{R}^+$. We observe that $f(r^2) = \sqrt{r^2} = r$, therefore f is onto.

Because f is one-to-one and onto, f is bijective. □

For a nonempty set A, a bijective function from A to A is also called a permutation of A.

1.4 Compositions of Bijective Functions

Theorem 1.7. *Let A, B and C be nonempty sets and let $f : A \to B$ and $g : B \to C$ be two functions.*

(a) If f and g are one-to-one, then so is $g \circ f$.

(b) If f and g are onto, then so is $g \circ f$.

Proof. (a) We assume that $f : A \to B$ and $g : B \to C$ are one-to-one functions. Then, let $a, b \in A$, such that $(g \circ f)(a) = (g \circ f)(b)$. We have that

$$\begin{aligned} (g \circ f)(a) &= (g \circ f)(b) \\ g(f(a)) &= g(f(b)) \end{aligned}$$

Because g is one-to-one, $f(a) = f(b)$. In addition,f is one-to-one, therefore $a = b$. It follows that $g \circ f$ is one-to-one.

(b) We assume that $f : A \to B$ and $g : B \to C$ are onto. Let an arbitrary $c \in C$. We need to show that there exists some element $a \in A$ such that $(g \circ f)(a) = c$.

Because g is onto, there exists an element $b \in B$ such that $g(b) = c$.

In addition, because f is onto, there is an element $a \in A$ such that $f(a) = b$.

It follows that

$$c = g(b) = g(f(a)) = (g \circ f)(a),$$

that is, $g \circ f$ is onto.

Because $g \circ f$ is one-to-one and onto it follows that $g \circ f$ is bijective.

□

Corollary 1.8. *Let A, B and C be nonempty sets and let $f : A \to B$ and $g : B \to C$ be two functions. If f and g are bijective, then so is $g \circ f$.*

1.5 Inverse Functions

Let a bijective function $f : A \to B$ and $(a, b) \in f$ an arbitrary ordered pair such that $a \in A$ and $b \in B$. The inverse function of f denoted by f^{-1} is obtained from f by replacing the ordered pair (a, b) with (b, a).

Theorem 1.9. *Let A and B be nonempty sets. A function $f : A \to B$ has an inverse function $f^{-1} : B \to A$ if and only if f is bijective. Moreover, if f is bijective, then so is f^{-1}.*

Example 1.3. The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^7 - 4$ for $x \in \mathbb{R}$ is known to be bijective. Determine f^{-1} for $x \in \mathbb{R}$.

Answer

Let $y \in \mathbb{R}$, such that $y = x^7 - 4$. In f^{-1} the image of y is $x = f^{-1}(y)$. Then we have that

$$\begin{aligned} y &= x^7 - 4 \\ x^7 &= y + 4 \\ x &= (y + 4)^{1/7} \end{aligned}$$

We observe that x is the image of y under $(y + 4)^{1/7}$. Hence, for $x \in \mathbb{R}$ the image of x under f^{-1} is $(x + 4)^{1/7}$. It follows that $f^{-1}(x) = (x + 4)^{1/7}$.

Theorem 1.10. *For nonempty sets A and B. let $f : A \to B$ be a bijective function. Then*

(a) $f^{-1} \circ f$ is the identity function on A and

(b) $f \circ f^{-1}$ is the identity function on B.

Discrete Math I - MTSC 213
Lecture 27

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 3, 2013

1 Cardinalities of Sets

1.1 Sets Having the Same Cardinality

Definition 1.1. Two nonempty sets A and B (finite or infinite) are defined to have the same cardinality, written $|A| = |B|$, if there exists a bijective function from A to B.

This definition is expected for finite sets but leads to interesting observations for infinite sets.

Assuming two infinite sets A and B with equal cardinalities, that is $|A| = |B|$, we observe that there is a bijective function $f : A \to B$. Because f is bijective, there exists an inverse function $f^{-1} : B \to A$ that is also bijective. So, to show that two infinite sets have the same cardinality we need to establish the existence of a bijective function either from A to B, or from B to A.

1.2 Denumerable Sets

Definition 1.2. A set A is called denumerable if $|A| = |\mathbb{N}|$.

So a set A is denumerable if there exists a bijective function from A to $\mathbb{N}$ or from $\mathbb{N}$ to A. The set of natural numbers $\mathbb{N}$ is denumerable because the identity function is bijective.

Result 1.3. *The set of positive even numbers is denumerable.*

Solution

Consider the function $f : \mathbb{N} \to A$, where A is the set of positive even integers, defined by $f(n) = 2n$ for $n \in \mathbb{N}$. We need to show that f is one-to-one and onto, therefore bijective, to establish that A is denumerable.

First, we assume two positive integers a, b, such that $f(a) = f(b)$, that is, $2a = 2b$. This leads to $a = b$, hence the function is one-to-one.

Next, we assume an arbitrary positive even integer r, which can be written as $r = 2k$, $k \in \mathbb{N}$. Therefore $r = f(k)$, thus f is onto.

We see that $f : \mathbb{N} \to A$ is bijective, therefore $|A| = |\mathbb{N}|$, and A is denumerable.

Theorem 1.4. *The function $f : \mathbb{N} \to \mathbb{Z}$ defined by*

$$f(n) = (-1)^n \lfloor n/2 \rfloor$$

for each $n \in \mathbb{N}$ is bijective.

Proof. (i) To show that f is one-to-one we assume that $f(a) = f(b)$ and show that $a = b$. We divide the co-domain into three cases.

(a) Let $f(a) = f(b) = 0$.
Then $a = b = 1$, so the function is one-to-one at $n = 1$.

(b) Let $f(a) = f(b) > 0$.
Then a and b are both even, that is $a = 2m$, $b = 2n$, $m, n \in \mathbb{N}$.
Then, $f(a) = m$ and $f(b) = n$.
Because $f(a) = f(b)$, we have that $m = n$, therefore, $a = b$.

(c) Let $f(a) = f(b) < 0$. Then a and b are both odd, that is, $a = 2m + 1$, $b = 2n + 1$, $m, n \in \mathbb{N}$.

(ii) Next, we show that f is onto.
Let $k \in \mathbb{Z}$.
If $k > 0$, then $f(2k) = k$.
If $k \leq 0$, then $f(-2k + 1) = k$.
Therefore f is onto.

□

Corollary 1.5. *The set of integers is denumerable.*

We showed that $|\mathbb{N}| = |\mathbb{Z}|$. This may seem counter-intuitive but when we deal with cardinalities we need to rely on definitions.

Theorem 1.6. *The set of positive rational numbers is denumerable.*

Please study the proof in Chartrand and Zhang textbook.

Theorem 1.7. *The set $\mathbb{Q}$ of rational numbers is denumerable.*

Proof. According to the previous theorem, $\mathbb{Q}^+$ is denumerable, so there is a bijective function $f : \mathbb{N} \to \mathbb{Q}^+$. If q_n denotes the image of n under f, then $\mathbb{Q}^+ = \{q_1, q_2, q_3, ...\}$, so $\mathbb{Q}$ can be defined by $\mathbb{Q} = \{0, q_1, -q_1, q_2, -q_2, q_3, -q_3, ...\}$.

We can define a bijective function $g : \mathbb{N} \to \mathbb{Q}$, as follows

$1 \to 0$
$2 \to q_1$
$3 \to -q_1$
$4 \to q_2$
$5 \to -q_2$
.
.
.

Therefore $|\mathbb{N}| = |\mathbb{Q}|$, which means that $\mathbb{Q}$ is denumerable. □

At this point we should note the following observation:

A set A is denumerable if and only if it is possible to list the elements of A as $a_1, a_2, a_3, ...$, that is, there is an infinite sequence $\{a_n\}$ in which every element of A appears exactly once.

Theorem 1.8. *Every infinite subset of a denumerable set is denumerable.*

Theorem 1.9. *The closed interval $[0, 1]$ of real numbers is not denumerable.*

Please study the proof in Chartrand and Zhang textbook.

Discrete Math I - MTSC 213
Lecture 28

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 4, 2013

0.1 Countable and Uncountable Sets

Definition 0.1. A set that is either finite or denumerable is called countable. A denumerable set is also called coutably infinite. A set that is not countable is called uncountable.

Therefore $\{1, 2, 3\}, \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are countable, but $[0, 1]$ is uncountable.

Theorem 0.2. *Every set that contains an uncountable subset is itself uncountable.*

Proof. Assume that there is a countable set A that contains an uncountable set B.

Because B is uncountable, B is infinite.

Because $B \subseteq A$, A is also infinite.

We observe that A is infinite and countable, therefore denumerable.

According to a theorem of the previous section any infinite subset of a denumerable set is also denumerable, therefore B is also denumerable.

This is a contradiction because we assumed that B is uncountable. □

We showed before that $[0, 1]$ is uncountable. As a consequence we have the following corollary.

Corollary 0.3. *The set $\mathbb{R}$ of real numbers is uncountable.*

The set $\mathbb{C}$ of complex numbers contains the set $\mathbb{R}$ of real numbers, that is $\mathbb{R} \subseteq \mathbb{C}$. According to the previous theorem we conclude the following.

Corollary 0.4. *The set $\mathbb{C}$ of complex numbers is uncountable.*

Theorem 0.5. *If A and B are disjoint denumerable sets, then $A \cup B$ is denumerable.*

Proof. Sets A and B are denumerable, therefore they can be expressed as

$$A = \{a_1, a_2, ...\} \text{ and } B = \{b_1, b_2, b_3, ...\}.$$

We can define a function $f : \mathbb{N} \to A \cup B$ as follows

1	2	3	4	5	...
a_1	b_1	a_2	b_2	a_3	...

Because f is bijective, then $A \cup B$ is denumerable. □

Theorem 0.6. *The set $\mathbb{I}$ of irrational numbers is uncountable.*

Proof. Let's assume that $\mathbb{I}$ is countable.

Because $\mathbb{Q}$ is countable, $\mathbb{Q} \cup \mathbb{I}$ is countable according to previous theorem.

Because $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$, it follows that the set of real numbers $\mathbb{R}$ is countable.

This contradicts our previous corollary, so $\mathbb{I}$ must be uncountable. □

We have reviewed methods for investigating the equality between cardinalities of two sets A and B. Using our function properties we can investigate inequalities between sets.

For example, for two nonempty sets A and B we showed that $|A| \leq |B|$, if there is an one-to-one function $f : A \to B$.

Furthermore, for two nonempty sets A and B we showed that $|A| = |B|$, if there exists a bijective function $f : A \to B$.

By definition $|A| < |B|$ means that $A \subseteq B$ and $A \neq B$. Therefore $|A| < |B|$, if there is a function $f : A \to B$ that is one-to-one but not bijective.

For example, if $A = \{a, b, c\}$ and $B = \{w, x, y, z\}$, then $|A| < |B|$.

Following the function properties, we can also show that $|\mathbb{Z}| < |\mathbb{R}|$.

Theorem 0.7. *Every set has a smaller cardinality than its power set, that is,*

$$|A| < |\mathcal{P}(A)|$$

for every set A.

Please study the proof in Chartrand and Zhang's textbook.

Based on the previous theorem we observe the following.

Corollary 0.8. *There is no set of largest cardinality.*

Discrete Math I - MTSC 213
Lecture 29

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 6, 2013

1 Integers

The branch of mathematics that deals with properties of integers has been traditionally called number theory.

In this chapter we will review the fundamentals of number theory.

Number theory has practical importance as it is linked with specific topics of computer science. One such topic is cryptography.

1.1 Divisibility Properties

1.1.1 Terminology

For integers a and b with $a \neq 0$, we say that a divides b if $b = ac$ for some integer c. We indicate this by writing $a \mid b$.

Therefore an integer n is even if and only if $2 \mid n$.

If $a \mid b$ then a is called a factor or divisor of b, and b is called a multiple of a.

For any two given integers a and b $a \mid b$ is a statement. For example $2 \mid 5$ is a false statement, while $2 \mid 6$ is a true statement.

If a does not divide b, we write $a \nmid b$.

We will prove some divisibility properties of integers next. We note that to show that $a \mid b$ then we need to show that there is an integer c such that $b = ac$. More frequently used proof methods in such problems are the direct proof and proof by induction.

Theorem 1.1. *Let a, b and c be integers with $a \neq 0$. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*

Proof. Assume that $a \mid b$ and $a \mid c$, that is $b = da$ and $c = ea$ for some $d, e \in \mathbb{Z}$. Then $b + c = da + ea = (d + e)a$.

Because $d + e \in \mathbb{Z}$ it follows that $a \mid b + c$. □

Theorem 1.2. *Let a and b be integers with $a \neq 0$. If $a \mid b$, then $a \mid bx$ for every integer x.*

Proof. Let $a \mid b$ for $a, b \in \mathbb{Z}$ and $a \neq 0$. Then $b = ra$ for some integer r.

We multiply both sides with an integer x and get $bx = xra = (xr)a$. Because $xr \in \mathbb{Z}$ this can be written as $a \mid bx$. □

Theorem 1.3. *Let a and b be integers with $a \neq 0$. If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for every two integers x and y.*

Proof. This can be considered to be a generalization of the previous two theorems.

Let $a \mid b$ and $a \mid c$ with $a \neq 0$. It follows that $b = ra$ and $c = sa$ for some $r, s \in \mathbb{Z}$.

Then we have that $bx = rax$ and $cy = say$ for $x, y \in \mathbb{Z}$.

Next, we have that $bx + cy = rax + say \rightarrow bx + cy = (rx + sy)a$.

Because $rx + sy$ is an integer it follows that $a \mid bx + cy$. □

Theorem 1.4. *Let a and b be integers with $a \neq 0$ and $b \neq 0$. If $a \mid b$ and $b \mid c$, then $a \mid c$.*

Proof. We assume that for two integers a, b with $a \neq 0$ and $b \neq 0$, $a \mid b$ and $b \mid c$.

This means that $b = ra$ and $c = sb$ for some integers r, s.

Therefore $c = sra = (sr)a$ and because sr is an integer, it follows that $a \mid c$. □

Result 1.5. *For every nonnegative integer n,*

$$3 \mid (n^3 - n).$$

Proof. We proceed by induction.

For $n = 0$, we observe that $0^3 - 0 = 0$, thus $3 \mid 0$.

We assume that $3 \mid (k^3 - k)$ for $k \geq 0$.

We show that $3 \mid (k+1)^3 - (k+1)$.

$$\begin{aligned}(k+1)^3 - (k+1) &= k^3 + 3k^2 + 3k + 1 - k - 1 \\ &= k^3 + 3k^2 + 2k \\ &= (k^3 - k) + 3k^2 + 3k \\ &= (k^3 - k) + 3(k^2 + k).\end{aligned}$$

Because $3 \mid (k^3 - k)$, we have that $k^3 - k = 3s$ for $s \in \mathbb{Z}$.
Therefore

$$\begin{aligned}(k+1)^3 - (k+1) &= 3s + 3(k^2 + k) \\ &= 3(k^2 + k + s).\end{aligned}$$

Based on fundamental properties of integers it follows that $k^2 + k + s$ is an integer, thus $3 \mid (k+1)^3 - (k+1)$.

By the principle of mathematical induction it follows that $3 \mid (n^3 - n)$. $\square$

Result 1.6. *For every nonnegative integer n,*

$$4 \mid (5^n - 1).$$

Proof. We proceed by induction.

For $n = 0$, we observe that $5^0 - 1 = 1 - 1 = 0$ and $4 \mid 0$.

Next, we assume that $4 \mid (5^k - 1)$ for $k \in \mathbb{Z}$ with $k \geq 0$.

We show that $4 \mid (5^{k+1} - 1)$. We have that $5^{k+1} - 1 = 5^k 5 - 1$. Because $4 \mid (5^k - 1)$, it follows that $5^k - 1 = 4r$ for some $r \in \mathbb{Z}$. Thus $5^k = 4r + 1$. Then

$$\begin{aligned} 5^{k+1} - 1 = 5^k 5 - 1 &= (4r + 1)5 - 1 \\ &= 20r + 5 - 1 \\ &= 20r + 4 \\ &= 4(5r + 1). \end{aligned}$$

Since $5r + 1$ is an integer, it follows that $4 \mid (5^{k+1} - 1)$.

By the principle of mathematical induction it follows that $4 \mid (5^n - 1)$. □

Discrete Math I - MTSC 213
Lecture 30

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 8, 2013

1 Primes

Definition 1.1. A prime is an integer $p \geq 2$ whose only positive integer divisors are 1 and p.

Some prime numbers are:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

1.1 The Fundamental Theorem of Arithmetic

Theorem 1.2 (The Fundamental Theorem of Arithmetic)**.** *Every integer $n \geq 2$ is either prime or can be expressed as a product of (not necessarily distinct) primes, that is,*

$$n = p_1 p_2 ... p_k,$$

where $p_1, p_2, ..., p_k$ are primes. This fatorization is unique except possibly for the order in which the primes appear.

Example 1.1.

In some cases we can check if a prime p divides an integer n.

- 2 divides n only if n is even. The last digit of an even number must be even.

- $4 = 2^2$ divides n if the last two digits of n are divided by 4. For example, $4 \mid 6912$ because $4 \mid 12$.
- 3 divides an integer n if and only if 3 divides the sum of the digits of n. For example $3 \mid 324$ because $3 \mid (3 + 2 + 4)$.
- $9 = 3^2$ divides n if and only if 9 divides the sum of the digits of n.
- 5 divides n if the last digit of n is 5 or 0.
- There is a method for finding if an integer n can be divided by 11. Let a the sum of alternating digits of n, and b the sum of the remaining digits. Then $11 \mid n$ if and only if $11 \mid (a - b)$. For example, $11 \mid 9,775,887$ because $11 \mid ((9 + 7 + 8 + 7) - (7 + 5 + 8))$, $11 \mid (31 - 20)$.

Definition 1.3. An integer $n \geq 2$ that is not prime is called a composite number (or simply composite).

Theorem 1.4. *An integer $n \geq 2$ is composite if and only if there exist integers a and b with $1 < a < n$ and $1 < b < n$ such that $n = ab$.*

Corollary 1.5. *If n is a composite number, then n has a prime factor p such that $p \leq \sqrt{n}$.*

Proof. Let n be a composite number. Then according to theorem 1.4 $n = ab$ for some integers a, b with $1 < a < n$ and $1 < b < n$. Suppose that $a < b$. Then $a^2 < ab = n$, thus $a < \sqrt{n}$. Because $a \geq 2$ according to theorem 1.2 there is some prime number p such that $p \mid a$ and so $p \leq a < \sqrt{n}$. According to previously proved theorem $p \mid ab$, that is $p \mid n$. □

We can use this corollary to find out if an integer is a prime.

Example 1.2. Show that 103 is a prime.

Answer We check if there are any primes lower than $\sqrt{103}$ that divide 103. We observe that $10 < \sqrt{103} < 11$, so we check the primes 2, 3, 5, 7. We observe that none of them is a factor of 11, therefore 103 is a prime number.

1.2 There are Infinitely Many Primes

Theorem 1.6. *There are infinitely many primes.*

Proof. We will use proof by contradiction.

We assume that there is a finite number of primes, $p_1, p_2, ..., p_k$.

Let $n = p_1p_2...p_k + 1$. Because n is greater than each prime, n must be composite. By the fundamental theorem of arithmetic, at least one prime must divide n say $p_j \mid n$. Therefore $n = p_jr$ for some integer r. That means

$$\begin{aligned} p_1p_2...p_k + 1 &= p_jr \\ p_1p_2...p_{j-1}p_jp_{j+1}...p_k + 1 &= p_jr \\ 1 &= p_jr - p_1p_2...p_{j-1}p_jp_{j+1}...p_k + 1 \\ 1 &= p_j(r - p_1p_2...p_{j-1}p_{j+1}...p_k + 1) \end{aligned}$$

We observe that $r - p_1p_2...p_{j-1}p_{j+1}...p_k + 1$ is an integer, hence $p_j \mid 1$. This is a contradiction because a prime number is by definition greater than 2. □

Theorem 1.7 (The Prime Number Theorem)**.** *The number $\pi(n)$ is approximately equal to $n/\ln n$. More specifically*

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1.$$

1.3 Unsolved Problems Involving Primes

1. Two positive integers p and $p + 2$ are called twin primes if they are both primes, for example, 5 and 7 are twin primes. The **two primes conjecture** is that there are infinitely many twin primes.

2. **Goldbach's Conjecture:** Every even integer that is 4 or more can be expressed by the sum of two primes.

3. Observe that the following Fibonacci numbers are primes: 2, 3, 5, 13. Are there infinitely many prime Fibonacci numbers?

Discrete Math I - MTSC 213
Lecture 31

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 11, 2013

1 The Division Algorithm

Theorem 1.1 (The Division Algorithm)**.** *For every two integers m and $n > 0$, there exist unique integers q and r such that*

$$m = nq + r, \text{ where } 0 \leq r < n.$$

The integer q is called the quotient produced when dividing m by n, and r is called the remainder of the division with values $0, 1, ...n - 1$.

For example for $m = 22$ and $n = 5$, $22 = 4.5 + 2$, therefore $q = 4$ and $r = 2$.

Example 1.1. For the following pairs of integers m, n find the quotient and remainder, when m is divided by n. Then write $m = nq + r$.

a) $m = 59$, $n = 7$

b) $m = -58$, $n = 7$

Answer

a) $q = 8$, $r = 3$, $59 = 7.8 + 3$

b) $q = -9$, $r = 5$, $-58 = 7.(-9) + 5$.

We note here that when the remainder is 0, then $m = nq + 0$ can also be expressed as $n \mid m$. We have the following

$$\text{If } m = nq + r \text{ and } 1 \leq r \leq n - 1 \text{ then } n \nmid m.$$

We also observe that we can use the floor function to express the quotient q and remainder r:

If $m = nq + r$ with $0 \leq r \leq n - 1$, then

$$q = \lfloor \tfrac{m}{n} \rfloor \text{ and } r = m - n\lfloor \tfrac{m}{n} \rfloor$$

Example 1.2. For the following pairs of integers m, n, find $\lfloor \frac{m}{n} \rfloor$ and $m - n\lfloor \frac{m}{n} \rfloor$.

a) $m = 18$, $n = 7$

b) $m = -18$, $n = 7$.

Answer

a) $\lfloor \frac{m}{n} \rfloor = \lfloor 18/7 \rfloor = 2$, $m - n\lfloor \frac{m}{n} \rfloor = 18 - 7.2 = 4$

b) $\lfloor \frac{m}{n} \rfloor = \lfloor -18/7 \rfloor = -3$, $m - n\lfloor \frac{m}{n} \rfloor = -18 - 7.(-3) = 3$.

In the previous exercise we evaluated the quotient and remainder of divisions. In computer terminology the quotient may be symbolized by **div** and the remainder may be symbolized by **mod**.

That is, if $m = nq + r$, then m **div** $n = q$ and m **mod** $n = r$.

Example 1.3. Determine m **div** n and m **mod** n for the following pairs of integers m, n.

a) $m = 75$, $n = 12$

b) $m = -36$, $n = 5$

Answer

a) 75 **div** $12 = 6$, 75 **mod** $12 = 3$.

b) -36 **div** $5 = -8$, -36 **mod** $5 = 4$.

Theorem 1.2. *Let n be an integer. Then $3 \mid n^2$ if and only if $3 \mid n$.*

Proof. Because the statement is a biconditional we have to prove the following two statements

$$\text{a) if } 3 \mid n \text{ then } 3 \mid n^2 \text{ .}$$
$$\text{b) if } 3 \mid n^2 \text{ then } 3 \mid n.$$

To show a) we assume that $3 \mid n$, therefore $n = 3k$ for some integer k. It follows that $n^2 = (3k)^2 = 3(3k^2)$. Because $3k^2$ is an integer, it follows that $3 \mid n^2$.

For the second statement we will use proof by contrapositive to show that if $3 \nmid n$ then $3 \nmid n^2$.

Let $3 \nmid n$. Then $n = 3q + r$ for some integers q and r.

The remainder r can be 1 or 2.

Case 1: $r = 1$. Then $n = 3q + 1$ and

$$\begin{aligned} n^2 &= (3q+1)^2 \\ &= 9q^2 + 6q + 1 \\ &= 3(3q^2 + 2q) + 1. \end{aligned}$$

Because $3q^2 + 2q$ is an integer, $3 \nmid n^2$.

Case 1: $r = 2$. Then $n = 3q + 2$ and

$$\begin{aligned} n^2 &= (3q+2)^2 \\ &= 9q^2 + 12q + 4 \\ &= 3(3q^2 + 4q + 1) + 1. \end{aligned}$$

Since $3q^2 + 4q + 1$ is an integer, $3 \nmid n^2$. □

Discrete Math I - MTSC 213
Lecture 32

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 13, 2013

1 Congruence

In several occasions we are interested in the parity of integers. We noticed that two integers are both even if both have a remainder 0 when divided by 2. Also, two integers are odd if they both have a remainder 1 when divided by 2.

In this section we deal with numbers that have the same remainder when divided by an integer n with $n \geq 2$. We begin with a definition of congruence and reach this observation.

Definition 1.1. For integers a, b and $n \geq 2$, the integer a is congruent to b modulo n if $n \mid (a - b)$.

To show that a is congruent to b modulo n we use the notation $a \equiv b(\mod n)$. To show that a is not congruent to b modulo n we write $a \not\equiv b(\mod n)$.

Example 1.1. We observe that
$47 \equiv 5(\mod 7)$, because $7 \mid (47 - 5)$.
$93 \equiv 84(\mod 9)$, because $9 \mid (93 - 84)$.
$58 \not\equiv 47(\mod 6)$, because $6 \mid (58 - 47)$.

Theorem 1.2. *Let a, b and $n \geq 2$ be integers. Then $a \equiv b(\mod n)$ if and only if $a = b + kn$ for some integer k.*

Proof. This is a biconditional so we need to prove two statements.

We first show that if $a \equiv b(\mod n)$, then $a = b + kn$ for some integer k.
Let $a \equiv b(\mod n)$ for $a, b, n \in \mathbb{Z}$ with $n \geq 2$.
Then according to the definition $n \mid (a - b)$.
Hence, $a - b = nk$ for some integer k and $a = b + nk$.

Next, we show that if $a = b + kn$, then $a \equiv b(\mod n)$.
We assume that $a = b + kn$ for an integer k.
Then $a - b = kn$, therefore $n \mid (a - b)$.
By definition this means that $a \equiv b(\mod n)$. □

Theorem 1.3. *Let a, b and $n \geq 2$ be integers. Then $a \equiv b(\mod n)$ if and only if a and b have the same remainder when divided by n.*

Proof. This is a biconditional so we need to prove two statements.

First, we show that if a and b have the same remainder when divided by n, then $a \equiv b(\mod n)$.

Let a and b have the same remainder $r > 0, r \in \mathbb{Z}$ when divided by n.

Therefore, $a = nk_1 + r$ and $b = nk_2 + r$, for $k_1, k_2 \in \mathbb{Z}$.

We have that $a - b = nk_1 + r - (nk_2 + r) = nk_1 + r - nk_2 - r = nk_1 - nk_2 = n(k_1 - k_2)$.

Because $k_1 - k_2$ is an integer, $n \mid (a - b)$.

We also need to show that if $a \equiv b(\mod n)$, then a and b have the same remainder when divided by n.

We use proof by contrapositive.

We assume that a and b have different remainders when divided by n.

Hence, $a = k_1 n + r_1$ and $b = k_2 n + r_2$ with $r_1 \neq r_2$.

We will show that $a \not\equiv b(\mod n)$.

Then $a - b = k_1 n + r_1 - (k_2 n + r_2) = k_1 n + r_1 - k_2 n - r_2 = (k_1 - k_2)n + (r_1 - r_2)$.

Because $r_1 \neq r_2 \rightarrow r_1 - r_2 \neq 0$, therefore $n \nmid (a - b)$. This means that $a \not\equiv b(\mod n)$. □

Corollary 1.4. *Let a, b and $n \geq 2$ be integers. Then $a \equiv b(\mod n)$ if and only if*

$$a \mod n = b \mod n.$$

Example 1.2. Use Corollary 1.4 to determine whether the following pairs of integers a, b for integer $n \geq 2$ are $a \equiv b(\mod n)$.

(a) $a = 31$, $b = 47$, $n = 3$.

(b) $a = 35$, $b = 59$, $n = 6$.

Answer

(a) We observe that $31 \mod 3 = 1$ and $47 \mod 3 = 2$. Because $31 \mod 3 \neq 47 \mod 3$, it follows by Corollary 1.4 that $31 \not\equiv 47(\mod 3)$.

(b) We observe that $35 \mod 6 = 5$ and $59 \mod 6 = 5$. Because $35 \mod 6 = 59 \mod 6$, it follows by Corollary 1.4 that $35 \equiv 59(\mod 6)$.

Discrete Math I - MTSC 213
Lecture 33

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 15, 2013

1 Greatest Common Divisors

Definition 1.1. Let a, b, d be integers, where a and b are not both 0 and $d \neq 0$. The integer d is a common divisor of a and b if $d \mid a$ and $d \mid b$.

Definition 1.2. For integers a and b not both 0, the greatest common divisor of a and b is the greatest positive integer that is a common divisor of a and b. The number is denoted by $\gcd(a, b)$.

Example 1.1. Determine by observation the greatest common divisor of each of the following pairs a, b of integers.
(a) $a = 15$, $b = 25$, (b) $a = 16$, $b = 80$
(c) $a = -14$, $b = -18$, (d) $a = 0$, $b = 6$

Answer
(a) $\gcd(15, 25) = 5$, (b) $\gcd(16, 80) = 16$
(c) $\gcd(-14, -18) = 2$, (d) $\gcd(0, 6) = 6$

From the previous example we observe the following:
(1) $\gcd(a, b) = \gcd(|a|, |b|)$
(2) $\gcd(a, 0) = |a|$
(3) if $a, b \neq 0$ and $a \mid b$, then $\gcd(a, b) = a$.

1.1 The Euclidean Algorithm

Theorem 1.3. *Let a and b be two positive integers. If $b = aq + r$ for some integers q and r, then*

$$gcd(a, b) = gcd(r, a).$$

Let $a < b$ in the previous theorem. If we also assume that q is the quotient and r is the remainder, when b is divided by a, then

$$\gcd(a, b) = \gcd(r, a), \text{ with } 0 \leq r < b.$$

Now if $r = 0$ then $\gcd(a, b) = \gcd(0, a) = a$.

If $r \neq 0$, then we continue and divide a by r with remainder r_2, so $gcd(r, a) = gcd(r_2, r)$. We continue this until we reach a remainder equal to 0.

$\gcd(a, b) = \gcd(r, a) = gcd(r_2, r) = gcd(r_3, r_2) = ... = \gcd(0, r_k) = r_k$.

Therefore, the greatest common divisor of a and b is the last nonzero remainder obtained when the sequence of divisions described above is performed. This method for determining $\gcd(a, b)$ is called the Euclidean algorithm.

Example 1.2. Use the Euclidean algorithm to find $\gcd(384, 477)$.

Answer We recursively apply the Euclidean algorithm to the remainder of each division as follows.

$$\begin{aligned} 477 &\mod 384 = 93 \\ 384 &\mod 93 = 12 \\ 93 &\mod 12 = 9 \\ 12 &\mod 9 = 3 \\ 9 &\mod 3 = 0. \end{aligned}$$

Therefore $\gcd(384, 477) = 3$.

1.2 Least Common Multiples

Definition 1.4. For two positive integers a and b, an integer n is a common multiple of a and b if n is a multiple of a and b. The smallest positive integer that is a common multiple of a and b is the least common multiple of a and b. The number is denoted by $\text{lcm}(a, b)$.

Example 1.3. Determine by observation the least common multiple of a and b.

(a) $a = 6$ $b = 9$, (b) $a = 10$ $b = 10$,
(c) $a = 5$ $b = 7$, (d) $a = 15$ $b = 30$,

Answer

(a) $\text{lcm}(6, 9) = 18$, (b) $\text{lcm}(10, 10) = 10$
(c) $\text{lcm}(5, 7) = 35$, (d) $\text{lcm}(15, 30) = 30$

Theorem 1.5. *For every two positive integers a and b,*

$$ab = \gcd(a, b)lcm(a, b)$$

1.3 Relatively Prime Integers

Definition 1.6. Two integers a and b not both 0, are relatively prime if $\gcd(a, b) = 1$.

Result 1.7. *Every two consecutive positive integers are relatively prime.*

Proof. Let n and $n+1$ be consecutive positive integers and let $d = \gcd(n, n+1)$.

Hence $d \mid n$ and $d \mid n+1$. This means that $n = dr$ and $n+1 = ds$ for some integers d and s.

Based on these two relations, $dr + 1 = ds \rightarrow 1 = ds - dr \rightarrow 1 = d(s - r)$.

Because $s - r$ is an integer, $d \mid 1$, therefore $d \leq 1$. Also, $d \geq 1$, so $d = 1$. □

1.4 Linear Combinations of Integers

Definition 1.8. Let a and b be two integers. An integer of the form $ax+by$, where x and y are integers, is a linear combination of a and b.

Theorem 1.9. *Let a and b be integers that are not both 0. Then $gcd(a, b)$ is the smallest positive integer that is a linear combination of a and b.*

Example 1.4. For each of the following pairs of integers, express $d = \gcd(a, b)$ as a linear combination of a and b.
(a) $a = 10$ $b = 14$, (b) $a = 12$ $b = 12$
(c) $a = 18$ $b = 30$, (d) $a = 25$ $b = 27$

Answer
(a) $\gcd(10, 14) = 2 = 10 \cdot 3 + 14 \cdot (-2)$
(b) $\gcd(12, 12) = 12 = 12 \cdot 1 + 12 \cdot 0$
(c) $\gcd(18, 30) = 6 = 18 \cdot 2 + 30 \cdot (-1)$
(d) $\gcd(25, 27) = 1 = 25 \cdot 13 + 27 \cdot (-12)$

We can solve (d) using the Euclidean algorithm
$27 = 25 \cdot 1 + 2 \rightarrow 2 = 27 - 25 \cdot 1$
$25 = 12 \cdot 2 + 1 \rightarrow 1 = 25 - 12 \cdot 2$
Therefore

$$\begin{aligned} 1 &= 25 - 12 \cdot (27 - 25 \cdot 1) \\ &= 25 - 12 \cdot 27 + 12 \cdot 25 \\ &= 13 \cdot 25 - 12 \cdot 27 \end{aligned}$$

Corollary 1.10. *Let a and b be integers that are not both 0 and let $d = gcd(a, b)$. If n is an integer that is a common divisor of a and b then $n \mid d$.*

Proof. Based on theorem 1.9 $d = ax + by$ for some integers x, y.

Also $n \mid a$ and $n \mid b$, therefore $a = nq$ and $b = nr$ for some integers q and r.

So $d = ax + by = nqx + nry = n(qx + ry)$.

Because $qx + ry$ is an integer, $n \mid d$. □

Corollary 1.11. *Two integers a and b are relatively prime if and only if 1 is a linear combination of a and b; that is, $gcd(a, b) = 1$ if and only if $ax + by = 1$ for some integers x and y.*

Example 1.5. Use Corollary 1.11 to show that the following pairs are relatively prime.

(a) every two consecutive integers

(b) every two odd integers that differ by 2.

Answer

(a) Let $n \in \mathbb{Z}$ and the consecutive integer $n + 1$.

Because $(-1) \cdot n + n + 1 = 1$.

By the Corollary 1.11 it follows that $\gcd(n, n + 1) = 1$ and $m - n = 2$.

(b) Let an odd integer m such that $m = 2k + 1$ and an odd integer $n = m + 2 = 2k + 1 + 2 = 2k + 3$ with $k \in \mathbb{Z}$.

Since $1 = (2k + 1)(k + 1) + (2k + 3)(-k)$, by the Corollary 1.11 it follows that $\gcd(m, n) = 1$.

Theorem 1.12. *Let a, b and c be integers with $a \neq 0$. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. Let $a \mid bc$. Then $bc = qa$ for some integer q.

Because $\gcd(a, b) = 1$, by the Corollary 1.11 it follows that $ax + by = 1$ for some integers a and b.

Therefore $c = c \cdot 1 = c(ax + by) = cax + cby = cax + qay = a(cx + qy)$.

Because $cx + qy$ is an integer, it follows that $a \mid c$. □

Corollary 1.13. *Let b and c be integers and let p be a prime. If $p \mid bc$, then either $p \mid b$ or $p \mid c$.*

Theorem 1.14. *Let $a_1, a_2, ..., a_n$ be $n \geq 2$ integers and let p be a prime. If*

$$p \mid a_1 a_2 ... a_n,$$

then $p \mid a_i$ for some integer i with $1 \leq i \leq n$.

Theorem 1.15 (The Fundamental Theorem of Arithmetic)**.** *Every integer $n \geq 2$ is either prime or can be expressed as a product of (not necessarily distinct) primes, that is,*

$$n = p_1 p_2 ... p_k,$$

where $p_1, p_2, ..., p_k$ are primes. This factorization is unique except possibly for the order in which the primes appear.

Discrete Math I - MTSC 213
Lecture 34

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 19, 2013

1 Counting

One of the topics of discrete mathematics is called combinatorics. This is a branch of mathematics that deals with the study of configurations or arrangements of objects.

Some fundamental topics that combinatorics deal with are the following:

1. Existence: Is such a configuration or arrangement possible?
2. Enumeration: How many such configurations are there?
3. Optimization: Is some arrangement of a certain type more desirable in some way?

In this chapter we are concerned with the second topic. This area is called enumerative combinatorics, that is the subject of counting. Next, we will review some fundamental principles of counting.

1.1 The Multiplication and Addition Principles

1.1.1 The Multiplication Principle

Definition 1.1 (The Multiplication Principle)**.** A procedure consists of a sequence of two tasks. To perform this procedure, one performs the first task followed by performing the second task. If there are n_1 ways to perform the first task and n_2 ways to perform the second task after the first task has been performed, then there are $n_1 n_2$ ways to perform the procedure.

Example 1.1. At DSU a student is required to take a 2-course sequence during the senior year. The first course can be any of the three courses CS 410, CS 420, or CS 430.

To complete a sequence the student has two choices after taking any of the previous three courses; she can take CS 411 or CS 412 after CS 410, CS 421 or CS 422 after CS 420, or she can take CS 431 or CS 432 after CS 430.

How many choices does she have for a required 2-course sequence?

Answer

We observe that there are three possible courses for the first course in a 2-course sequence.

Once the first course has been taken, the student can select between two options for the second course to complete the sequence.

Therefore, by the Multiplication Principle it follows that the total number of possibilities for this 2-course sequence is $3 \cdot 2 = 6$.

The previous 2-course sequence can be represented by a specific type of diagram called a tree diagram depicted in Figure **??**. Each course sequence can be created by following the tree diagram from top to bottom.

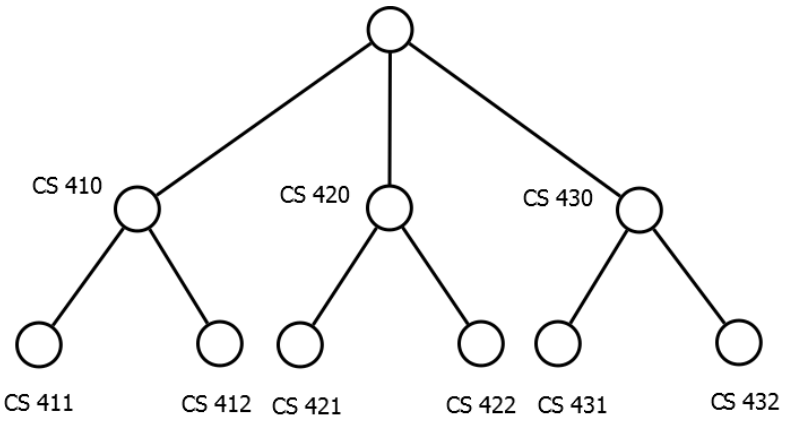


Figure 1: Tree diagram for course sequence.

The Multiplication Principle determines the number of ways of performing a procedure that consists of two tasks. We can generalize this principle for more than two tasks, for example if we have three tasks T_1, T_2, T_3 in one procedure. This can be done by grouping two tasks, let's say T_1 and T_2, in a procedure B, then create a procedure A that consists of the procedure B and task T_3. So the number of ways for performing B is $n_1 n_2$ and the number of ways for performing procedure A is $(n_1 n_2)n_3 = n_1 n_2 n_3$. This leads to the General Multiplication Principle.

Definition 1.2 (The (General) Multiplication Principle)**.** Performing a certain procedure consists of performing a sequence of $m \geq 2$ tasks $T_1, T_2, ..., T_m$. If there are n_i ways of performing T_i after any preceding tasks have been performed for $i = 1, 2, .., m$, then the total number of ways of performing the procedure is $n_1 n_2 ... n_m$.

Example 1.2. In a certain computer science course, there is a weekly quiz. The quiz for today consists of ten true-false questions. How many different sequences are possible for this quiz?

Answer

Each of the ten questions can be answered by true or false, that is two ways.

Therefore, the numer of different responses to the test is

$$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}.$$

This example can be interpreted as the number of 10-bit sequences, where zero corresponds to false and 1 corresponds to true.

Theorem 1.3. *If A and B are two finite nonempty sets with $|A| = m$ and $|B| = n$, then the number of different functions from A to B is $|B|^{|A|} = n^m$.*

Proof. Let $A = \{a_1, a_2, ..., a_m\}$. Then a function $f : A \to B$ has the form

$$f = \{(a_1, \_), (a_2, \_), ..., (a_m, \_)\}.$$

Each blank space is to be filled by an element of the co-domain B.

Because there are n choices for each image, the Multiplication Principle supports that the number of all choices is

$$n \cdot n ... \cdot n = n^m.$$

□

Theorem 1.4. *If A and B are two sets with $|A| = m$ and $|B| = n$, where $m \leq n$, then the number of different one-to-one functions from A to B is* $\frac{n!}{(n-m)!}$.

Proof. First, when $m = n$, we observe that an one-to-one function $f : A \to B$ can be written as

$$f = \{(a_1, \_), (a_2, \_), ..., (a_n, \_)\}.$$

We note that there are n possible images in the ordered pair $(a_1, \_)$.

Because f is one-to-one, the image of for a_1 will be excluded from the possible images of a_2, therefore there are $n - 1$ possible images for $(a_2, \_)$.

We continue this logic until we reach the last element of the domain, that has to have 1 image.

By the multiplication principle it follows that the number of possible images for the one-to-one function f is:

$$n \cdot (n-1) \cdot (n-2) \cdot ... \cdot 1 = n!.$$

Next we assume that $m < n$. Then each one-to-one function $f : A \to B$ can be written as

$$f = \{(a_1, \_), (a_2, \_), ..., (a_m, \_)\}.$$

Following similar logic, the number of possible one-to-one functions $f : A \to B$ is

$$n \cdot (n-1) \cdot (n-2) \cdot ... \cdot (n-m+1).$$

This is equivalent to

$$n \cdot (n-1) \cdot (n-2) \cdot ... \cdot (n-m+1) \cdot \frac{(n-m)!}{(n-m)!} = \frac{n!}{(n-m)!}.$$

□

Example 1.3. Determine the number of one-to-one functions from A to B, where $|A| = 6$ and $|B| = 8$.

Answer

The number of possible one-to-one functions from A to B according to the Theorem **??** is:

$\frac{8!}{(8-6)!} = \frac{8!}{2!} = \frac{8 \cdot 7 \cdot 6 ... \cdot 2 \cdot 1}{2 \cdot 1} = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = 20160.$

We now assume a procedure of m tasks T_i, $i \in [1, m]$, where A_i is the set of possible ways to perform T_i.

If $n_i = |A_i|$, then the number of ways for performing the procedure is $n_1 n_2 ... n_m$. Each way for performing the procedure can be represented by the Cartesian product $A_1 \times A_2 \times ... \times A_m$. Then we have

$$|A_1 \times A_2 \times ... \times A_m| = n_1 n_2 ... n_m.$$

This leads to

$$|A_1 \times A_2 \times ... \times A_m| = |A_1| \cdot |A_2| \cdot ... \cdot |A_m|.$$

Discrete Math I - MTSC 213
Lecture 35

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 20, 2013

1 The Addition Principle

Definition 1.1 (The Addition Principle)**.** A procedure consists of two tasks that cannot be performed simultaneously. To perform this procedure, either of the two tasks is performed. If the first task can performed in n_1 ways and the second can be performed in n_2 ways, then the number of ways of performing this procedure is $n_1 + n_2$.

The Addition Principle can be generalized for more tasks as follows.

Definition 1.2 (The (General) Addition Principle)**.** Performing a certain procedure consists of performing one of $m \geq 2$ tasks $T_1, T_2, ..., T_m$, no two of which can be performed at the same time. If the task T_i can be performed in n_i ways for $1 \leq i \leq m$, then the number of ways of performing this procedure is $n_1 + n_2 + ... + n_m$.

Example 1.1. After a student graduates from college, he wants to work on a Master's degree in computer science. He is considering two universities in Iowa, four universities in Pennsylvania and three universities in West Virginia. By the Addition Principle the number of choices he has for graduate studies are $2 + 4 + 3 = 9$.

Let a procedure consist of $m \geq 2$ tasks $T_1, T_2, ..., T_m$. Let A_i be the set of ways for performing task T_i with $|A_i| = n_i$. Given that A_i are pairwise disjoint sets, the procedure can be performed in $n_1 + n_2 + .. + n_m$ ways. Then $A_1 \cup A_2 \cup ... \cup A_m$ is the set of all ways of performing the procedure and the corresponding number of ways is

$$|A_1 \cup A_2 \cup ... \cup A_m| = n_1 + n_2 + .. + n_m.$$

Therefore if $A_1, A_2, ..., A_m$ are pairwise disjoint sets with $m \geq 2$, then

$$|A_1 \cup A_2 \cup ... \cup A_m| = |A_1| + |A_2| + ... + |A_m|.$$

Example 1.2. A recent graduate has obtained a position with an electronics company and has to spend the first four months in training either in the Eastern US or the Western US. In the Western US she can spend the first two months in Portland or Los Angeles and the second two months in Sacramento, Seattle or San Francisco. In the Western US, she can spend the first 2 months in Miami, Boston, or Dover and the second two months in Wilkes-Barre, Niskayuna, Baltimore, or Virginia Beach. How many choices does the new employee have for training?

Answer

First, by the Multiplication Principle, the employee has $2 \cdot 3 = 6$ options in the Western US and $3 \cdot 4 = 12$ options in the Eastern US. It follows by the Addition Principle that the total number of options is $6 + 12 = 18$.

Example 1.3. How many 9-bit sequences begin with

$$10101\_\_\_\_ \text{ or } 0101\_\_\_\_\_?$$

Answer

By the Multiplication Principle it follows that the number of 9-bit sequences starting with 10101 is $2 \cdot 2 \cdot 2 \cdot 2 = 2^4 = 16$.

Similarly, we observe that the number of 9-bit sequences starting with 0101 is $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5$.

By the Addition Principle it follows that the total requested number of 9-bit sequences is $16 + 32 = 48$.

Example 1.4. In a school election, three students are to be elected to the student council. One student must be freshman, one sophomore and one junior.

(a) Given that there are 6 freshman, 4 sophomore and 7 junior candidates in how many different ways can a ballot be marked?

(b) After the election the president of the student council will select one of the remaining candidates as an at-large member. How may options are there?

Answer

(a) First, by the Multiplication Principle it follows that the ballot can be marked in $6 \cdot 4 \cdot 7 = 168$ different ways.

(b) The Addition Principle dictates that the total number of options for the at-large member are $5 + 3 + 6 = 14$.

Discrete Math I - MTSC 213
Lecture 36

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 22, 2013

1 The Principle of Inclusion-Exclusion

We have seen that if A and b are two disjoint finite sets, then $|A \cup B| = |A| + |B|$.

Another question is what is $|A \cup B|$ equal to, when A and B are not disjoint? For example, what is the cardinality of the set of the 50 largest cities or the state capitals of the US?

Such questions can be resolved by the Principle of Inclusion-Exclusion.

Definition 1.1 (The Principle of Inclusion-Exclusion)**.** A procedure consists of two tasks. To perform the procedure, one performs either of the two tasks. If the first task can be performed in n_1 ways, the second task can be performed in n_2 ways and the two tasks can be performed simultaneously in n_{12} ways, then the total number of ways of performing the procedure is

$$n_1 + n_2 - n_{12}.$$

The Principle of Inclusion-Exclusion can also be expressed in terms of finite sets as follows

Definition 1.2 (The Principle of Inclusion-Exclusion (for two sets))**.** For every two sets A and B

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

In particular, if A and B are disjoint

$$|A \cup B| = |A| + |B|.$$

The last case corresponds to the Addition Principle.

Example 1.1. How many 8-bit sequences begin with 110 and end with 1100?

Answer

We are considering 8-bit sequences of one of the types

$$110\_\_\_\_\_ \text{ or } \_\_\_\_1100.$$

By the Multiplication Principle it follows that the number of bitstrings beginning with $110\_\_\_\_\_$ is $2^5 = 32$.

Similarly, the number of bitstrings ending with $\_\_\_\_1100$ is $2^4 = 16$.

We also observe that there are bit-strings beginning with $110\_\_\_\_\_$ and ending with $\_\_\_\_1100$. These are of the form 110_1100 and their number is 2^1.

Therefore by the Inclusion-Exclusion Principle it follows that our requested number is $32 + 16 - 2 = 46$.

Now let's examine the case of three sets. The Addition Principle states that $|A \cup B \cup C| = |A| + |B| + |C|$.

What happens though when the sets A, B and C are not pairwise disjoint?

Example 1.2. In a discrete mathematics course there are 26 students majoring in CS, 22 majoring in Math and 8 majoring in both CS and Math. How many students major in CS or Math?

Answer

We have that $|C| = 26$, $|M| = 22$ and $|C \cap M| = 8$. We are looking for $|C \cup M|$.

By the Principle of Inclusion-Exclusion it follows that

$$|C \cup M| = |C| + |M| - |C \cap M| = 26 + 22 - 8 = 40.$$

There are 40 students majoring in CS or Math.

Definition 1.3 (The Principle of Inclusion-Exclusion (for three sets))**.** For every three finite sets A, B and C,
$|A \cup B \cup C| = |A| + |B| + |C|$ - $|A \cap B|$ - $|A \cap C|$ - $|B \cap C|$ + $|A \cap B \cap C|$.

Example 1.3. In a convention venue 60 attendees were questioned about their lunch preferences and their responses were listed as follows

25 like beef
26 like tofu
24 like chicken
15 like beef and tofu
12 like beef and chicken
5 like tofu and chicken.
4 like all three.
The question is, how many do not like any of the above food types?

Answer

We have the following cardinalities in set notation: $|B| = 25$, $|T| = 26$, $|C| = 24$, $|B \cap T| = 15$, $|B \cap C| = 12$, and $|T \cap C| = 15$.

By the Principle of Inclusion-Exclusion we have that

$$|B \cup T \cup C| = |B| + |T| + |C| - |B \cap T| - |B \cap C| - |T \cap C| + |B \cap T \cap C|$$
$$|B \cup T \cup C| = 25 + 26 + 24 - 15 - 12 - 5 + 4 = 47.$$

Therefore 47 conference attendees like beef, tofu, or chicken, and $60-47 = 13$ do not like any of the above food types.

The above reasoning can be extended to an arbitrary number of sets as follows

Definition 1.4 (The Principle of Inclusion-Exclusion (for $n \geq 2$ sets))**.** If $A_1, A_2, ..., A_n$ are $n \geq 2$ finite sets, then

$$|A_1 \cup A_2 \cup ... \cup A_n| = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - ...$$
$$+(-1)^{n+1} |A_1 \cap A_2 \cap ... \cap A_n.$$

Discrete Math I - MTSC 213
Lecture 37

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

November 25, 2013

1 The Pigeonhole Principle

We begin with an observation: when an athlete has won four medals in a tournament, we expect that at least two of these medals must be gold, silver, or bronze.

Let's consider the following:

Example 1.1. A student has been collecting stamps from three countries, let's say Germany, France and Jamaica. If she has n stamps in total, then at least $\lceil n/3 \rceil$ come from Germany, or at least $\lceil n/3 \rceil$ come from France, or at least $\lceil n/3 \rceil$ come from Jamaica.

Definition 1.1 (The Pigeonhole Principle)**.** If a set S with n elements is divided into k pairwise disjoint subsets $S_1, S_2, ..., S_k$, then at least one of the subsets must have at least $\lceil n/k \rceil$ elements.

Proof. Assume that none of the subsets has at least $\lceil n/k \rceil$ elements.

Because $\lceil n/k \rceil$ is an integer, every subset S_i has at most $\lceil n/k \rceil - 1$ elements.

We observe that that $0 \leq \lceil n/k \rceil - (n/k) < 1$, therefore $n/k \leq \lceil n/k \rceil < (n/k) + 1$, and $\lceil n/k \rceil - 1 < n/k$.

Because S_i with $i = 1, 2, ..., k$ are pairwise disjoint subsets of S and $S = S_1 \cup S_2 \cup ... \cup S_k$, by the Addition Principle it follows that $n = |S| = |S_1| + |S_2| + ... + |S_k| < k(n/k) = n$.

Therefore $n < n$, which is a contradiction. □

Example 1.2. A teacher of a Discrete Mathematics course has 28 students.

(a) The teacher must assign each student one of the grades A, B, C, D, F. What is the largest number of students that must be assigned the same grade?

(b) It is known that the ages of the students in class range from 16 to 43. What is the maximum number of students in the class who must be the same age?

(c) In order to qualify for this discrete math class, each student must have passed one of three prerequisite courses. What is the maximum number of students in the class who must have passed the same prerequisite course?

Answer

(a) The number of students that must be assigned the same grade is $\lceil 28/5 \rceil = 6$.

(b) There are 28 years in the range 16 to 43.

The maximum number of students who must be the same age are $\lceil 28/28 \rceil = 1$.

(c) The maximum number of students who must have passed the same prerequisite course is $\lceil 28/3 \rceil = 10$.

Definition 1.2 (The (General) Pigeonhole Principle)**.** A set S with n elements is divided into k pairwise disjoint subsets $S_1, S_2, ..., S_k$, where $|S_i| \geq n_i$ for a postive integer n_i with $i = 1, 2, ..., k$. Then each subset of S with at least

$$1 + \sum_{i=1}^{k}(n_i - 1)$$

elements contains at least n_i elements of S_i for some integer i with $1 \leq i \leq k$.

Proof. Suppose that there is some subset A of S such that

$$|A| \geq 1 + \sum_{i=1}^{k}(n_i - 1)$$

but A does not contain at least n_i elements of S_i for some integer i with $1 \leq i \leq k$.

Then A must contain at most $n_i - 1$ elements of S_i for every integer i with $1 \leq i \leq k$.

Then $|A| \leq \sum_{i=1}^{k}(n_i - 1) \leq |A| - 1$, which is a contradiction. □

Example 1.3. At a certain university, discrete mathematics is often taught at a large lecture class. Let's suppose that, on the average, 10% of the students receive A's, 25% receive B's, 40% receive C's, 20% receive D's, and 5% receive F's.

How many students would have to be in the classe so that the professor assigns either 10 A's, 25 B's, 40 C's, 20 D's, or 5 F's?

Answer

We apply the General Pigeonhole Principle.

We have that the least number of students that have to be in the class is

$$\begin{aligned} N &= 1 + 9 + 24 + 39 + 19 + 4 \\ &= 96. \end{aligned}$$

Example 1.4. How many people need to be present at a party to be sure that at least 3 of them have a birthday during June, at least 3 of them have a birthday during July, at least 3 of them have a birthday during August, or at least 4 of them have a birthday during the same month for one of the other months?

Answer

By the General Pigeonhole Principle it follows that the smallest number of people that need to be at the party is

$$1 + 2 + 2 + 2 + 9 \cdot 3 = 7 + 27 = 34.$$

Discrete Math I - MTSC 213
Lecture 38

Sokratis Makrogiannis, PhD, Assistant Professor
Department of Mathematical Sciences, Delaware State University

December 1, 2013

1 Permutations and Combinations

1.1 Permutations

Definition 1.1 (Permutation)**.** A permutation of a nonempty set S is an arrangement or ordered list of the elements of S.

Example 1.1. Consider the set $S = \{1, 2, 3\}$. One permutation of S is $3, 1, 2$ or 312.

All of the permutations of the set S are:

123 213 312
132 231 321

We can also use a tree diagram to represent all permutations. We observe that this procedure is analogous to finding the number of one-to-one functions from A to B, where $|A| = |B| = 3$.

For the general case of a positive integer n, the number of permutations of the integers $1, 2, ..., n$ (or of any n objects) is given by

$$n(n-1)(n-2)...3 \cdot 2 \cdot 1 = n! \text{ (n factorial)}$$

Definition 1.2 (r-Permutation)**.** An ordered list of r elements of an n-element set S is called an r-permutation of the elements of S. The number of r-permutations of an n-element set is denoted by $P(n, r)$.

Theorem 1.3. *The number of r-permutations of an n-element set (where $1 \leq r \leq n$) is*

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+2)(n-r+1) = \frac{n!}{(n-r)!}).$$

Example 1.2. Let $S = \{a, b, c, d, e, f, g\}$.

(a) Give two examples of permutations of S.

(b) How many permutations of S are there?

(c) Give two examples of 4-permutations of S.

(d) How many 4-permutations of S are there?

Answer

(a) Two permutations are $abcdegf$ and $bacdefg$.

(b) There are $7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ permutations in total.

(c) Two 4-permutations of S are $abcd$ and $dcba$.

(d) There are $\frac{7!}{3!} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3!}{3!} = 7{\cdot}6{\cdot}5{\cdot}4 = 210{\cdot}4 = 820$ 4-permutations in total.

Example 1.3. Seven students namely 4 men and 3 women, are to present their solutions to seven different problems in class.

(a) In how many different orderings can this be done?

(b) In how many orderings can these presentations be made if the presentations are to alternate between men and women?

(c) In how many orderings can these presentations be made if the women are to present their problems consecutively and the men are to present their problems consecutively?

Answer

(a) The presentations can be done in the following number of ways: $P(7,7) = 7! = 5040$.

(b) We would have this type of ordering

$$MWMWMWM$$

So by the Multiplication Principle the number of possible orderings is

$$4 \cdot 3 \cdot 3 \cdot 2 \cdot 2 \cdot 1 \cdot 1 = 144.$$

(c) Then we would have $4! = 24$ possible orderings of presentations for men and $3! = 6$ possible orderings of presentations for women.

If women present first, by the Multiplication Principle we have $3! \cdot 4! = 6 \cdot 24 = 144$ possible orderings.

If men present first, by the Multiplication Principle we have $4! \cdot 3! = 24 \cdot 6 = 144$ possible orderings.

By the Addition Principle it follows that the total number of orderings is $(3! \cdot 4!) + (4! \cdot 3!) = 144 + 144 = 288$.

1.2 Combinations

Definition 1.4 (r-Combination)**.** Let S be an n-element set. An r-element subset of S, where $0 \leq r \leq n$, is called an r-combination of S. Therefore, the number of r-combinations of an n-element set is $C(n, r)$. An r-combination is also referred to as an unordered list of r-elements or as an r-selection.

Let $S = \{a_1, a_2, ..., a_n\}$ be an n-element set and T be one of the $C(n, r)$ element subsets with $1 \leq r \leq n$.

The number of ways to order the elements of T is $r!$.

The number of possible orderings of all r-element subsets of S is $r! \cdot C(n, r)$.

The last quantity is equal to $P(n, r)$.

Therefore $C(n, r) = \dfrac{P(n, r)}{r!}$.

Because $P(n, r) = \dfrac{n!}{(n-r)!}$, it follows that $C(n, r) = \dfrac{n!}{r!(n-r)!}$.

Theorem 1.5. *For integers r and n with $0 \leq r \leq n$, the number of r-element subsets of an element set (also called r-combinations or r-selections of an n-element set) is*

$$C(n, r) = \binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Example 1.4. A certain committee is required to meet 3 days during each February excluding weekends. If the coming February does not occur during the leap year, how many different choices are there for meeting days?

Answer

Because the coming February has exactly 4 weeks, there are $4 \cdot 5$ weekdays available for meetings.

So the 3-combinations within 20 days are:

$$\frac{20!}{3!17!} = \frac{20 \cdot 19 \cdot 18 \cdot 17!}{3!17!} = \frac{20 \cdot 19 \cdot 18}{3 \cdot 2 \cdot 1} = 20 \cdot 19 \cdot 3 = 1140.$$

Therefore, there are 1140 possible orderings for meetings in February.

Theorem 1.6. *For each integer $n \geq 0$,*

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$$

Theorem 1.7. *For every two integers r and n with $0 \leq r \leq n$,*

$$C(n,r) = C(n,n-r) \text{ or } \binom{n}{r} = \binom{n}{n-r}.$$

Proof #1. Observe that $C(n,r)$ is the number of r-element subsets of an n-element set S. However for each choice of an r-element subset belonging to S, there is an $n-r$ subset that does not belong to S, therefore $C(n,r) = C(n,n-r)$.

□

Proof #2. Observe that

$$C(n,r) = \frac{n!}{r!(n-r)!}$$

and

$$C(n,n-r) = \frac{n!}{(n-r)!(n-(n-r))!} = \frac{n!}{(n-r)!r!} = \text{C(n,r)}.$$

□

Example 1.5. How many subsets of $S = \{1,2,...,8\}$ contain three or more elements?

Answer

The requested number is :

$$\binom{8}{3} + \binom{8}{4} + \binom{8}{5} + \binom{8}{6} + \binom{8}{7} + \binom{8}{8} = 56+70+56+28+8+1 = 219.$$

Another way is to utilize Theorem 1.6 to find the total number of subsets and subtract the number of subsets with up to 2 elements. That is,

$$2^8 - \binom{8}{0} - \binom{8}{1} - \binom{8}{2} = 256 - 1 - 8 - 28 = 256 - 37 = 219.$$

Let's consider the usual case of $C(n,2) = \binom{n}{2}$.

This is equal to

$$C(n,2) = \binom{n}{2} = \frac{n!}{2!(n-2)!} = \frac{n \cdot (n-1) \cdot (n-2)!}{2(n-2)!} = \frac{n \cdot (n-1)}{2}. \qquad (1)$$

Example 1.6. By Equation 1 it follows that

$$C(5,2) = (5 \cdot 4)/2 = 10.$$

Also by Theorem 1.7 and Equation 1, we have that

$$C(9,7) = C(9,2) = (9 \cdot 8)/2 = 36.$$
$$C(20,18) = C(20,2) = (20 \cdot 19)/2 = 190.$$