TopicsCovered-2014

MACM 101

List of sections covered

- Chapter 1 (Fundamental Principles of Counting)
  - The rules of sum and product (1.1)
  - Permutations (1.2)
  - Combinations and binomial theorem (1.3)
  - Combinations with repetitions (1.4)
- Chapter 2 (Fundamental of Logic)
  - Basic connectives and truth table (2.1)
  - Logical equivalence (2.2)
  - Logical implication: rule of inference (2.3)
  - The use of quantifiers (2.4)
  - The proofs of theorems (2.5)

Sections covered

- Chapter 3 (Set Theory)
  - Sets and subsets (3.1)
  - Set operations and the laws of set theory (3.2)
  - Counting and Venn diagram (3.3)
  - A first word on probability (3.4)
  - The axioms of probability (3.5)

  Sections skipped: 3.6, 3.7
- Chapter 4 (Properties of integers)
  - Mathematical induction (4.1)
  - Recursive definitions (4.2)
  - The division algorithm (4.3)
  - The greatest common divisor (4.4)
  - The fundamental theorem of arithmetic (4.5)

Sections covered

- Chapter 5 (Relations and functions)
  - Cartesian products and relations (5.1)
  - Functions plain and One-to-one (5.2)
  - Onto functions: Stirling number of second kind (5.3)
  - Special functions (5.4)
  - Pigeonhole principle (5.5)
  - Function composition and inverse functions (5.6)

Sections skipped: 5.7, 5.8

Sections covered

- Chapter 7 (Relations: The Second Time Around)
  - Properties of relations (7.1)
  - Zero-one matrices and directed graphs (7.2)
  - Partial orders (7.3)
  - Equivalence relations (7.4)

Section skipped: 7.5

Acknowledgement

- I have used materials from the following sources:
  - Textbook
  - Lecture notes slides prepared by Prof. Bulatov.

    www.cs.sfu.ca/CC/101/101.MACM/abulatov/#lec
  - Lecture notes slides prepared by Prof. Grunschlag

    www.cs.columbia.edu/~zeph/3203s04/lectures.html
  - "Book of Proof" by Richard Hammock
    - http://www.people.vcu.edu/~rhammack/BookOfProof/

Counting

Sections 1.1, 1.2, 1.3, 1.4

Permutations and combinations

- Combinatorics, the study of arrangements of objects, is an important part of discrete mathematics.
- Combinatorics are used in
  - Discrete probability: What is the probability to guess a 6-symbols password in the first attempt?
  - Analysis of algorithms: Why a comparison-based sorting algorithm cannot be more efficient than cnlogn for any constant c.

The Rule of Sum

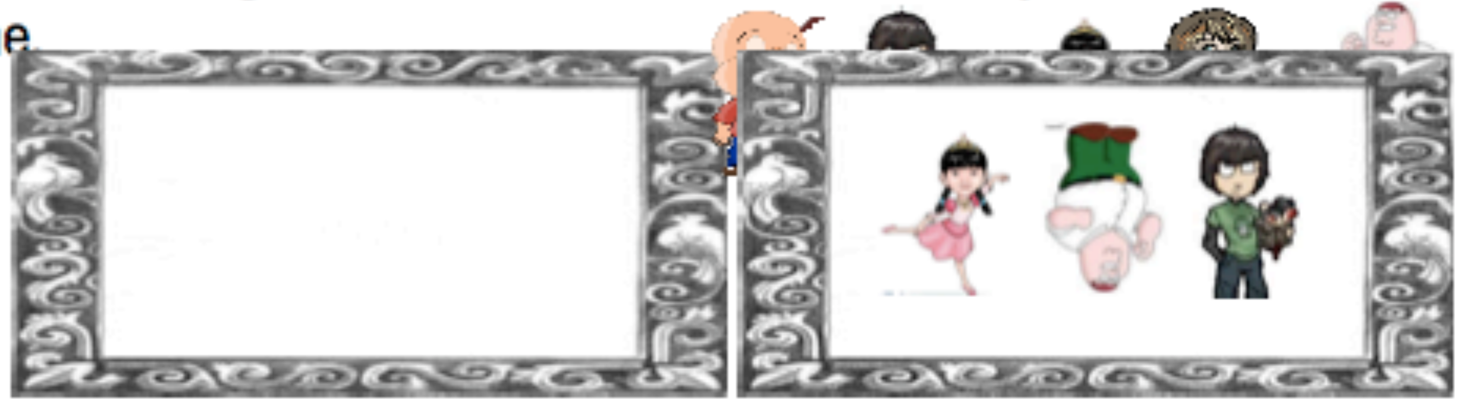
- If the first task can be performed in m ways, while a second task can be performed in n ways, and the two tasks cannot be performed simultaneously, performing either task can be accomplished in any one of m + n ways.
- Example: A deck of cards.
  - How many ways can I draw a heart? (13 ways)
  - How many ways can I draw a heart and a spade? (13 + 13 = 26 ways)
  - .... a heart or a king of spade? (13 hearts and 1 king → 14 ways.)
  - .... a king? (4 ways)
  - .... a heart or a king? (13 hearts (includes 1 king) + 3 other kings)

The Rule of Product

- If a procedure can be broken down into n stages and second stages, and if there are m possible outcomes for the first stage and if, for each of these outcomes, there are n possible outcomes, the total procedure can be carried out, in the designated order, in m.n ways.
- Example: A new company with two employees rents a floor of a building with 12 offices. How many ways are there to assign different offices to these two employees?
  - The office to the first employee can be done in 12 ways.
  - After the first assignment, the office to the second employee can be assigned in 11 ways. By the product rule, there are 12.11 = 132 ways to assign 12 offices to two employees.

Permutations

- Example: In how many ways can we select 3 students from a group of 5 student to stand in a line for a picture?
- Solution: First, note that the order in which we select students matters. There are 5 ways to select the first student. Once the first one is selected we are left with 4 ways to select the second student. After selecting the first 2 students there are 3 ways to select the third one.

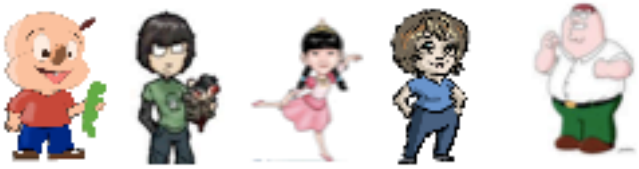


By the rule of product, there are $5 \cdot 4 \cdot 3 = 60$ ways to select students.

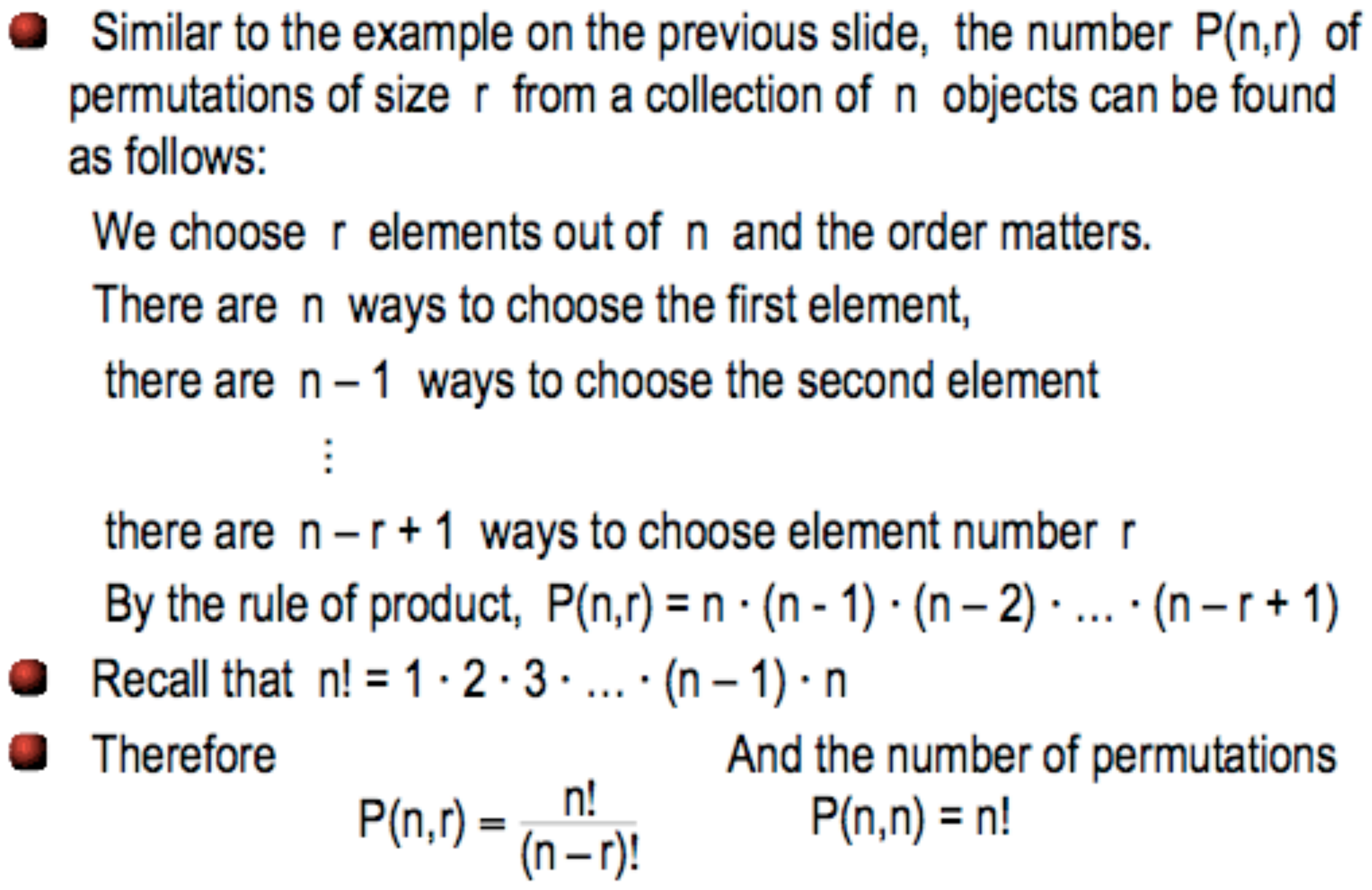
Permutations

- Given a collection of n distinct objects, any (linear) arrangement of these objects is called a permutation of the collection.

- A permutation of size r $(0 \leq r \leq n)$ is any (linear) arrangement of r distinct objects from the collection



The Number of Permutations



- Similar to the example on the previous slide, the number P(n,r) of permutations of size r from a collection of n objects can be found as follows:

  We choose r elements out of n and the order matters.

  There are n ways to choose the first element,

  there are $n - 1$ ways to choose the second element

  $\vdots$

  there are $n - r + 1$ ways to choose element number r

  By the rule of product, $P(n,r) = n \cdot (n - 1) \cdot (n - 2) \cdot \ldots \cdot (n - r + 1)$

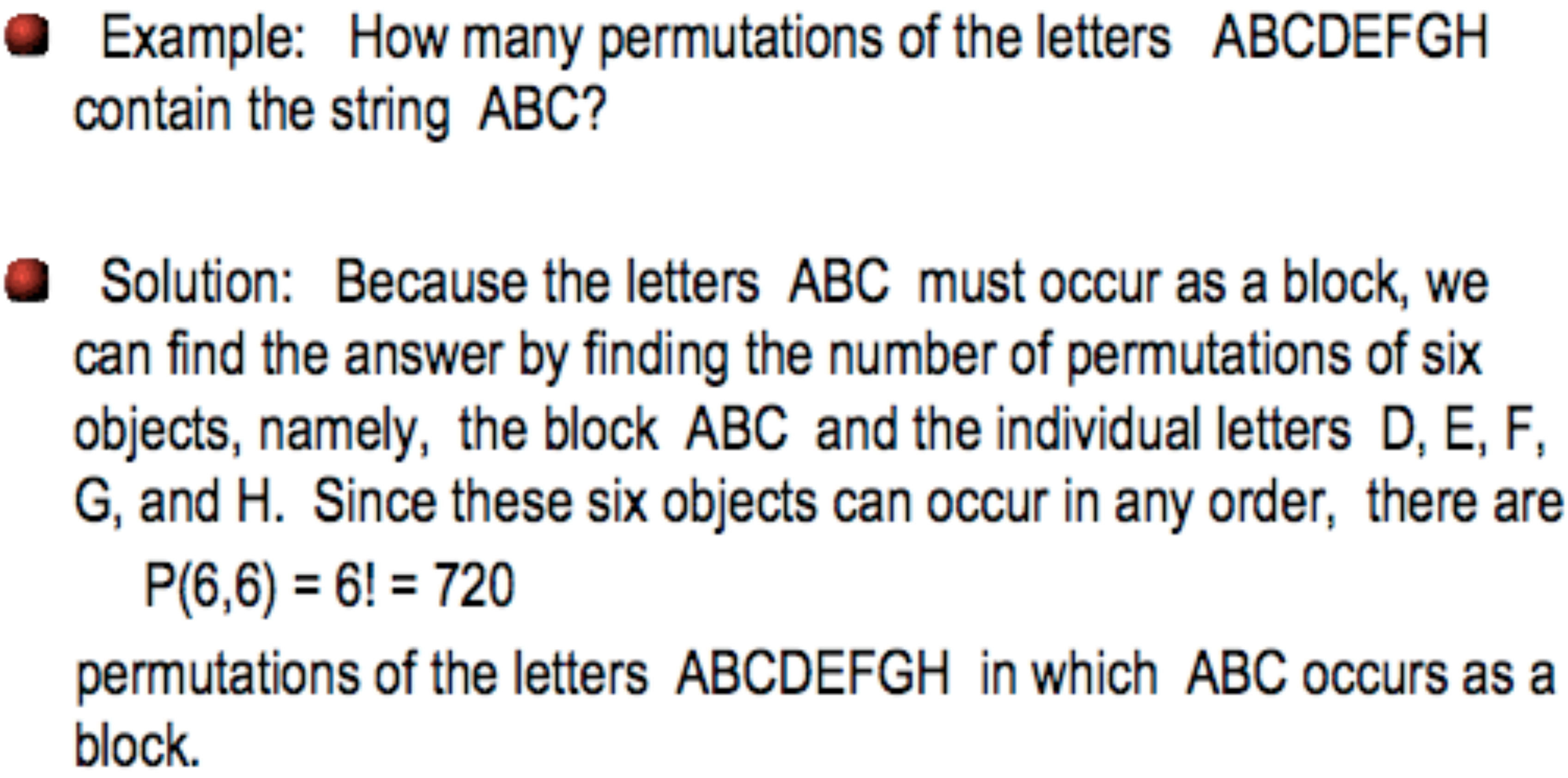
- Recall that $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n - 1) \cdot n$
- Therefore

  $$P(n,r) = \frac{n!}{(n-r)!}$$

  And the number of permutations

  $$P(n,n) = n!$$

Example



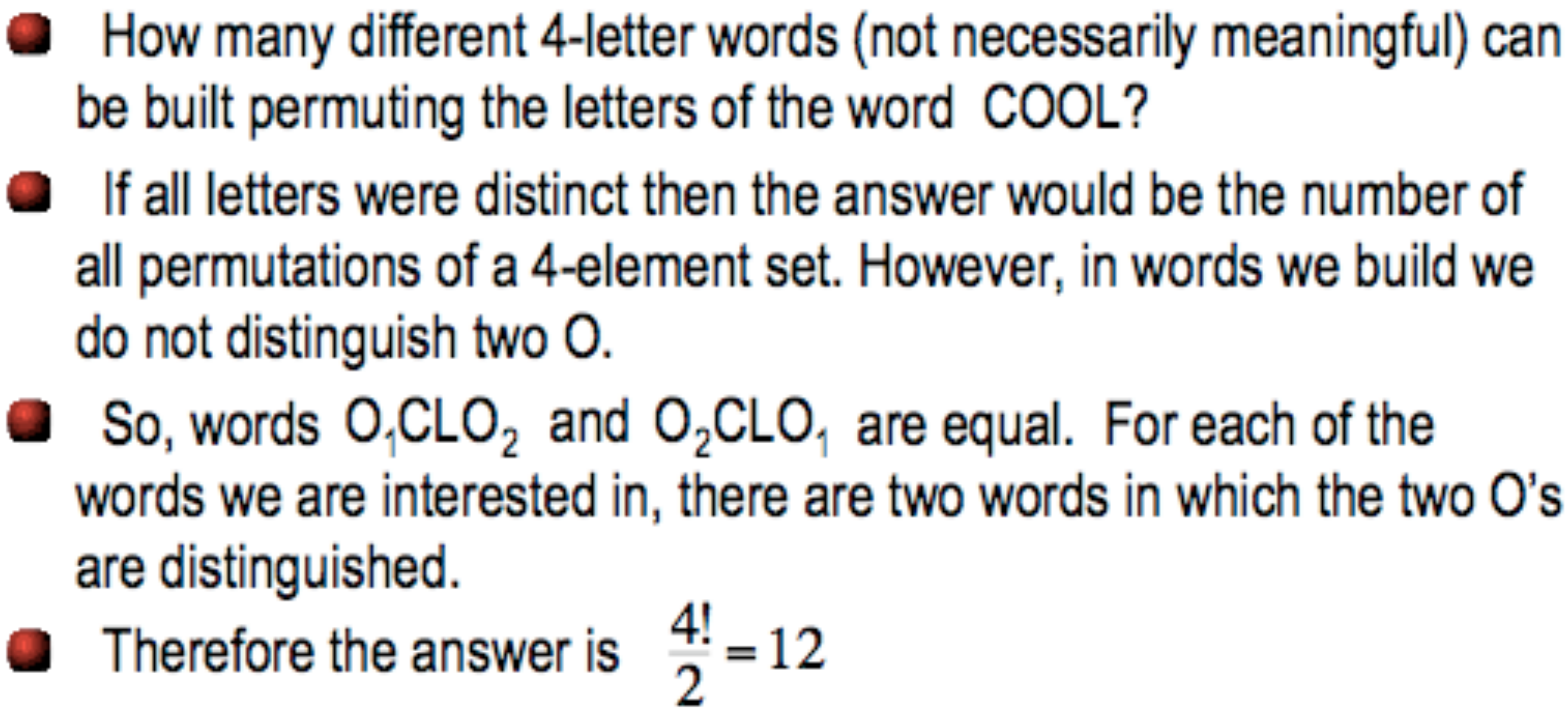
- Example: How many permutations of the letters ABCDEFGH contain the string ABC?

- Solution: Because the letters ABC must occur as a block, we can find the answer by finding the number of permutations of six objects, namely, the block ABC and the individual letters D, E, F, G, and H. Since these six objects can occur in any order, there are

  P(6,6) = 6! = 720

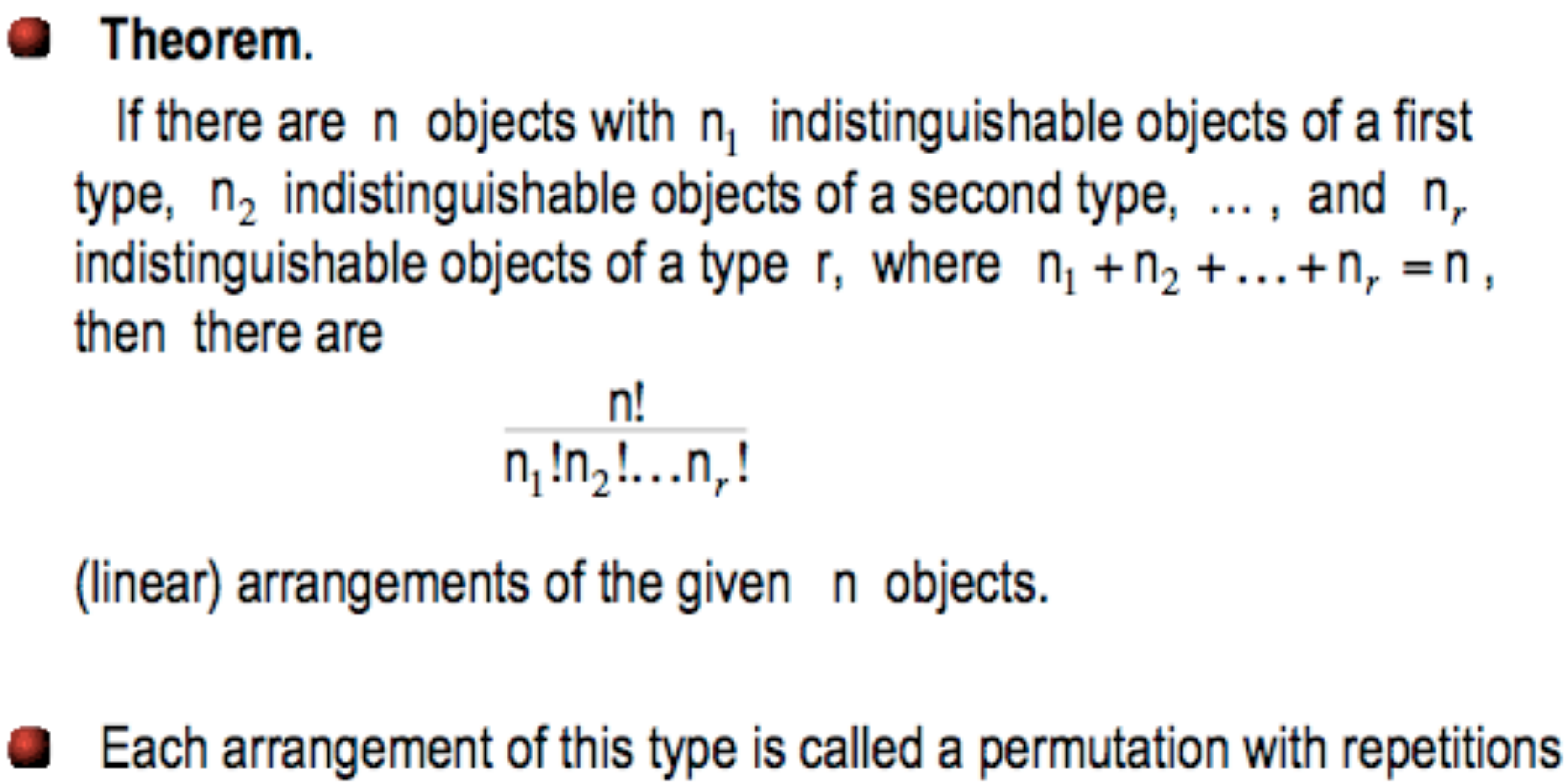
  permutations of the letters ABCDEFGH in which ABC occurs as a block.

Permutations with Repetitions



- How many different 4-letter words (not necessarily meaningful) can be built permuting the letters of the word COOL?
- If all letters were distinct then the answer would be the number of all permutations of a 4-element set. However, in words we build we do not distinguish two O.
- So, words O_1CLO_2 and O_2CLO_1 are equal. For each of the words we are interested in, there are two words in which the two O's are distinguished.
- Therefore the answer is $\frac{4!}{2} = 12$

Permutations with Repetitions



- **Theorem.**

  If there are n objects with n_1 indistinguishable objects of a first type, n_2 indistinguishable objects of a second type, … , and n_r indistinguishable objects of a type r, where $n_1 + n_2 + \ldots + n_r = n$, then there are

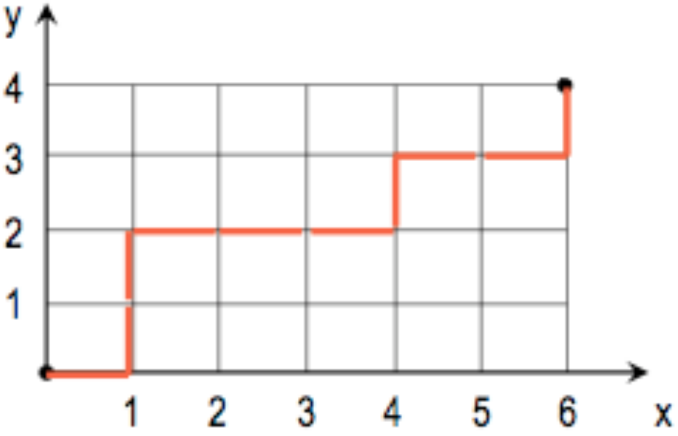
  $$\frac{n!}{n_1!n_2!\ldots n_r!}$$

  (linear) arrangements of the given n objects.

- Each arrangement of this type is called a permutation with repetitions

Example

- Determine the number of (staircase) paths in the xy-plane from (0,0) to (6,4), where each such path is made up of individual steps going one unit to the right (R) or one unit upward (U).



- Every path like this can be encoded as a sequence of R's and U's
- For example, the path on the picture is encoded as RUURRRURRU

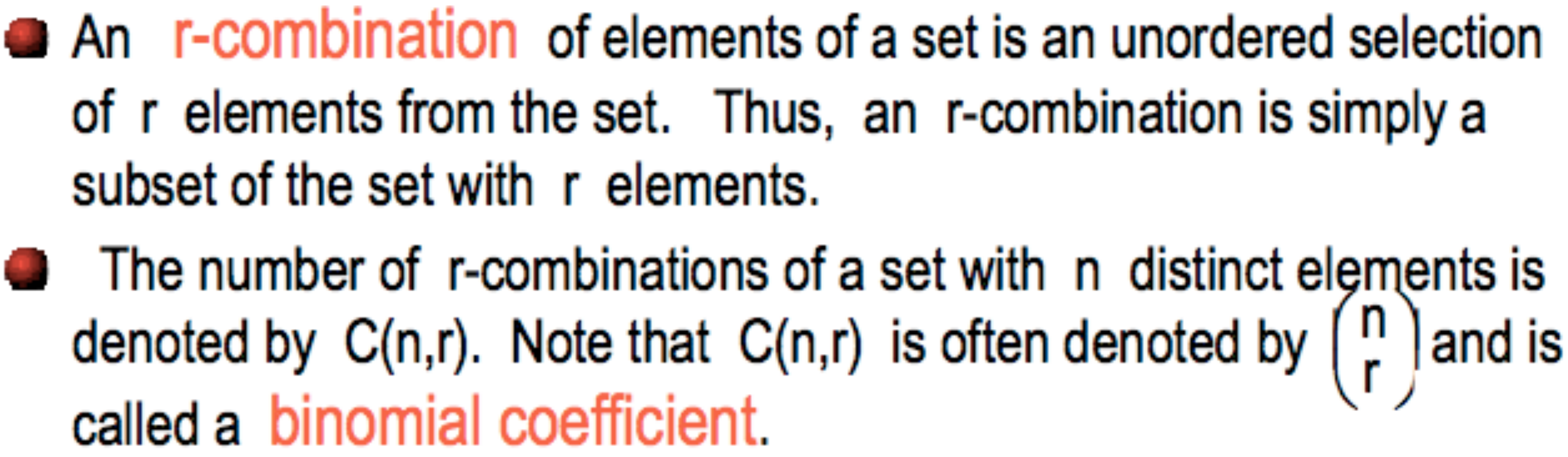
- Therefore, the number of paths equals to the number of permutations with repetitions: 6 R's and 4 U's:

$$\frac{10!}{6!4!} = 210$$

Combinations

- How many committees of three students can be formed from a group of four students?
- Solution: To answer this question, we need only to find the number of subsets with three elements from the set containing four elements. As is easily seen, there are four such subsets. Note that order in which these students are chosen does not matter.

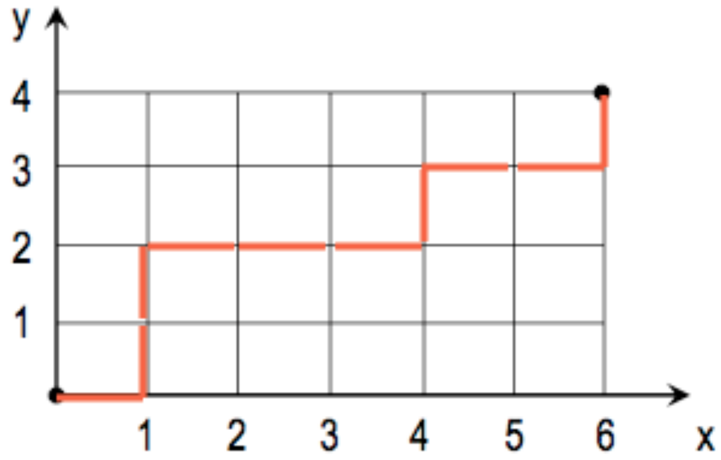
Combinations



- An r-combination of elements of a set is an unordered selection of r elements from the set. Thus, an r-combination is simply a subset of the set with r elements.
- The number of r-combinations of a set with n distinct elements is denoted by C(n,r). Note that C(n,r) is often denoted by $\binom{n}{r}$ and is called a binomial coefficient.

Example

- Reconsider the example with paths in the plain



- To get from (0,0) to (6,4) we need to make 10 steps. Among them 4 steps are upward and the rest to the right.
- Therefore every path corresponds to a selection from steps 1,2,…,10 four steps upward.
- Thus, the number of steps equals $C(10,4) = \frac{10!}{4!(10-4)!} = \frac{10!}{4!6!} = 210$

Combinations with Repetitions

- How many ways are there to select four pieces of fruit from a bowl containing apples, oranges, and pears if the order in which the pieces are selected does not matter, only the type of fruit and not the individual piece matter, and there are at least four pieces of each type of fruit in the bowl?
- Solution (brute force): List all possibilities

4 apples

3 apples, 1 orange

3 oranges, 1 pear

2 apples, 2 oranges

2 apples, 1 orange, 1 pear

4 oranges

3 apples, 1 pear

3 pears, 1 apple

2 apples, 2 pears

2 oranges, 1 apple,1 pear

4 pears

3 oranges, 1 apple

3 pears, 1 orange

2 oranges, 2 pears

2 pears, 1 apple,
1 orange

Combinations with Repetitions

- A better way:

$$\overbrace{\underbrace{*}_{\text{apples}} \mid \underbrace{*\quad *}_{\text{oranges}} \mid \underbrace{*}_{\text{pear}}}^{\text{four pieces of fruit}}$$

- Every choice of fruits corresponds to an arrangement of 4 stars and 2 bars.

  We have six positions to place a symbol, and two of them must be bars. Therefore the number we are looking for is

$$C(6,2) = \frac{6!}{2!(6-2)!} = \frac{6 \cdot 5}{1 \cdot 2} = 15$$

Combinations with Repetitions

- Theorem: There are C(n+r-1,n-1) r-combinations from a set with n elements when repetitions of elements are allowed.
- This is equivalent to placing r balls (indistinguishable) into n bins.

Example

- How many solutions does the equation

$$x + y + z = 11$$

have, where x, y, and z are nonnegative integers?

(In other words, in how many ways can we represent 11 as the sum of 3 nonnegative summands?)

- Solution:

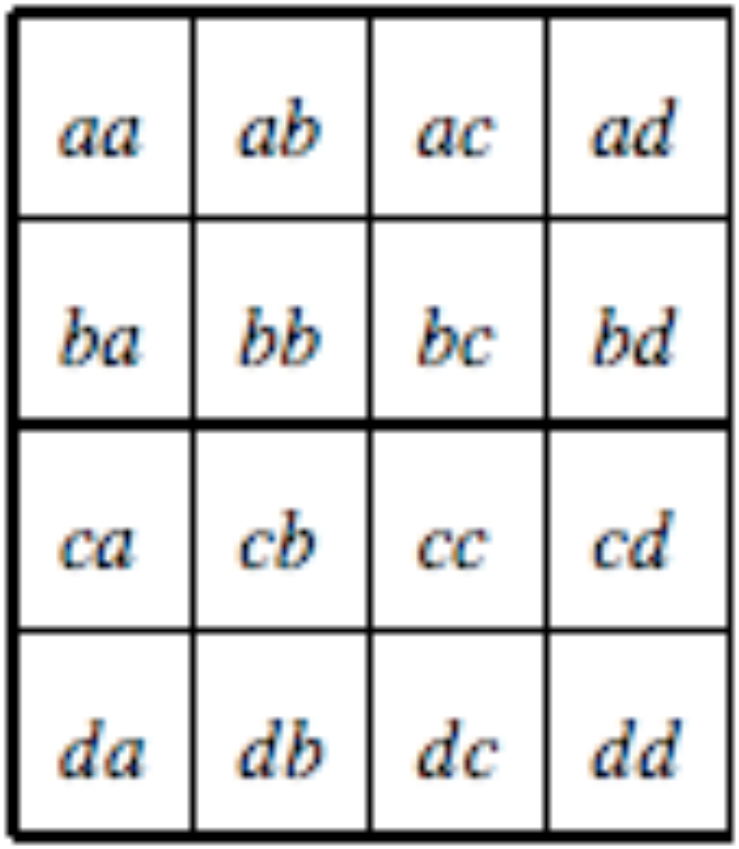
A solution corresponds to a way of selecting 11 items from a set with three elements so that x items of type one, y items of type two, and z items of type three are chosen.

Hence, the number of solutions is equal to the number of 11-combinations with repetitions from a set with 3 elements

$$C(3+11-1,3-1) = C(13,2) = \frac{13!}{2!(13-2)!} = \frac{13\cdot 12}{1\cdot 2} = 78$$

Example: Consider the set {a, b, c, d}. Suppose we select two letters from these four. Depending on our interpretation, we may obtain the following answers.

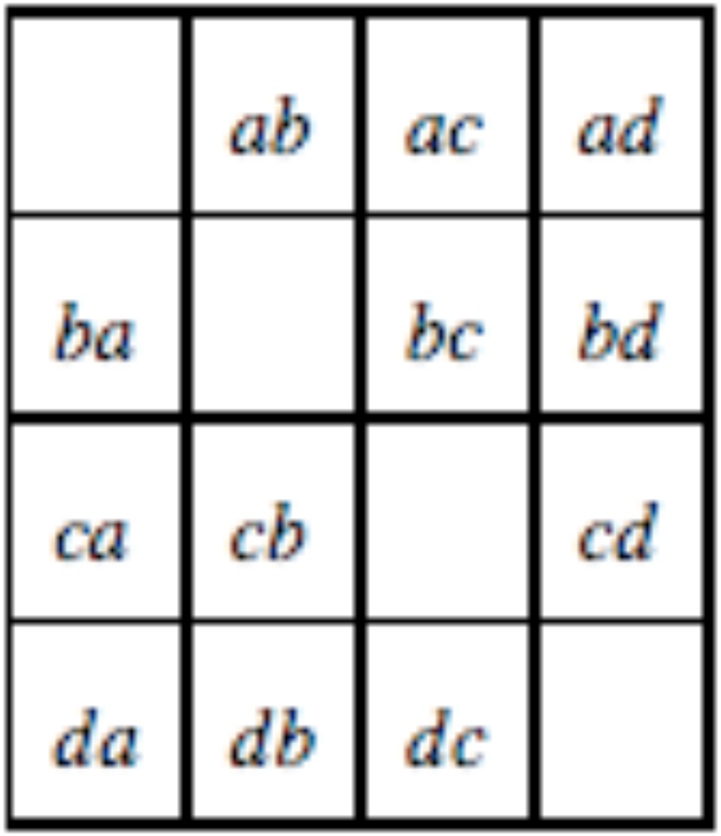
- Permutations with repetitions. The order is important, repetitions allowed. In this case there are 4 x 4 = 16 possible selections.



aa	*ab*	*ac*	*ad*
ba	*bb*	*bc*	*bd*
ca	*cb*	*cc*	*cd*
da	*db*	*dc*	*dd*

Example: Consider the set {a, b, c, d}. Suppose we select two letters from these four. Depending on our interpretation, we may obtain the following answers.

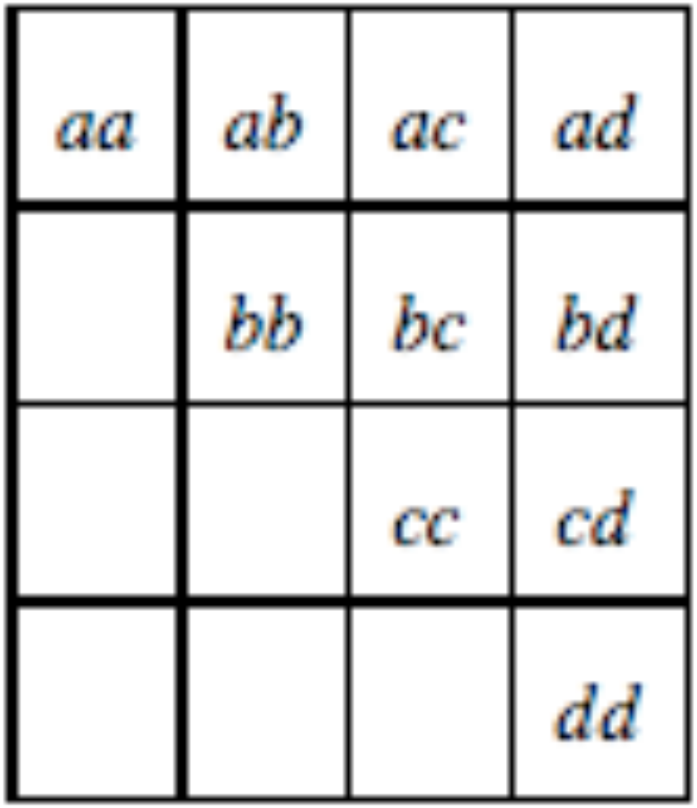
- Permutations without repetitions. The order is important, repetitions are not allowed. In this case there are 4 x 3 = 12 possible selections.



	ab	*ac*	*ad*
ba		*bc*	*bd*
ca	*cb*		*cd*
da	*db*	*dc*	

Example: Consider the set {a, b, c, d}. Suppose we select two letters from these four. Depending on our interpretation, we may obtain the following answers.

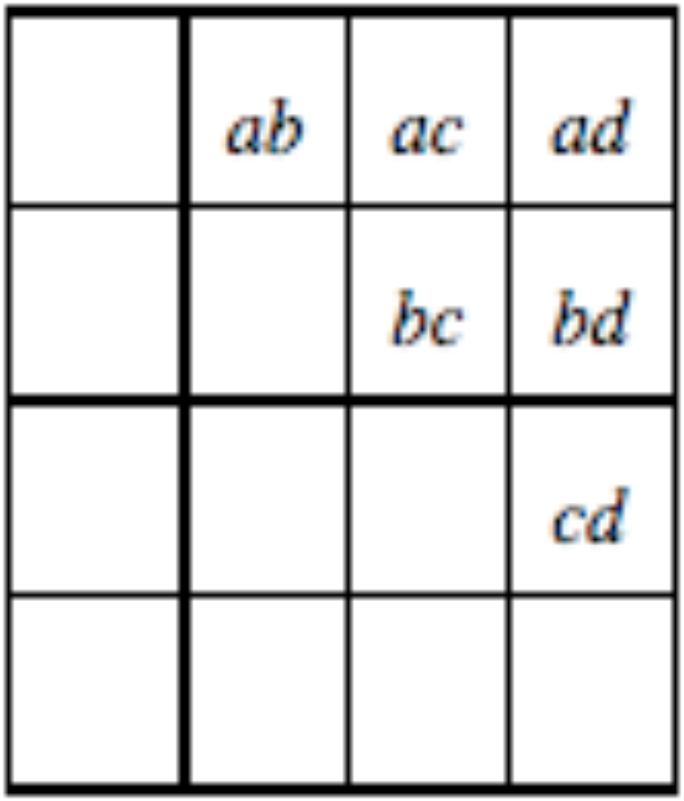
- Combinations with repetitions. The order is not important, repetitions are allowed. In this case there are 4 x 3/2 + 4 = 10 possible selections.



aa	*ab*	*ac*	*ad*
	bb	*bc*	*bd*
		cc	*cd*
			dd

Example: Consider the set {a, b, c, d}. Suppose we select two letters from these four. Depending on our interpretation, we may obtain the following answers.

- Combinations without repetitions. The order is not important, repetitions are not allowed. In this case there are 4 x 3/2 = 6 possible selections.



	ab	*ac*	*ad*
		bc	*bd*
			cd

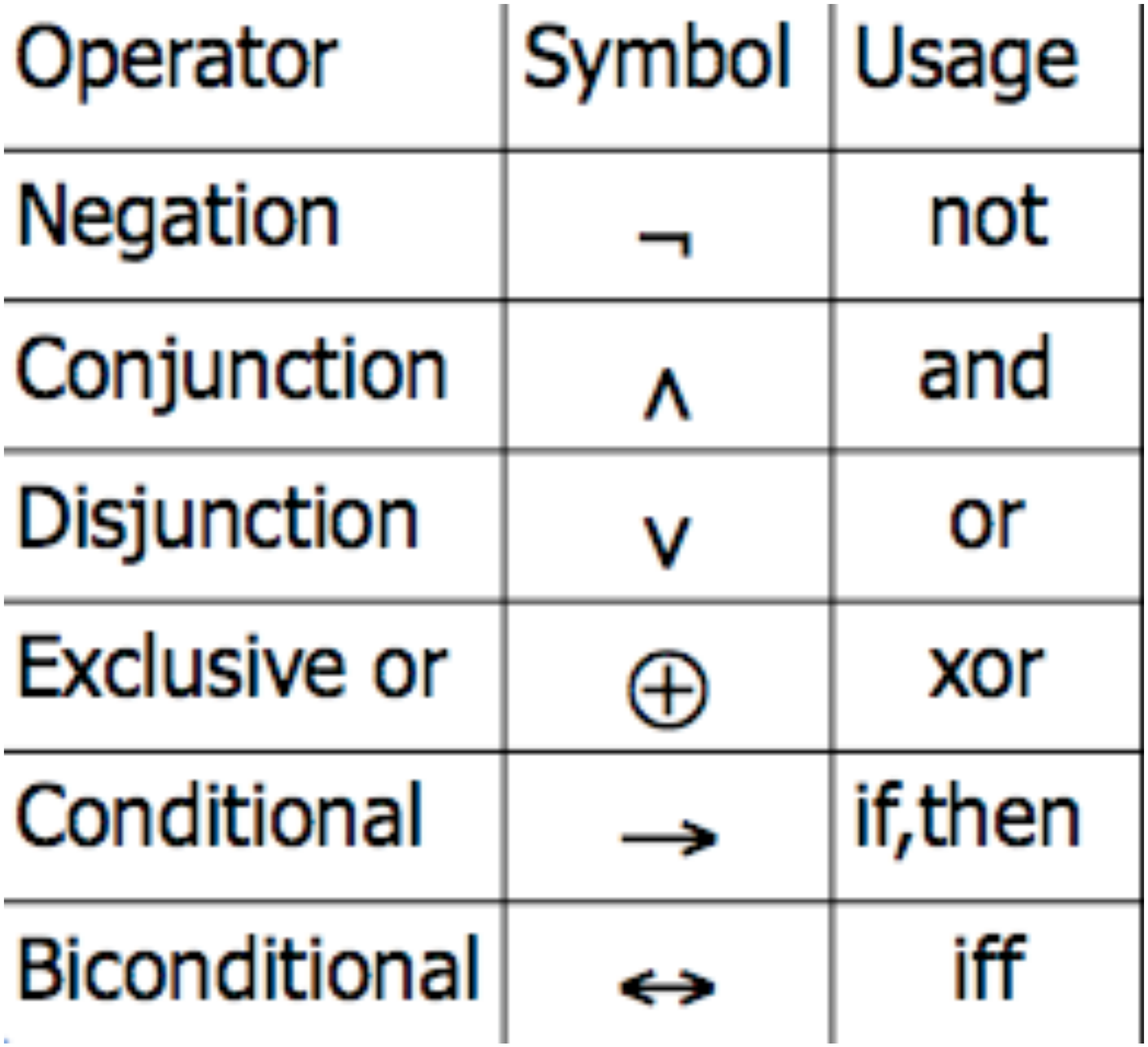
Fundamentals of Logic

Sections 2.1, 2.2, 2.3, 2.4

Logic

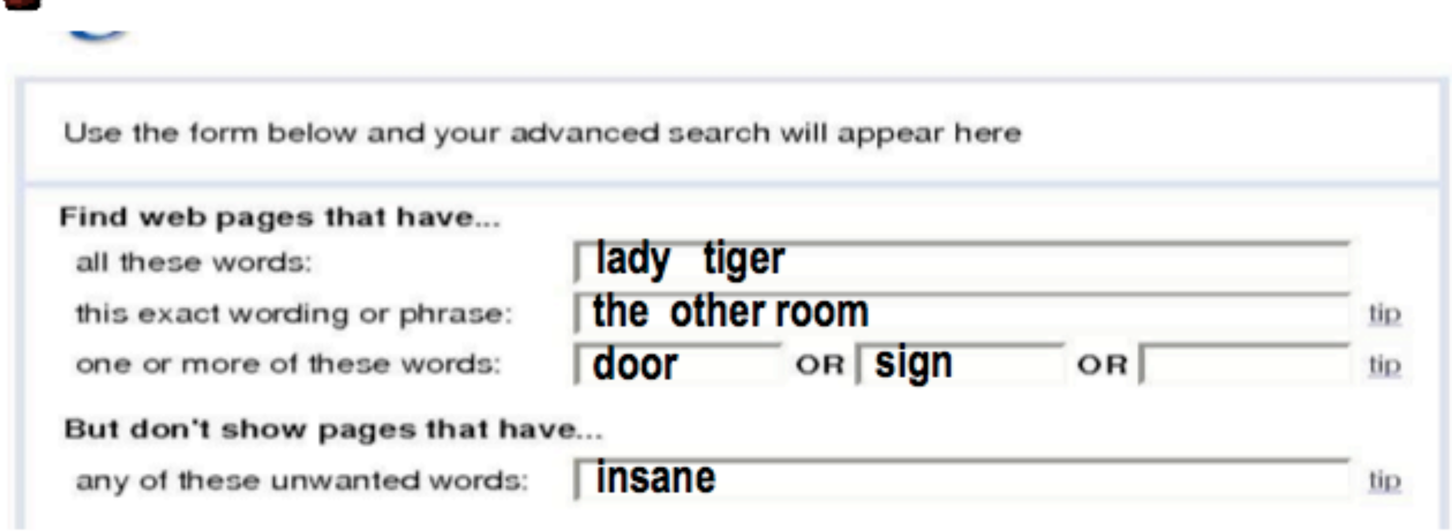
A proposition is a statement that is either true or false. Atomic propositions p,q,r… are combined to form compound propositions using the following logical connectives :

Logical Connectives



Operator	Symbol	Usage
Negation	$\neg$	not
Conjunction	$\wedge$	and
Disjunction	$\vee$	or
Exclusive or	$\oplus$	xor
Conditional	$\rightarrow$	if,then
Biconditional	$\leftrightarrow$	iff

Web Search

- 

Use the form below and your advanced search will appear here

Find web pages that have...

all these words: lady tiger

this exact wording or phrase: the other room tip

one or more of these words: door OR sign OR tip

But don't show pages that have...

any of these unwanted words: insane tip

- $(\text{lady} \wedge \text{tiger}) \wedge (\text{the other room}) \wedge (\text{door} \vee \text{sign}) \wedge \neg\, \text{insane}$

Truth Tables

Logical operators/connectives are defined by truth tables:

- Negation truth table (unary):

p	$\neg p$
F	T
T	F

- Binary truth tables:

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	T	T	F	T	T
T	F	F	T	T	F	F
F	T	F	T	T	T	F
F	F	F	F	F	T	T

Logically Equivalent

- Two statements s and s’ are logically equivalent, s $\Leftrightarrow$ s’, when s is true if and only if s’ is true and s is false if and only if s’ is false.
- The truth value columns of s and s’ are the same.

Contrapositive vs. Converse

Given an implication $p \rightarrow q$

- the converse is $q \rightarrow p$
- the contrapositive is $\neg q \rightarrow \neg p$

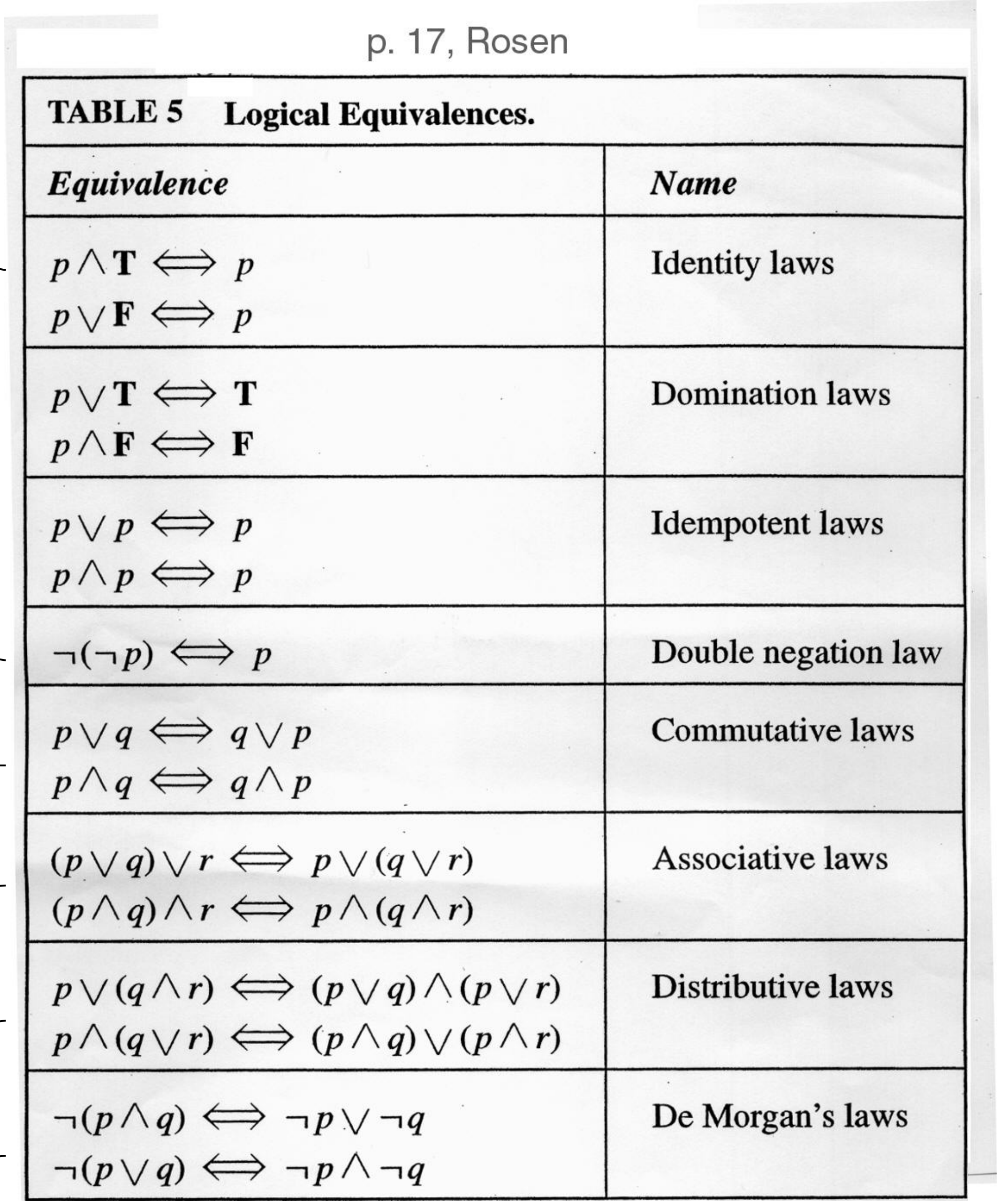
Logical Proofs

There are two basic techniques for proving tautologies and logical equivalences:

- Build a truth table. Verify that…
  - last column is all TRUE for tautology
  - relevant columns equal for equivalence
- Using tables on next, derive…
  - TRUE starting from supposed tautology
  - 1st proposition from 2nd

Tables of Logical Equivalences

- Identity laws
  - Like adding 0
- Domination laws
  - Like multiplying by 0
- Idempotent laws
  - Delete redundancies
- Double negation
  - “I don’t like you, not”
- Commutativity
  - Like “*x*+*y* = *y*+*x*”
- Associativity
  - Like “(*x*+*y*)+*z* = *y*+(*x*+*z*)”
- Distributivity
  - Like “(*x*+*y*)*z* = *xz*+*yz*”
- De Morgan



p. 17, Rosen

TABLE 5 Logical Equivalences.

Equivalence	*Name*
$p \wedge \mathbf{T} \Longleftrightarrow p$ $p \vee \mathbf{F} \Longleftrightarrow p$	Identity laws
$p \vee \mathbf{T} \Longleftrightarrow \mathbf{T}$ $p \wedge \mathbf{F} \Longleftrightarrow \mathbf{F}$	Domination laws
$p \vee p \Longleftrightarrow p$ $p \wedge p \Longleftrightarrow p$	Idempotent laws
$\neg(\neg p) \Longleftrightarrow p$	Double negation law
$p \vee q \Longleftrightarrow q \vee p$ $p \wedge q \Longleftrightarrow q \wedge p$	Commutative laws
$(p \vee q) \vee r \Longleftrightarrow p \vee (q \vee r)$ $(p \wedge q) \wedge r \Longleftrightarrow p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \Longleftrightarrow (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \Longleftrightarrow (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \Longleftrightarrow \neg p \vee \neg q$ $\neg(p \vee q) \Longleftrightarrow \neg p \wedge \neg q$	De Morgan’s laws

Quantifiers

- Existential Quantifier

  "∃" reads "there exists"

- Universal Quantifier

  "∀" reads "for all"

- Order matters:

$\exists y\ \forall x\ R(x,y)$ and $\forall x\ \exists y\ R(x,y)$ may not be logically equivalent.

DeMorgan Identities

- "Not all true iff one is false."
  - Conjunctional version:

$$\neg(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Leftrightarrow (\neg p_1 \vee \neg p_2 \vee \ldots \vee \neg p_n)$$

  - Universal quantifier version:

$$\neg\ \forall x\, \mathrm{P}(x) \Leftrightarrow \exists x\ \ \neg \mathrm{P}(x)$$

- "Not one is true iff all are false."
  - Disjunctional version:

$$\neg(p_1 \vee p_2 \vee \ldots \vee p_n) \Leftrightarrow (\neg p_1 \wedge \neg p_2 \wedge \ldots \wedge \neg p_n)$$

  - Existential quantifier version:

$$\neg\ \exists x\, \mathrm{P}(x) \Leftrightarrow \forall x\ \ \neg \mathrm{P}(x)$$

Translating English statements into symbolic form

Every integer that is not odd is even.

$\forall n \in \mathbb{Z}, \sim (n \text{ is odd }) \Rightarrow (n \text{ is even}),$ or $\forall n \in \mathbb{Z}, \sim O(n) \Rightarrow E(n).$

There is an integer that is not even.

$\exists n \in \mathbb{Z}, \sim E(n).$

For every real number x, there is a real number y for which $y^3 = x$.

$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x.$

Given any two rational numbers a and b, it follows that ab is rational.

$\forall a, b \in \mathbb{Q}, ab \in \mathbb{Q}.$

Goldbach's conjecture

- Conjecture: Every integer greater than 2 is the sum of two primes.
  - This can be translated in the following way, where P is the set of prime numbers and S={ 4,6,8,10, ….} is the set of even integers greater than 2. Both the translations are equivalent.

$$(n \in S) \Rightarrow (\exists\, p, q \in P, n = p + q)$$

$$\forall\, n \in S, \exists\, p, q \in P, n = p + q$$

Proofs

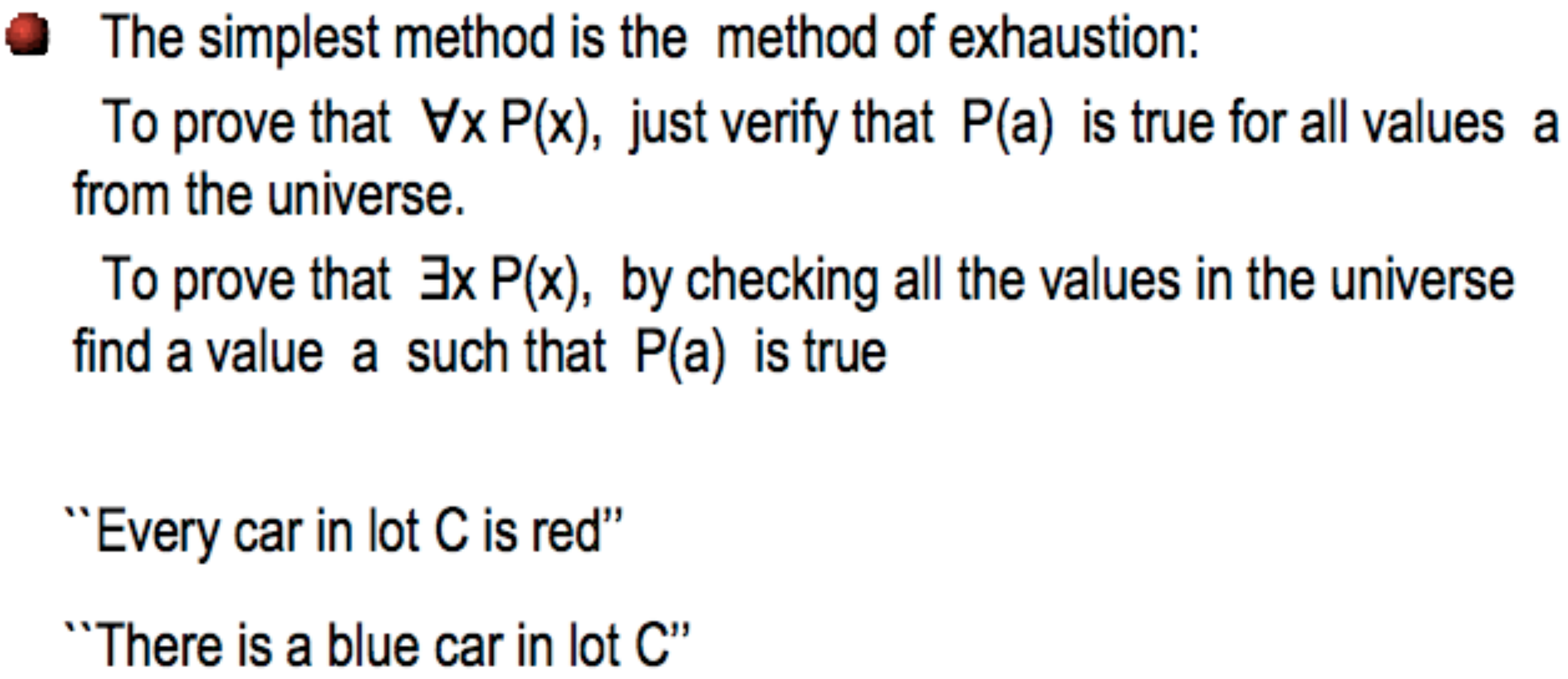
Section 2.5, 4.1, 5.5

Definition

- Theorem: A theorem is a statement that is true and has been proved to be true.
- Lemma: A lemma is a theorem whose main purpose is to help prove another theorem.
- Corollary: A corollary is a result that is an immediate consequence of a theorem.

Proof Methods

- Exhaustive method



- The simplest method is the method of exhaustion:

  To prove that ∀x P(x), just verify that P(a) is true for all values a from the universe.

  To prove that ∃x P(x), by checking all the values in the universe find a value a such that P(a) is true

``Every car in lot C is red”

``There is a blue car in lot C”

Direct Proofs

- Direct proofs are used when we need to proof statements like

  $$\forall x\,(P(x) \rightarrow Q(x))$$

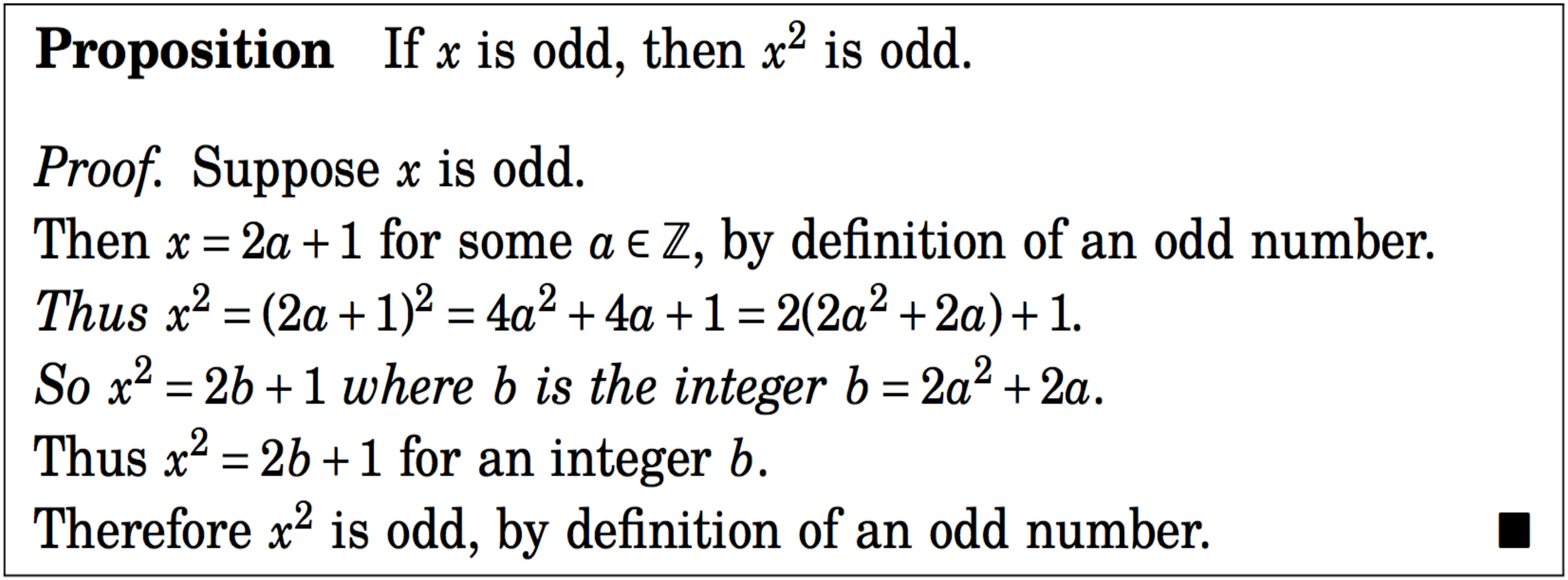
- Main steps

  Our goal is to prove that $P(a) \rightarrow Q(a)$ is a tautology for a generic value a.

  1. Assume that $P(a)$ is true
  2. Using axioms, previous theorems etc. prove that $Q(a)$ is true
  3. Conclude that $P(a) \rightarrow Q(a)$ is true
  4. Use the rule of universal generalization to infer

     $$\forall x\,(P(x) \rightarrow Q(x))$$

Direct Proofs



Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.

Then $x = 2a+1$ for some $a \in \mathbb{Z}$, by definition of an odd number.

Thus $x^2 = (2a+1)^2 = 4a^2+4a+1 = 2(2a^2+2a)+1$.

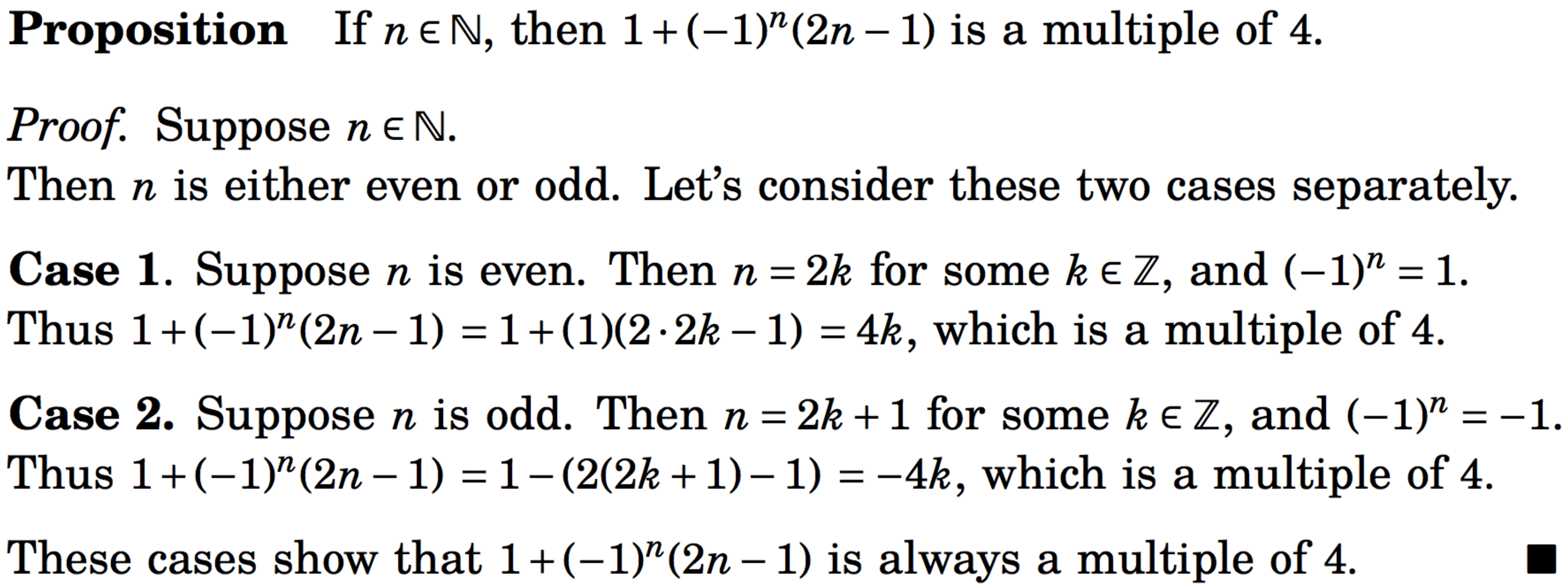
So $x^2 = 2b+1$ *where* b *is the integer* $b = 2a^2+2a$.

Thus $x^2 = 2b+1$ for an integer b.

Therefore x^2 is odd, by definition of an odd number. ■

Proof by cases

- In proving a statement is true, we sometimes have to examine multiple case before showing the statement is true in all possible scenarios.



Proposition If $n \in \mathbb{N}$, then $1+(-1)^n(2n-1)$ is a multiple of 4.

Proof. Suppose $n \in \mathbb{N}$.
Then n is either even or odd. Let's consider these two cases separately.

Case 1. Suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$, and $(-1)^n = 1$.
Thus $1+(-1)^n(2n-1) = 1+(1)(2 \cdot 2k-1) = 4k$, which is a multiple of 4.

Case 2. Suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$, and $(-1)^n = -1$.
Thus $1+(-1)^n(2n-1) = 1-(2(2k+1)-1) = -4k$, which is a multiple of 4.

These cases show that $1+(-1)^n(2n-1)$ is always a multiple of 4. ■

Proof by Contraposition

- Sometimes direct proofs do not work
- Definition: n is even if and only if there is k such that $n = 2k$
- Prove that if $3n + 2$ is even, then n is also even

  That is $\forall x\,(E(3x + 2) \rightarrow E(x))$
- Let us try the direct approach:

  As for the generic value n the number $3n + 2$ is even, for some k we have $3n + 2 = 2k$. Therefore $3n = 2(k + 1)$.

  Now what?
- What if instead of $\forall x\,(E(3x + 2\,) \rightarrow E(x))$ we prove the contrapositive, $\forall x\,(\neg E(x\,) \rightarrow \neg E(3x + 2))$?

Proof by Contraposition (contd.)

- So assume that n is odd, that is there is k such that $n = 2k + 1$.

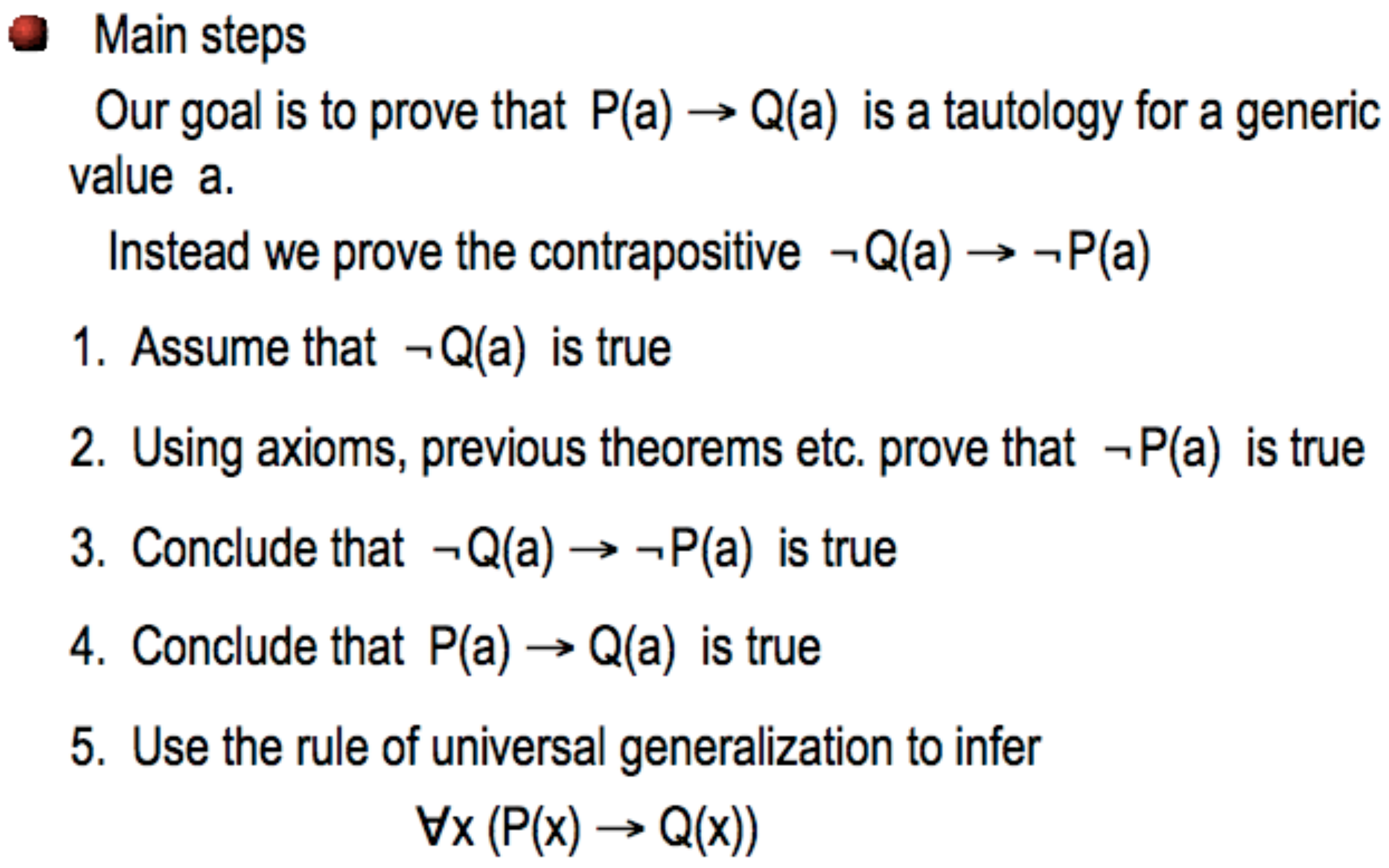
- Then $3n + 2 = 3\cdot(2k + 1) + 2 = 6k + 5 = 2(3k + 2) + 1$.

  That is $3n + 2$ is odd.

- We have proved that $\neg\mathrm{E}(3n + 2)$ is true, and therefore the contraposition $\forall x\,(\neg\mathrm{E}(x) \rightarrow \neg\mathrm{E}(3x + 2))$ is true.

  Finally, we conclude that the theorem $\forall x\,(\mathrm{E}(3x + 2) \rightarrow \mathrm{E}(x))$ is also true.

Proof by Contraposition (contd.)



- Main steps

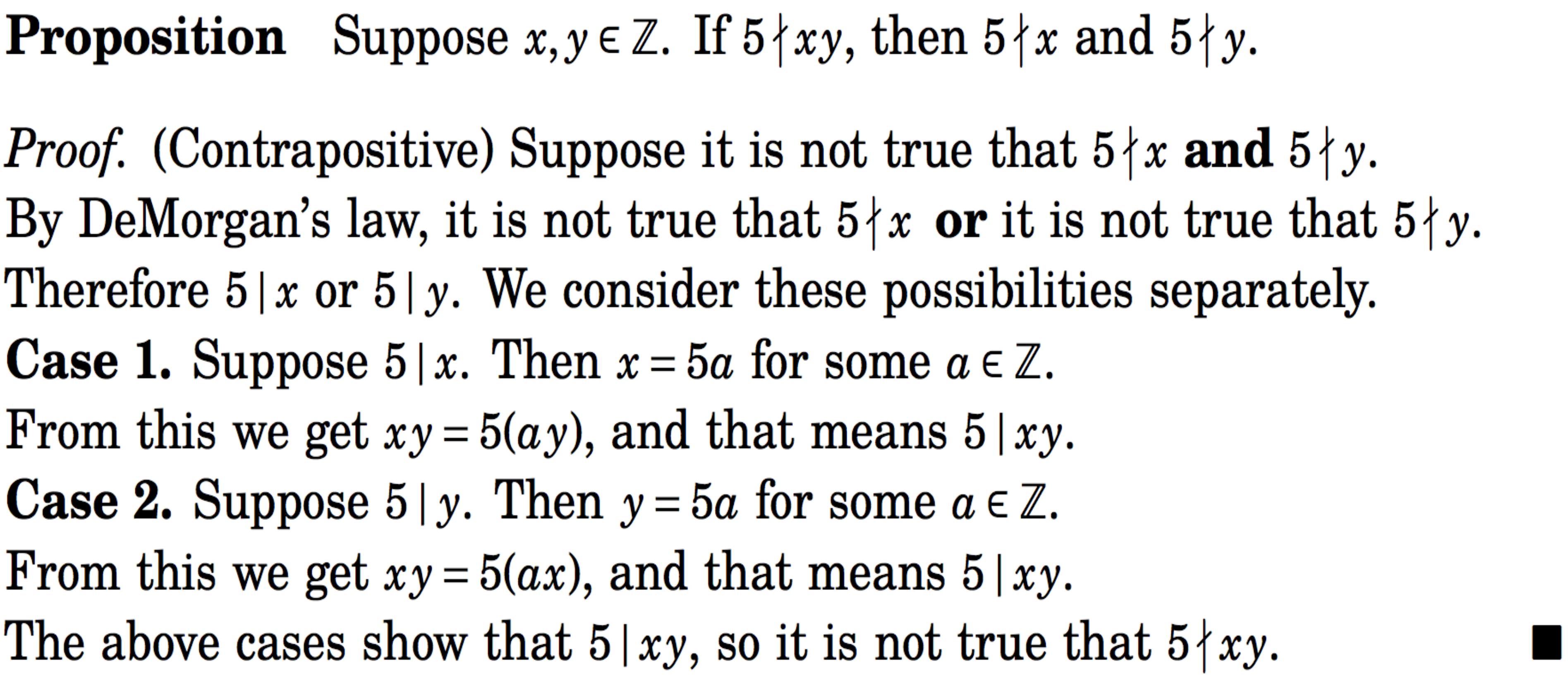
  Our goal is to prove that $P(a) \rightarrow Q(a)$ is a tautology for a generic value a.

  Instead we prove the contrapositive $\neg Q(a) \rightarrow \neg P(a)$

1. Assume that $\neg Q(a)$ is true
2. Using axioms, previous theorems etc. prove that $\neg P(a)$ is true
3. Conclude that $\neg Q(a) \rightarrow \neg P(a)$ is true
4. Conclude that $P(a) \rightarrow Q(a)$ is true
5. Use the rule of universal generalization to infer

$$\forall x\,(P(x) \rightarrow Q(x))$$

Example



Proposition Suppose $x, y \in \mathbb{Z}$. If $5 \nmid xy$, then $5 \nmid x$ and $5 \nmid y$.

Proof. (Contrapositive) Suppose it is not true that $5 \nmid x$ **and** $5 \nmid y$.
By DeMorgan's law, it is not true that $5 \nmid x$ **or** it is not true that $5 \nmid y$.
Therefore $5 \mid x$ or $5 \mid y$. We consider these possibilities separately.
Case 1. Suppose $5 \mid x$. Then $x = 5a$ for some $a \in \mathbb{Z}$.
From this we get $xy = 5(ay)$, and that means $5 \mid xy$.
Case 2. Suppose $5 \mid y$. Then $y = 5a$ for some $a \in \mathbb{Z}$.
From this we get $xy = 5(ax)$, and that means $5 \mid xy$.
The above cases show that $5 \mid xy$, so it is not true that $5 \nmid xy$. ■

Proof by Contradiction

- Proofs by contradiction use the Rule of Contradiction

$$\begin{array}{l} \quad \neg p \rightarrow F \\ \hline \therefore\ p \end{array}$$

- Can be used to prove statements of any form

- Main steps
  1. Assume $\neg p$.
  2. Using axioms, previous theorems etc. infer a contradiction
  3. Conclude p.

- Usually the contradiction has the form $\exists x\,(Q(x) \wedge \neg Q(x))$

Example

- The following problems have been solved using the proof by contradiction method.
  1. Show that square-root(2) is irrational
  2. Show that there are infinitely many primes.
  3. For any integer a, if a^2 is even, then a is even.

Outline for Proving a Conditional Statement with Contradiction

Proposition If P, then Q.

Proof. Suppose P and $\sim Q$.

$$\vdots$$

Therefore $C \wedge \sim C$. ■

Some words of advice

- It is best to use proof by contradiction when the direct and the contrapositive approaches do not seem to work.

Proving Existential Statements

- How to prove $\exists x\, P(x)$.
- Constructive proofs: find or construct a value a such that $P(a)$ is true.

  Prove that there is a grey car…

  My car is grey!
- Pure proofs of existence:

  Assume that $\forall x\, \neg P(x)$.

  Using axioms, previous theorems etc. infer a contradiction

  Thus, this is a proof by contradiction.

Set Theory

Sections 3.1, 3.2, 3.3

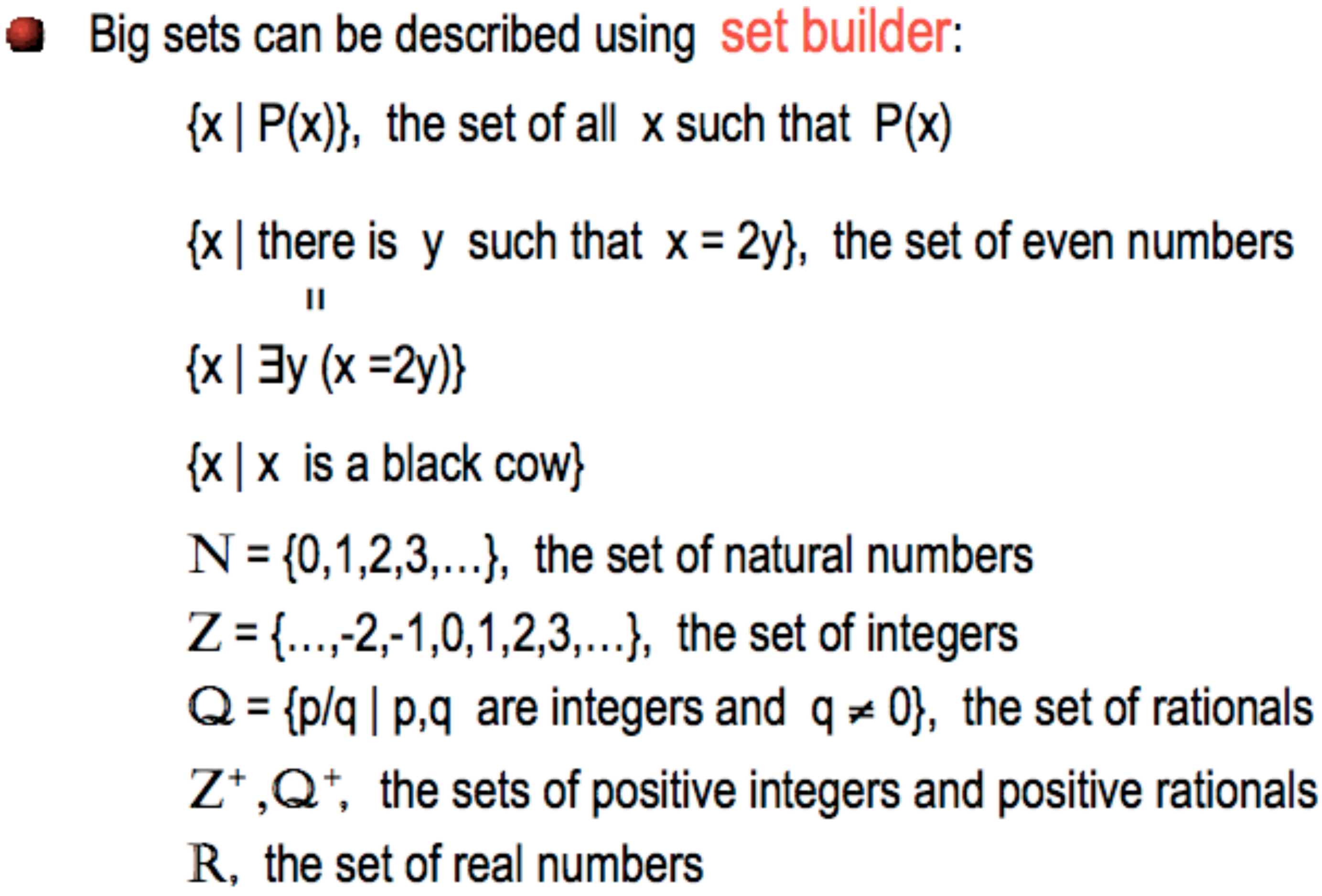
Set Theory

- A set is an unordered collection of objects.
- The objects in a set are called elements.
- One way to describe a set is to list its elements
  {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} – the set of digits

  (a, b, …., x, y, x} – the alphabet set
- A set can be element of another set

  {{a,b, ...}, {0,1,2, …., 9}, ... ,{α, β, ….}, ….} – set of all alphabets

Set builder



- Big sets can be described using set builder:

  {x | P(x)}, the set of all x such that P(x)

  {x | there is y such that x = 2y}, the set of even numbers

  ||

  {x | ∃y (x =2y)}

  {x | x is a black cow}

  N = {0,1,2,3,…}, the set of natural numbers

  Z = {…,-2,-1,0,1,2,3,…}, the set of integers

  Q = {p/q | p,q are integers and q ≠ 0}, the set of rationals

  Z^+, Q^+, the sets of positive integers and positive rationals

  R, the set of real numbers

Some illustrations of set-builder notation

1. $\{n : n \text{ is a prime number}\} = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$
2. $\{n \in \mathbb{N} : n \text{ is prime}\} = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$
3. $\{n^2 : n \in \mathbb{Z}\} = \{0, 1, 4, 9, 16, 25, \ldots\}$
4. $\{x \in \mathbb{R} : x^2 - 2 = 0\} = \{\sqrt{2}, -\sqrt{2}\}$
5. $\{x \in \mathbb{Z} : x^2 - 2 = 0\} = \emptyset$
6. $\{x \in \mathbb{Z} : |x| < 4\} = \{-3, -2, -1, 0, 1, 2, 3\}$
7. $\{2x : x \in \mathbb{Z}, |x| < 4\} = \{-6, -4, -2, 0, 2, 4, 6\}$
8. $\{x \in \mathbb{Z} : |2x| < 4\} = \{-1, 0, 1\}$

Special sets

- The empty set: $\emptyset = \{\}$
- The natural numbers: $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$
- The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots\}$
- The rational numbers: $\mathbb{Q} = \{x : x = \frac{m}{n},$ where $m, n \in \mathbb{Z}$ and $n \neq 0\}$
- The real numbers: $\mathbb{R}$ (the set of all real numbers on the number line)

Universe

- Although, in theory, elements of sets can be anything, in practice, it is not very convenient to allow such diversity. Say, if we are talking about numbers, all sets we can encounter have numbers as elements. If we work in propositional logic, then we are dealing with sets of statements, etc.
- This is why we usually have some sort of a universal set or a universe in mind, that contains all objects we may need.
- Example

$\{ x \mid 1 \le x \le 10 \}$	What is this set?
$\{ x \in \mathbb{Z} \mid 1 \le x \le 10 \}$	the set of all integers from 1 to 10
$\{ x \in \mathbb{Q} \mid 1 \le x \le 10 \}$	the set of all rationals from 1 to 10

Equality of Sets, Subsets

- Two sets are equal if they have the same elements.
- If B is a subset of A, every element of B is an element of A. We write $B \subseteq A$

Equality of Sets, Subsets (contd.)

$\{1,3\} \subseteq \{1,3,5\}$

$$\begin{tikzcd}[column sep=small, row sep=small]
 & Z \arrow[dr, phantom, "\subseteq" sloped] & & \\
Z^+ \arrow[ur, phantom, "\subseteq" sloped] \arrow[dr, phantom, "\subseteq" sloped] & & Q \arrow[r, phantom, "\subseteq"] & R \\
 & Q^+ \arrow[ur, phantom, "\subseteq" sloped] & &
\end{tikzcd}$$

- Set B is not a subset of a set A if

  $\exists x\,(x \in B \wedge x \notin A)$

  There is an element in B that is not an element of A

- Another way to say that two sets are equal: each of them is a subset of the other

Equality of Sets, Subsets (contd.)

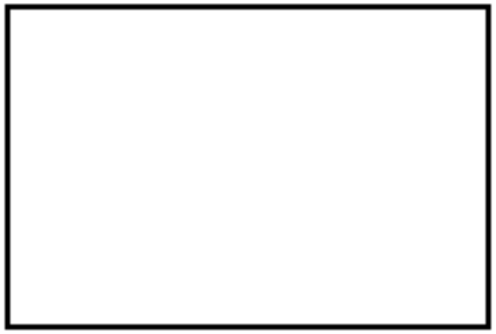
- A set B is a proper subset of a set A, if it is a subset A and is not equal to A ($B \subset A$).
- If A is a subset of B and B is a subset of C, A is a subset of C. (Transitive relation)
- Empty set has no element, denoted by $\varnothing$
  - How many elements does the set $\{\varnothing\}$ contain?
- **Theorem.** For any set A, (i) $\varnothing \subseteq A$, and (ii) $A \subseteq A$.
- Cardinality of a set: It is the number of elements in the set. The cardinality of A: |A|=n.
  - A set with finite number of elements is called a finite set.
  - A set with infinite number of elements is called an infinite set.
  - Sets N, Z, Q, R are infinite.

Power set of a set

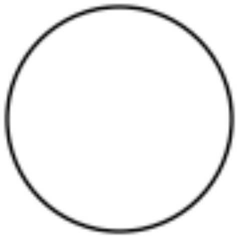
- Given a set A, the power set of A, P(A), is the set of all subsets of A.
- Theorem: If A is finite, $|P(A)| = 2^{|A|}$.

Venn Diagram

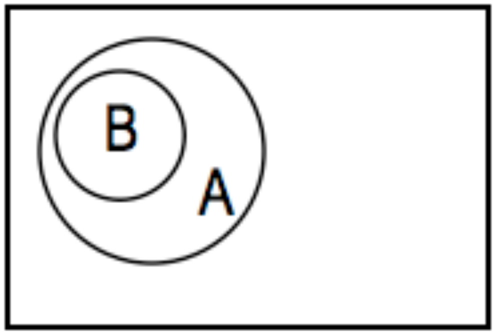
- It is often used to visualize the various relations between the sets.



universe



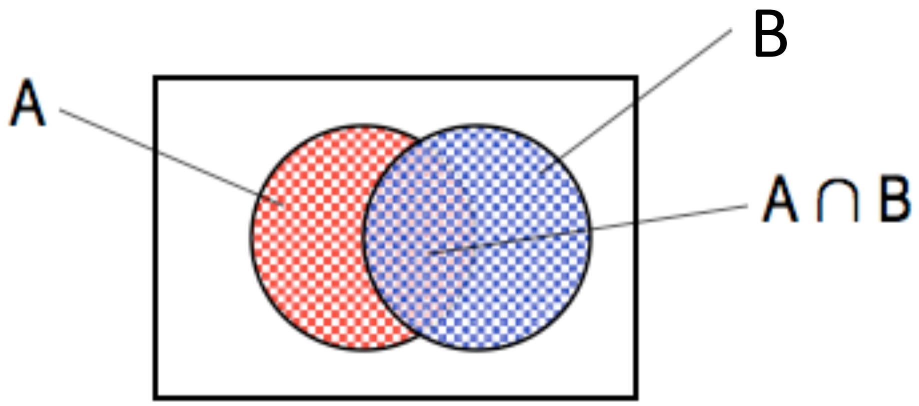
set



B is a subset of A

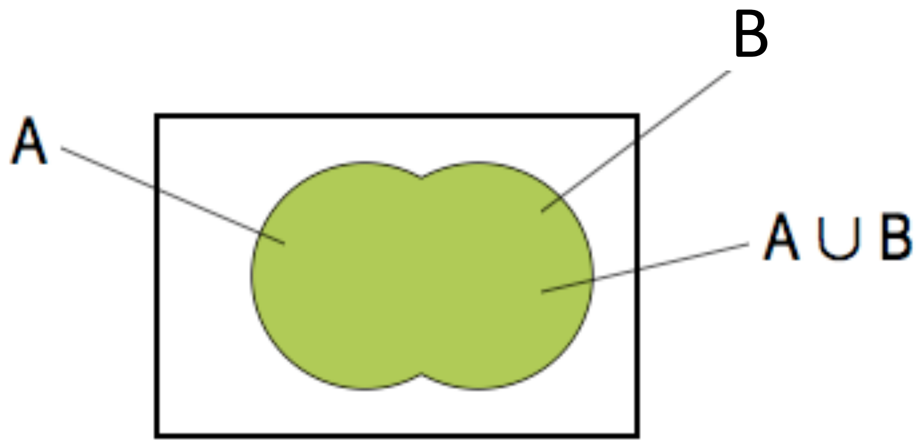
Intersection

- The intersection of sets A and B, denoted by A B,∩; the set that contains those elements in both A and B.



Union

- The union of sets A and B, denoted by A ∪ B, is the set that contains those elements that are in either A or B.



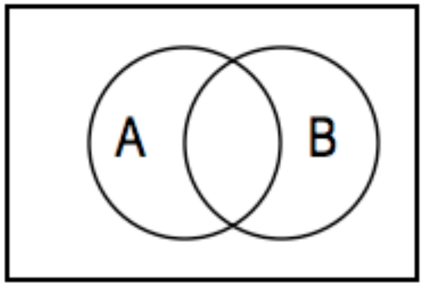
Disjoint Sets and Principle of Inclusion-Exclusion

- Sets A and B are said to be disjoint if $A \cap B = \varnothing$.

  Sets {Mon,Tue,Wed,Thu,Fri} and {Sat,Sun} are disjoint.

- Principle of inclusion-exclusion. For any finite sets A and B

$$|A \cup B| = |A| + |B| - |A \cap B|$$

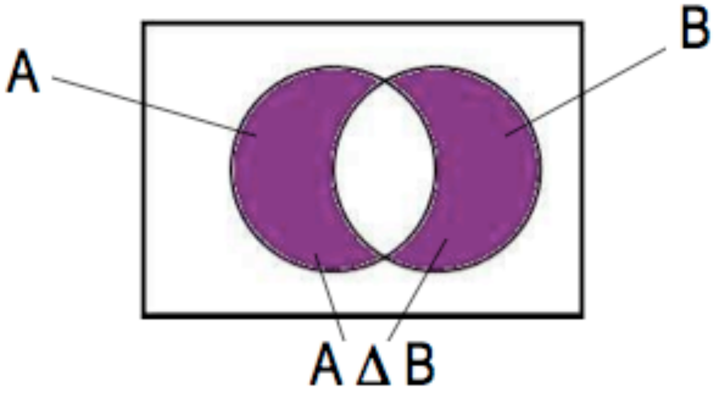


To count elements in $A \cup B$ we first count elements of A, then elements of B. Elements of $A \cap B$ are counted twice, so, we subtract the number of such elements

- If A and B are disjoint, then $|A \cup B| = |A| + |B|$

Symmetric Difference

- The symmetric difference of sets A and B, denoted by A Δ B, is the set that contains those elements that are either in A or in B, but not in both.
- $A \Delta B = \{ x \mid x \in A \oplus x \in B\}$

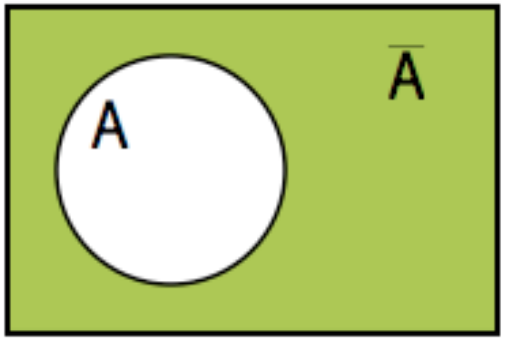


- Example
  {Jan.,Feb.,Mar.} Δ {Dec.,Jan.,Feb.} = {Dec.,Mar.}

Complement

- Let A be a set and U a universe, $A \subseteq U$. The complement of A, denoted by $\overline{A}$, is the set that comprises all elements of U that do not belong to A.

$$\overline{A} = \{ x \mid x \in U \text{ and } x \notin A \} = \{ x \mid x \notin A \}$$

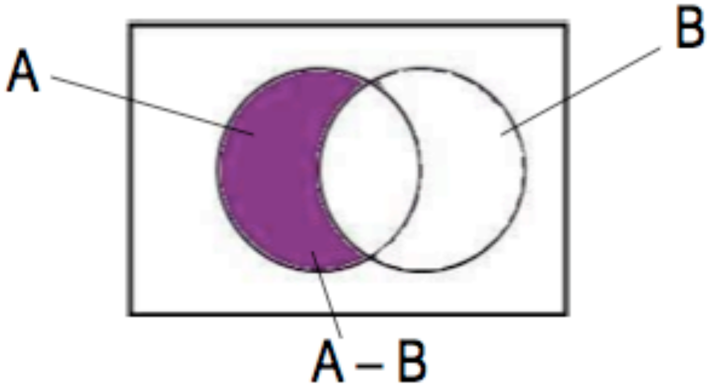


- Let the universe be the set of all integers, and $A = \{ x \mid \exists y \ \ x=2y \}$ Then $\overline{A}$ is the set of all odd numbers

Difference

- The difference of sets A and B (or relative complement of B in A), denoted by A – B, is the set containing those elements that are in A, but not in B.

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



- $\{1,3,5\} - \{1,2,3\} = \{5\}$
- Clearly, $\overline{A} = U - A$.

Sets and Logic

- If we look closer at the second proof, we notice that there is a very tight connection between set operations and logic connectives

$\neg$ corresponds to complement $\overline{}$

$\vee$ corresponds to union $\cup$

$\wedge$ corresponds to intersection $\cap$

$\oplus$ corresponds to symmetric difference Δ

0 (false) corresponds to the empty set $\varnothing$

1 (truth) corresponds to the universe U

Laws of Set Theory

$\overline{A \cap B} = \overline{A} \cup \overline{B}$	
$A \cup \varnothing = A$ $A \cap U = A$	Identity laws
$A \cup U = U$ $A \cap \varnothing = \varnothing$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws

More Laws of Set Theory

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cap (A \cup B) = A$ $A \cup (A \cap B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \varnothing$	Complement laws

Inclusion-Exclusion (revisit)

- 2 sets:

  $|A \cup B| = |A|+|B| - |A \cap B|$

- 3 sets:

  $|A \cup B \cup C| = |A|+|B|+|C|-|A \cap B|-|A \cap C|-|B \cap C|+|A \cap B \cap C|$

- *n* - sets:

  $|A_1 \cup A_2 \cup \cdots \cup A_n| =$

  $|A_1|+|A_2|+\cdots+|A_n|$

  $-|A_1 \cap A_2|-|A_1 \cap A_3|-\cdots$

  $+|A_1 \cap A_2 \cap A_3|+|A_1 \cap A_2 \cap A_4|+\cdots$

  $\vdots$

  $+(-1)^{n-1}|A_1 \cap A_2 \cap \cdots \cap A_n|$

Proof involving sets

- Some important definitions; Let A and B be sets.

$$\begin{aligned}
A \times B &= \{(x, y) : x \in A,\ y \in B\}, \\
A \cup B &= \{x : (x \in A) \vee (x \in B)\}, \\
A \cap B &= \{x : (x \in A) \wedge (x \in B)\}, \\
A - B &= \{x : (x \in A) \wedge (x \notin B)\}, \\
\overline{A} &= U - A.
\end{aligned}$$

Proof involving sets

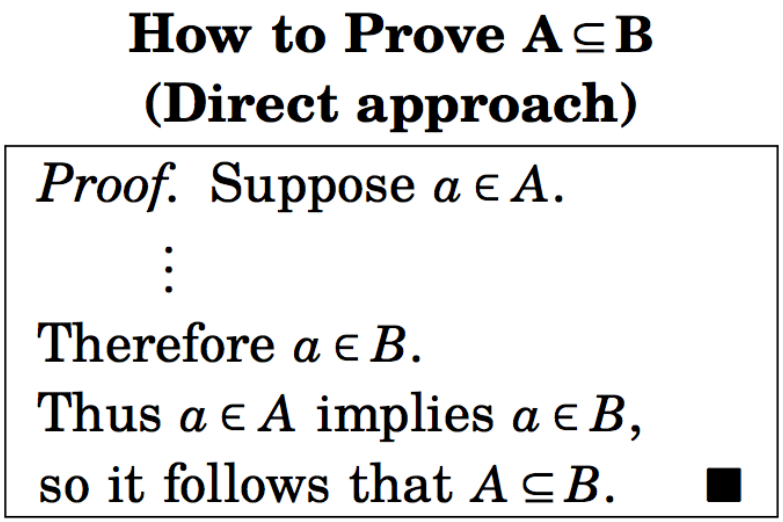
How to show $\mathbf{a} \in \{\mathbf{x} : \mathbf{P}(\mathbf{x})\}$

Show that $P(a)$ is true.

How to show $\mathbf{a} \in \{\mathbf{x} \in \mathbf{S} : \mathbf{P}(\mathbf{x})\}$

1. Verify that $a \in S$.
2. Show that $P(a)$ is true.

Proof involving sets

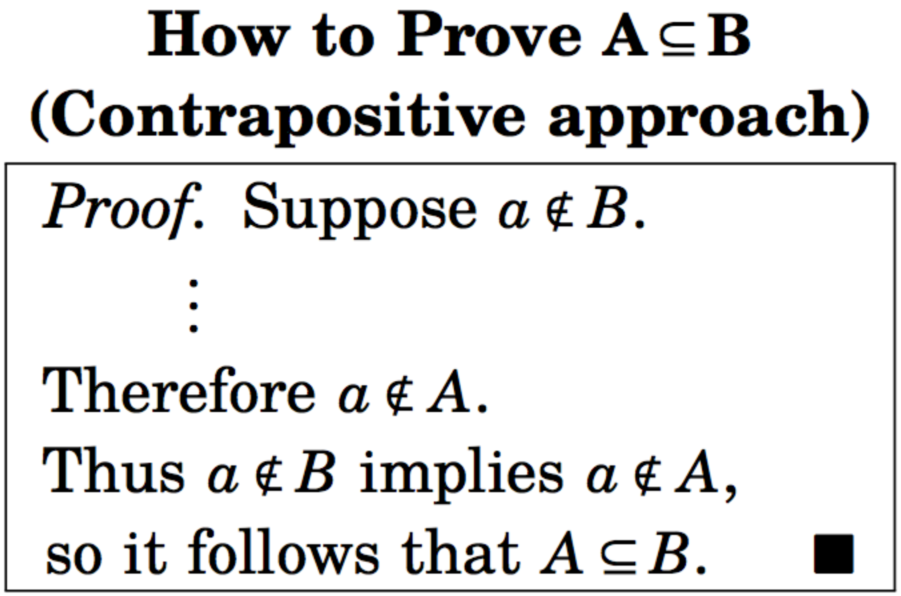


How to Prove A ⊆ B
(Direct approach)

Proof. Suppose $a \in A$.

$\vdots$

Therefore $a \in B$.
Thus $a \in A$ implies $a \in B$,
so it follows that $A \subseteq B$. ■



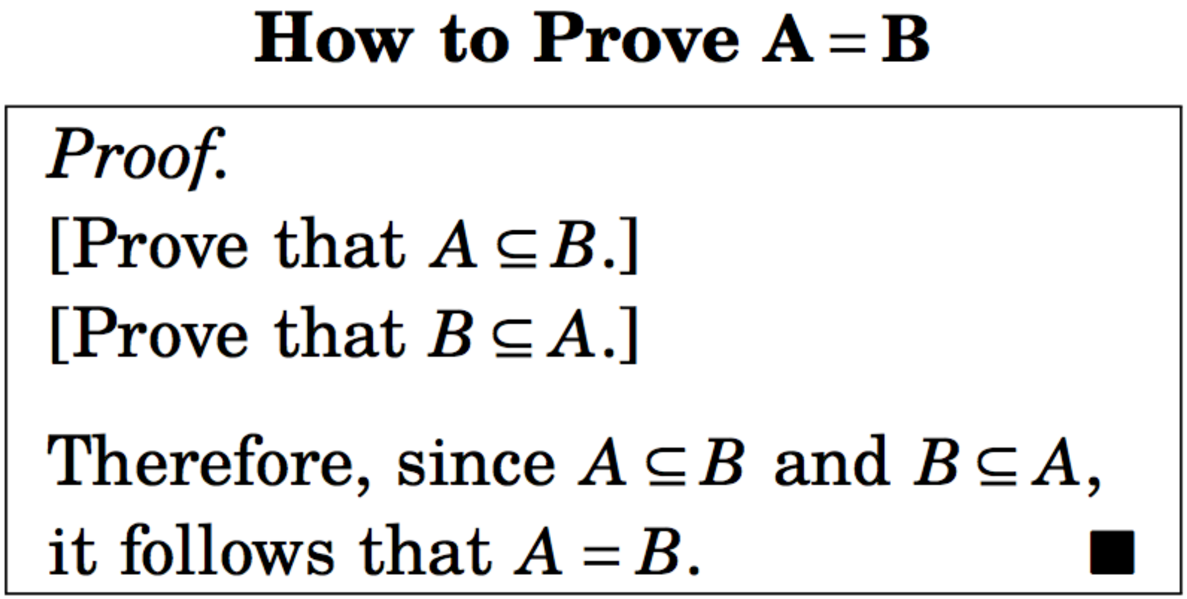
How to Prove A ⊆ B
(Contrapositive approach)

Proof. Suppose $a \notin B$.

$\vdots$

Therefore $a \notin A$.
Thus $a \notin B$ implies $a \notin A$,
so it follows that $A \subseteq B$. ■

Proof involving sets



How to Prove $\mathbf{A = B}$

Proof.

[Prove that $A \subseteq B$.]

[Prove that $B \subseteq A$.]

Therefore, since $A \subseteq B$ and $B \subseteq A$, it follows that $A = B$. ■

Probability Theory

Section 3.4 and 3.5

Sample space

- Experiment: tossing a coin, rolling a die, selecting subjects from a group at random
- The set of all possible outcomes of an experiment is called a sample space.
- Under the assumption of equal likelihood, let S be the sample space for an experiment E. Each subset of S, including empty set, is called an event. Each element of S determines an outcome, so if |S| =n and a ε S, A ⊆ S, then
  – Pr({a}) = Pr(a) = |{a}|/|S| = 1/n
  – Pr(A) = |A|/n

Axioms of Probability

- Let S be the sample space for an experiment E. If A and B are any events – that is $\Phi \subseteq A, B \subseteq S$, then
  - $\Pr(A) \geq 0$
  - $\Pr(S)=1$
  - if A, B are disjoint (or, mutually disjoint) the $\Pr(A \cup B) = \Pr(A) + \Pr(B)$.
- The Rule of Complement: $\Pr(\overline{A})=1-\Pr(A)$

Examples of sample space

1. **Tossing a fair (unbiased) coin:** Sample space $S = \{H, T\}$, and $Pr(\{H\}) = Pr(\{T\}) = \frac{1}{2}$

2. **Tossing a fair coin three times:** Here $S = \{(t_1, t_2, t_3) | t_i \in \{H, T\}\}$. Here t_i is the outcome of the i^{th} toss. The probability of each outcome, such as (H, T, T), is $\frac{1}{8}$. If we toss the coin n times, the size of the sample space is 2^n, and each point having probability $\frac{1}{2^n}$.

3. **Rolling two distinguishable dice (one red, one blue):** The sample space is $S = \{(i, j) : 1 \leq i, j \leq 6\}$. There are 36 elements in the sample space. Each of the outcomes has equal probability, $\frac{1}{36}$.

Examples of sample space

4. **Rolling two indistinguishable dice (both red):** The sample space here is $S = \{\{i, j\} : 1 \leq i \leq j \leq 6\}$. An outcome of one die 3 and the other 5 is written as $\{3, 5\}$ with the smaller one first. There are 21 elements in the sample space. Now the probability of each sample point is not the same. The probability of an outcome of the form $\{i, i\}$ is $\frac{1}{36}$. However the probability of an outcome $\{i, j\}$, $i \neq j$, is $\frac{2}{36}$ (why?).

5. **Card shuffling:** The deck of cards has 52 cards. Shuffle a deck of cards. The sample space consists of 52! permutations of the deck, each with equal probability $\frac{1}{52!}$.

6. **Poker hands:** The sample space consists of all possibe five-card hands. The sample space has $\binom{52}{5}$ elements, each with probability $\frac{1}{\binom{52}{5}}$.

Examples of sample space

7. **Balls and bins with distinguishable balls:** Bins (there are k such bins) are distinguishable and the balls (there are n such balls) are distinguishable. An outcome is $(b_1, b_2, \ldots b_n)$ where b_i is the bin number ball i lies. The sample space has k^n n-tuples, each with equal probability $\frac{1}{k^n}$.

8. **Balls and bins with indistinguishable balls:** Bins (there are k such bins) are distinguishable and the balls (there are n such balls) are indistinguishable. After throwing the balls, we see only the number of balls that landed in each bin. Each outcome is a k-tuple $(m_1, m_2, \ldots, m_k)$ where m_i denotes the number of balls in bin i. The number of sample points is therefore $\binom{n+k-1}{k-1}$. The probalities of sample points are not the same. Why?

Mathematical Induction

Section 4.1

Mathematical Induction

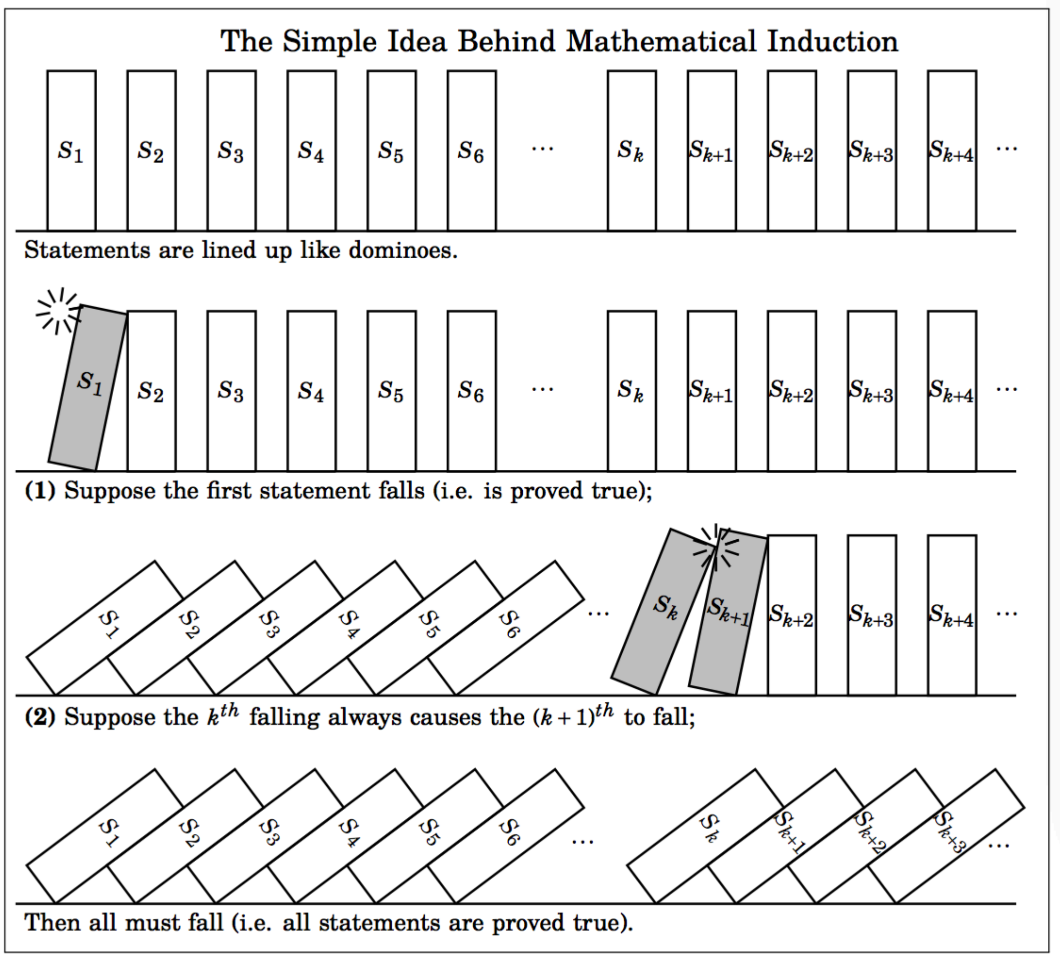
(section 4.1)

- Mathematical induction is a rigorous method that proves statements with absolute certainty.

Mathematical Induction

- It is a powerful proof techniques.

The Simple Idea Behind Mathematical Induction



Statements are lined up like dominoes.

(1) Suppose the first statement falls (i.e. is proved true);

(2) Suppose the k^{th} falling always causes the $(k+1)^{th}$ to fall;

Then all must fall (i.e. all statements are proved true).

Principle of Mathematical Induction

- Let S(n) denote a mathematical statement for all positive integers n. In order to prove S(n) is true for all positive integers n, we complete two steps:
  - – Basis step: We verify that S(1) is true.
  - – Inductive step: We show that, given any integer $k \geq 1$, conditional statement $S(k) \rightarrow S(k + 1)$ is true
  - – It follows by mathematical induction that every S(n) is true.
- Symbolically

$$(S(1){}^\wedge\ \forall(k \geq 1)\ \ (S(k) \rightarrow S(k+1))) \rightarrow \forall(n \geq 1)\ S(n)$$

Example: Suppose $a_1, a_2, \ldots, a_n$ are n integers, where $n \geq 2$. If p is prime and $p|(a_1 \times a_2 \times \ldots \times a_n)$, then $p|a_i$ for at least one of the a_i.

Proof: The proof is on induction on n.

- The basis step involves $n = 2$. Suppose $p|a_1a_2$. We have seen that either $p|a_1$ or $p|a_2$.
- Suppose that $k \geq 2$ and $p|(a_1 \times a_2 \times \ldots \times a_k)$ implies then $p|a_i$ for some a_i. (Inductive hypothesis)
- Now let $p|(a_1 \times a_2 \times \ldots \times a_k \times a_{k+1})$. Then $p|((a_1 \times a_2 \times \ldots \times a_k) \times a_{k+1})$. By what we proved in the basis step, it follows that $p|(a_1 \times a_2 \times \ldots \times a_k)$ or $p|a_{k+1}$. This and the inductive hypothesis imply that p divides one of the a_i.

Principle of Strong Mathematical Induction

- Sometimes mathematical induction is not enough.
- In order to prove that $S(n)$ is true for all positive integer $n \geq n_0$, we complete two steps:
  - Basis step: We verify that $S(n_0)$, $S(n_0+1)$, ..., $S(n_1)$ are true.
  - Inductive step: We show that conditional statement $(S(n_0)\wedge S(n_0+1)\wedge \ldots\wedge S(k)) \rightarrow S(k + 1)$ for all positive integers $k \geq n_1$.
  - It follows by mathematical induction that every $S(n)$, $n\geq n_0$ is true.
- Symbolically

$$(S(n_0)\wedge S(n_0+1)\wedge \ldots\wedge S(n_1)\wedge \forall k(S(n_1+1)\wedge \ldots\wedge S(k)) \rightarrow \forall(n\geq n_0)\, S(n)$$

The Well-Ordering Principle

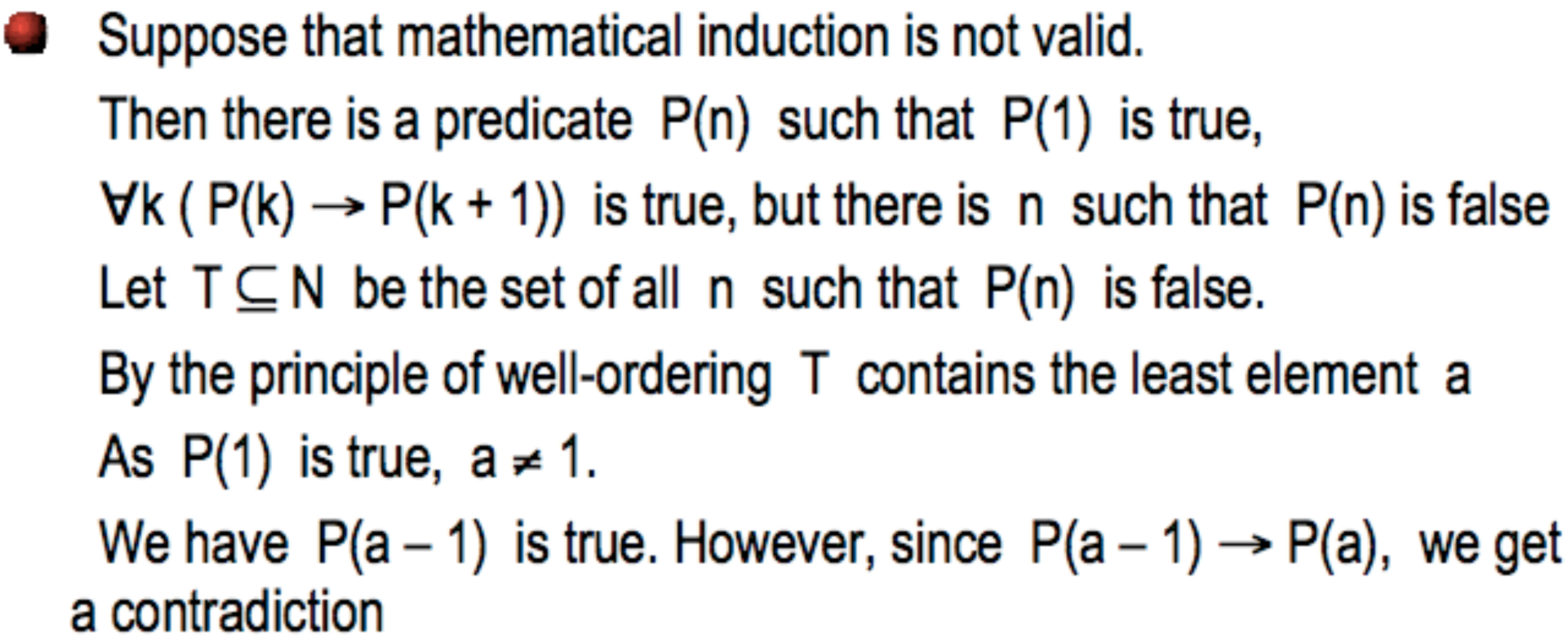
- The proofs of principle of induction and proof of strong induction use the well-ordering principle.

  (Principle)

  – Every non-empty subset of N, set of nonnegative integers, contains a smallest element. (We often express this by saying that N is well-ordered.

  – Note that sets of all integers, rational numbers, real numbers do not have this property. (Why?)

Why Induction Works



- Suppose that mathematical induction is not valid.

  Then there is a predicate $P(n)$ such that $P(1)$ is true,

  $\forall k\,(P(k) \rightarrow P(k+1))$ is true, but there is n such that $P(n)$ is false

  Let $T \subseteq N$ be the set of all n such that $P(n)$ is false.

  By the principle of well-ordering T contains the least element a

  As $P(1)$ is true, $a \neq 1$.

  We have $P(a-1)$ is true. However, since $P(a-1) \rightarrow P(a)$, we get a contradiction

Summation

- Prove that the sum of the first n natural numbers equals $\frac{n(n+1)}{2}$ that is $1+2+3+\cdots+n=\frac{n(n+1)}{2}$

- P(n): `the sum of the first n natural numbers …
- Basis step: P(1) means $1=\frac{1(1+1)}{2}$

- Inductive step: Make the inductive hypothesis, P(k) is true, i.e.

$$1+2+3+\cdots+k=\frac{k(k+1)}{2}$$

Prove P(k + 1): $1+2+3+\cdots+k+(k+1)=\frac{(k+1)((k+1)+1)}{2}$

$$1+2+3+\cdots+k+(k+1)=\frac{k(k+1)}{2}+(k+1)$$

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

More Summation

- Prove that $1+2+2^2+\cdots+2^n = 2^{n+1}-1$
- Let P(n) be the statement `$1+2+2^2+\cdots+2^n = 2^{n+1}-1$' for the integer n

- Basis step: P(0) is true, as $2^0 = 1 = 2^{0+1}-1$
- Inductive step: We assume the inductive hypothesis

$$1+2+2^2+\cdots+2^k = 2^{k+1}-1$$

and prove P(k + 1), that is

$$1+2+2^2+\cdots+2^k+2^{k+1} = 2^{(k+1)+1}-1 = 2^{k+2}-1$$

We have
$$\begin{aligned} 1+2+2^2+\cdots+2^k+2^{k+1} &= (2^{k+1}-1)+2^{k+1} \\ &= 2\cdot 2^{k+1}-1 \\ &= 2^{k+2}-1 \end{aligned}$$

Problems

1. Show that 43 is the largest number you cannot write as the sum of 6, 9 or 20.
2. Show that p(x): $x=3a+8b$ for all $x \geq 14$ is true.
3. Show that $3|(5^{2n} - 1)$ for all non-negative integers n.

Class notes on sections 4.2, 5.1, 5.2 and 5.3

- Topics covered:
  - Recursive definition
  - Rudimentary discussion on relations
  - Functions: injective, surjective and bijective

Recursive Definitions

- Recursively defined sequence
  - Consider the Fibonacci sequence:

    $\{F_n\}$ = 1, 1, 2, 3, 5, ….

    Here F_1=1, F_2=1, F_3=2, …..

    Recursive Definition of $\{F_n\}$

    - Initialization: $F_1 = 1$, $F_2=2$
    - Recursion $F_n = F_{n-1} + F_{n-2}$, $n >= 3$

Recursive Definitions (contd.)

- Recursively defined functions
  - Consider the factorial function:

    n! = 1.2.3. ….(n-2)(n-1)n

    Here 0!=0, 1!=1, 2!=2

    Recursive Definition of n!

    - Initialization: 1! = 1
    - Recursion n! = n.(n-1)!, n >= 2

Recursive Definitions (contd.)

- **Recursively defined functions**
  - Consider the binomial function:
    $C(n,k) = \binom{n}{k} = \frac{n!}{k!(n-k)!}$
    Recursive definition of $C(n,k)$

    $C(n,k) = 0$ if $k < 0$ or $k > n$.

    $C(n,k) = 1$ if $k = 0; n = 0$

    $C(n,k) = C(n-1,k) + C(n-1,k-1)$, otherwise.

Recursive Definitions (contd.)

- Recursively defined mathematical notations
  - Consider the sum

    $S_n = a_1+a_2+ .... +a_n$

    Here $S_0=0$, $S_1 = a_1$, $S_2=a_2$

    Recursive Definition of S_n

    - Initialization: $S_1 = a_1$
    - Recursion $S_n= S_{n-1} + a_n$, $n >= 2$

  - Similar definitions can be described for the product

    $P_n= a_1a_2.....a_n$ where $P_1 = a_{1.}$

Recursive Definitions (contd.)

- Recursively defined sets (defining the elements of a set recursively)
  - Consider the set S of prices (cents) payable using quarters and dimes.

    Recursive Definition of S

    - Initialization: 0 ε S
    - Recursion If x ε S, x+10 ε S and x+25 ε S.

    Note that only the distinct elements of S are kept.
  - Recursive defn. of +ve and –ve powers of 2
    - Initialization: 1 ε T
    - IF x ε T, 2x ε T and x/2 ε T.

Recursive Definitions (contd.)

- Recursively defined sets (defining the elements of a set recursively)
  - Consider the power set of A.

$\mathcal{P}(\mathrm{A}) = \{\{\}\}$ when $A = \{\}$

$\mathcal{P}(\mathrm{A}) = \mathcal{P}(\mathrm{A}\text{-}\{\mathrm{x}\}) \cup \mathcal{P}(\mathrm{X} \cup \{\mathrm{x}\} | \mathrm{X} \in \mathcal{P}(\mathrm{A} - \{\mathrm{x}\})$ when A is not empty.

Recursive Definitions (contd.)

- Recursively defined character strings
  - Defn: A string is a finite sequence of 0 (null string) or more letters of alphabet Σ.

    For binary strings the alphabet set Σ = {0,1}.

    Defining binary strings B recursively:

    - Initialization: {} ε B
    - IF u ε B, u || ’0’ ε B and u || ’1’ ε B.

    Here || indicates concatenation.

Recursive Definitions

- Factorial

$$n! = \begin{cases} 1, \text{ if } n = 0 \\ n(n-1)!, \text{ if } n \geq 1 \end{cases}$$

- Fibonacci sequence

$$f(n) = \begin{cases} n, \text{ if } k = 0 \text{ or } 1 \\ f(n-2) + f(n-1), \text{ if } k \geq 2 \end{cases}$$

- Binomial Coefficients "*n*-choose-*k*"

$$C(n,k) = \begin{cases} 0, \text{ if } k < 0 \text{ or } k > n \\ 1, \text{ if } k = n = 0 \\ C(n-1,k-1) + C(n-1,k), \text{ otherwise} \end{cases}$$

- Addition of non-negative integers

$$m + n = \begin{cases} m, \text{ if } n = 0 \\ m+1, \text{ if } n = 1 \\ (m + (n-1)) + 1, \text{ if } n > 1 \end{cases}$$

- Summation Notation

$$\sum_{i=1}^{n} a_i = \begin{cases} 0, \text{ if } n = 0 \\ \sum_{i=1}^{n-1} a_i + a_n, \text{ if } n > 0 \end{cases}$$

- Product Notation

$$\prod_{i=1}^{n} a_i = \begin{cases} 1, \text{ if } n = 0 \\ \left(\prod_{i=1}^{n-1} a_i \right) \cdot a_n, \text{ if } n > 0 \end{cases}$$

Applications of Recursions

- Example: Find the recurrence for the number of n digit binary sequences with no pair of consecutive 1's.
  - Let A(n) denote the number of n digit binary sequences with no pair of consecutive 1s.
  - To write A(n) we condition on the last digit. If it is 0, the number of such sequence is A(n-1). If it is 1, the penultimate digit must be 0, and the number of such sequences sought is A(n-2).
  - Thus A(n) = A(n-1)+A(n-2) (inductive step)
  - Basis step: A(1) = 2; A(2) = 3

Relations

(sections 5.1)

- Let A and B are sets; A x B = {(a,b) | a ε A and b ε B}; (a,b) are ordered pairs, also known as 2-tuple.
- The universes of A and B could be different.
- R x R = {(x,y)| x,y ε R} is the two-dimensional real plane.
- Binary relation:
  - For sets A and B, any subset of AxB is a binary relation from A to B. Any subset of A x A is called binary relation on A.
  - A = Z^+; {(x,y)| x <= y} is a relation on A.

Relations

(sections 5.1)

- Let A_1, A_2, … , A_n be sets. An n-ary relation on these sets (in this order) is a subset of $A_1 \times A_2 \times \ldots \times A_n$.
- Most of the times we consider n = 2.

Relations as Subsets

A: Siblinghood. *A* = {people}

Because relations are just subsets, all the usual set theoretic operations are defined between relations which belong to the same Cartesian product.

Q: Suppose we have relations on {1,2} given by *R* = {(1,1), (2,2)}, *S* = {(1,1),(1,2)}. Find:

1. The union $R \cup S$
2. The intersection $R \cap S$
3. The symmetric difference $R \oplus S$
4. The difference *R*-*S*
5. The complement of *R*

Relations as Subsets

A: $R = \{(1,1),(2,2)\}$, $S = \{(1,1),(1,2)\}$

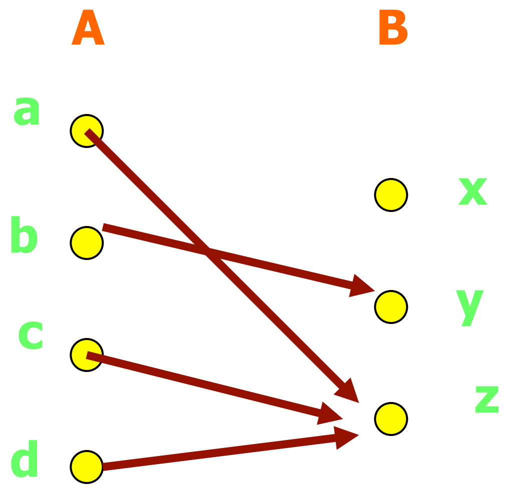
1. $R \cup S = \{(1,1),(1,2),(2,2)\}$
2. $R \cap S = \{(1,1)\}$
3. $R \oplus S = \{(1,2),(2,2)\}$.
4. $R - S = \{(2,2)\}$.
5. $\overline{R} = \{(1,2),(2,1)\}$

Functions (5.1,5.2,5.3)

- For non-empty sets A and B, a function (mapping) f from A to B (f: A → B) is a relation f (a subset of AxB) from A to B in which every element a ε A, the relation f contains exactly one pair of the form (a,b). The element (a,b) ε f is abbreviated as f(a) = b.
- A is the domain of f
  - B is the codomain of f
  - if f(a) = b, b is the image of a; a is the preimage of b
  - f is treated as a set
  - The range of f is the set {f(a): a ε A} = {b|(a,b) ε f}. The range is the set of all possible “output values” for f.

Example

- f(a) = z
- the image of d is z
- the domain of f is A = {a, b, c, d}
- the codomain is B = {x, y, z}
- f(A) = {y, z}
- the preimage of y is b
- the preimages of z are a, c and d
- f({c,d}) = {z}
- The range of f is {y,z}



Functions

- f: A→ B means
  - all a ε A have an image b ε B
  - some b ε B may not have a preimage a ε V
  - some b ε B may have more than one preimages a ε B
- f(A) denotes the subset X ⊆ B such that for any x ε X, there exists an element a ε A such that f(a) = x, and for any y ε B-X, there does not exist any a ε A such that f(a) = y.
  - X is called the range of f.

Functions

- Three things:
  - A function can be viewed as sending (mapping) elements from one set A to another set B.
  - Such a function can be regarded as a relation from A → B.
  - For every input value a (of A), there is exactly one output value f(a). (Vertical line test)

Some useful functions

- floor functions: real R → integer Z
  - floor(x) = greatest integer $\le$ x

    $= \lfloor x \rfloor$
- ceiling functions: real R → integer Z
  - ceiling(x) = least integer $\ge$ x

    $= \lceil x \rceil$
- $\lfloor 3.5 \rfloor = 3$; $\lfloor \pi \rfloor = 3$; $\lfloor -3.5 \rfloor = - 4$
- $\lceil 3.5 \rceil = 4$; $\lceil \pi \rceil = 4$; $\lceil -3.5 \rceil = -3$

Some examples

- $g: Z \times Z \rightarrow Z$ which is defined as

  $g((m,n)) = g(m,n) = 6m - 9n$.

  - Note that $g = \{((m,n),6m\text{-}9n) \mid (m,n) \in Z \times Z\}$
  - Domain is $Z \times Z$
  - Codomain is Z
  - Range is $\{ 3x : x \in Z\}$ (why? Discussed in the class)
- $A = \{p,q,r,s\}$; $B = \{0,1,2\}$;

  $f = \{(p,0), (q,1), (r,2), (s,2)\}$

  - f is a function with domain A, codomain B and range B.

Equality of functions

- Two functions $f:A \rightarrow B$ and $g:C \rightarrow D$ are equal if $A=C$, $B=D$ and $f(x)=g(x)$ for all $x \ \varepsilon\ A$.
- Caution: $f:Z \rightarrow N$ and $g:Z \rightarrow Z$, $f(x) = |x| +2$, and $g(x) = |x| +2$ are technically not equal.

Injective (one-to-one) Surjective (onto) functions

- A function f: A → B is:
  - Injective (one-to-one) if for every x,y ε A, x ≠ y, f(x) ≠ f(y). Equivalently:

$$\forall x, y \in A, x \neq y \to f(x) \neq f(y)$$
$$\text{Contraposition: } \forall x, y \in A, f(x) = f(y) \to x = y$$

  - Surjective (onto) if for every b ε B, there is an element a ε such that f(a) = b.

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

  - Bijective (one-to-one and onto) if f is injective and bijective.

one-to-one (injective) functions

- f: $Z^+ \rightarrow Z^+$ where $f(a) = a^2$ is one-to-one
- f: $Z \rightarrow Z^+$ where $f(a) = a^2$ is not one-to-one
- floor and ceiling function is not one-to-one.

onto (surjective) functions

- $f{:}Z \rightarrow Z$, $f(x) = x + 1$ is onto.
- $\lfloor . \rfloor : R \rightarrow Z$ is onto, but not one-to-one
- $\lceil . \rceil : R \rightarrow Z$ is onto, but not one-to-one

one-to-one and onto (bijection)

- f: R → R, f(x) = x + 1 is one-to-one correspondence
- f: [0,1] → [0,1/3], f(x) = x/3 is one-to-one and onto.
- f: R → R^+, f(x) = x^2 is not one-to-one, but onto.
- f: R → R, f(x) = x^3 is injective and surjective.

How to show a function f: A → B is injective?

- Direct approach: $\forall x, y \in A, x \neq y \rightarrow f(x) \neq f(y)$
  - Consider arbitrary x,y ε A; x ≠ y

    …. Reduction steps with the goal to show that f(x) ≠ f(y)
- Contraposition approach:

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

  - Suppose x,y ε A; f(x) = f(y)

    ….. Reduction steps with the goal to show that x=y.
- Often contrapositive approach is easy when f is an algebraic function

How to show a function f: A → B is surjective?

- f is surjective if for all b ε B, there exists a ε A such that f(a) = b. That is

  f is surjective if $\forall b \in B \; \exists a \in A \; f(a) = b$

- Contrapositive approach:

  not ($\forall b \in B \; \exists a \in A \; f(a) = b$ → f is not surjective

  i.e. $\exists b \in B \; \forall a \in A \; f(a) \neq b$ → f is not surjective

How to show a function f: A → B is surjective?

- f: R – {0} → R – {0}, f(x) = 1/x +1. Is it surjective?
  - Let b ε B be an arbitrary element. Let f(x) = b for some x ε A. This means that

    1/x + 1 = b

    i.e. x = 1/(b-1). Now x is not defined if b=1.

  Therefore f, as defined above, is not an onto function.
- Show that g : Z x Z → Z x Z, g(m,n)=(m+n,m+2n)

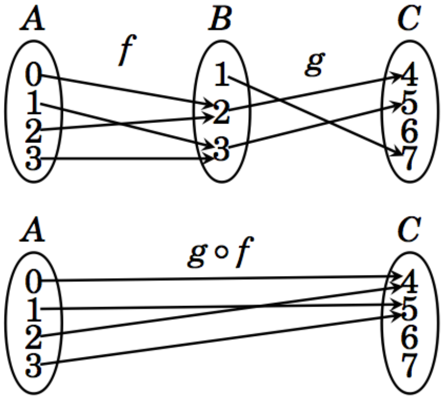
  is bijective. (Discussed in the class)

Section 5.6
Composition and inverse function

Composition functions

Composition

Suppose $f : A \to B$ and $g : B \to C$ are functions with the property that the codomain of f is the domain of g. $g \circ f : A \to C$ is the function called the composition of f with g. Here $g \circ f(x) = g(f(x))$. Thus $g \circ f$ sends elements of A to elements of C.



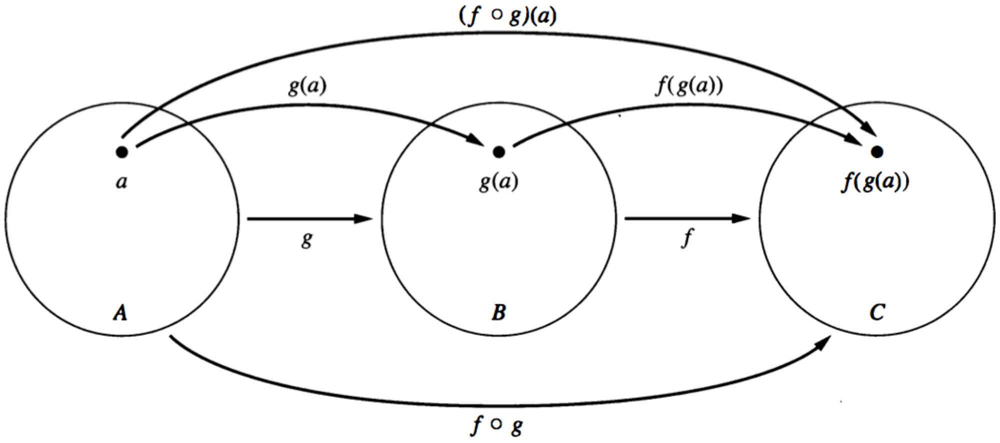
Notice that the composition $g \circ f$ also makes sense if the range of f is a subset of the domain of g.

Composition functions (contd)

Notice that the composition $g \circ f$ also makes sense if the range of f is a subset of the domain of g.

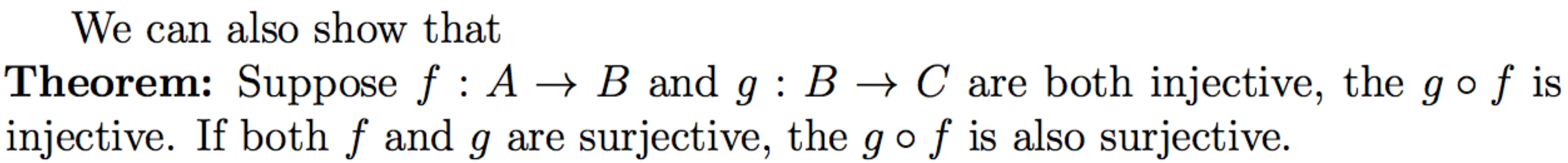
Example Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = x^2 + x$, and $g : \mathbb{R} \to \mathbb{R}$ be defined as $g(x) = x + 1$. Then $g \circ f : \mathbb{R} \to \mathbb{R}$ is the defined by $g \circ f(x) = g(f(x)) = g(x^2 + x) = x^2 + x + 1$.

Since the domains and the codomains of g and f are the same, $f \circ g$ is also defined. In this case $f \circ g(x) = f(g(x)) = f(x+1) = (x+1)^2 + (x+1)$. Note that $f \circ g$ and $g \circ f$ are not the same. This says that function composition is not commutative. However, the function composition is associative. That is if $f : A \to B$, $g : B \to C$, and $h : C \to D$, then $h \circ (g \circ f) = (h \circ g) \circ f$ show this).



A diagram of compositions of two functions. There is a nice diagram in the text, page 281.

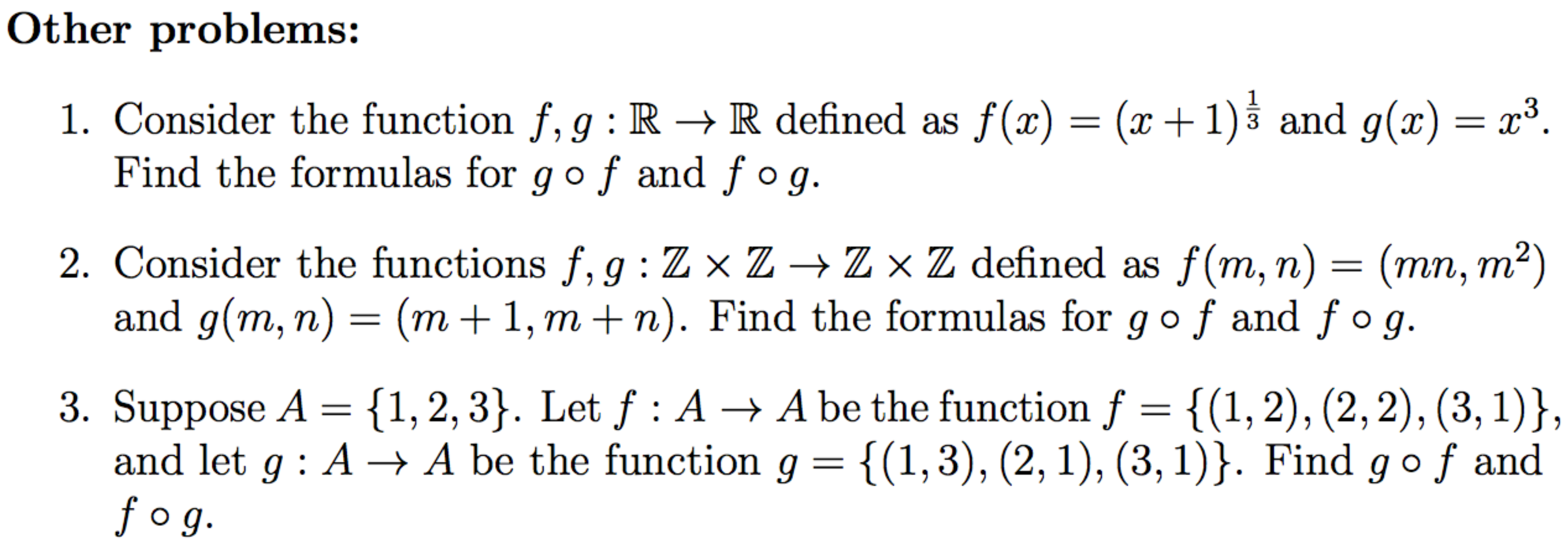
Composition functions (contd)



We can also show that

Theorem: Suppose $f : A \to B$ and $g : B \to C$ are both injective, the $g \circ f$ is injective. If both f and g are surjective, the $g \circ f$ is also surjective.

Problems from the text: Section 5.6: 3, 4, 7



Other problems:

1. Consider the function $f, g : \mathbb{R} \to \mathbb{R}$ defined as $f(x) = (x+1)^{\frac{1}{3}}$ and $g(x) = x^3$. Find the formulas for $g \circ f$ and $f \circ g$.

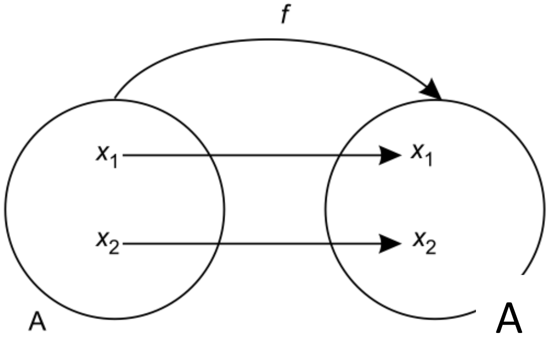
2. Consider the functions $f, g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined as $f(m, n) = (mn, m^2)$ and $g(m, n) = (m+1, m+n)$. Find the formulas for $g \circ f$ and $f \circ g$.

3. Suppose $A = \{1, 2, 3\}$. Let $f : A \to A$ be the function $f = \{(1, 2), (2, 2), (3, 1)\}$, and let $g : A \to A$ be the function $g = \{(1, 3), (2, 1), (3, 1)\}$. Find $g \circ f$ and $f \circ g$.

Important functions

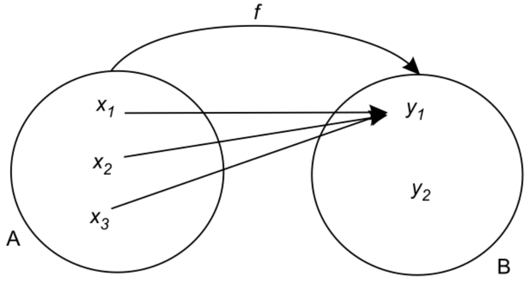
Identity function

Let A be a set. The function $f : A \to A$ is said to be an identity function on A if $\forall x \in A,\ f(x) = x$. f is also known as i_A.



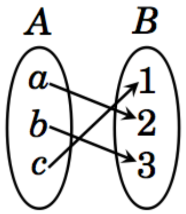
Constant function

The function $f : A \to B$ ıs saıd to be a constant tunctıon if $\forall a \in A,\ f(a) = y$ where $y \in B$ is a unique element.

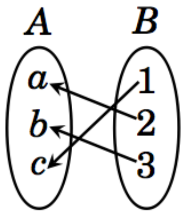


Inverse functions

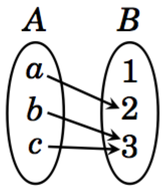
Definition: Let $R \subseteq A \times B$ be a relation. The inverse relation $R^{-1} \subset B \times A$ is the **inverse relation** where $R^{-1} = \{(y,x) : (x,y) \in R\}$. Alternately, the inverse relation R^{-1} of R is obtained by reversing the elements in every 2-tuple in R.



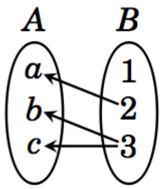
$f = \{(a,2),(b,3),(c,1)\}$



$f^{-1} = \{(2,a),(3,b),(1,c)\}$



$g = \{(a,2),(b,3),(c,3)\}$



$g^{-1} = \{(2,a),(3,b),(3,c)\}$

Note that in the second case g^{-1} is not a function. However f^{-1} is a function. We can show that that

Theorem: A function $f : A \to B$ is invertible (has an inverse) if and only if f is bijective. (Theorem 5.8 of the text)

Definition: If $f : A \to B$ is bijective then its inverse is the function $f^{-1} : B \to A$. Functions f and f^{-1} have the following properties:

1. $f^{-1} \circ f = i_A$ (i_A is the identity function on A), and
2. $f \circ f^{-1} = i_B$ (i_B is the identity function on B).

Definition: $f : A \to B$ is a function.

- If $X \subseteq A$, (image of X) $f(X) = \{f(x) : x \in X\} \subseteq B$.
- If $Y \subseteq B$, (pre-image of Y) $f^{-1}(Y) = \{x \in A : f(X) = Y\} \subseteq A$.

Example: Suppose $f : \{s, t, u, v, w, x, y, z\} \to \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
Let $f = \{(s, 4), (t, 8), (v, 1), (w, 2), (x, 4), (y, 6), (z, 4)\}$.
Show that

1. $f(\{s, t, u, z\}) = \{8, 4\}$
2. $f(\{s, x, z\}) = \{4\}$
3. $f(\{s, v, w, y\}) = \{1, 2, 4, 6\}$
4. $f^{-1}(\{4\}) = \{s, x, z\}$
5. $f^{-1}(\{4, 9\}) = \{s, x, z\}$.
6. $f^{-1}(\{9\}) = \Phi$
7. $f^{-1}(\{1, 4, 8\}) = \{s, t, u, v, x, z\}$

Theorem: Let $f : A \to B$. Let $W, X \subseteq A$ and $Y, Z \subseteq B$. Show that

1. $f(W \cap X) = f(W) \cap f(X)$
2. $f(W \cup X) = f(W) \cup f(X)$
3. $f^{-1}(Y \cap Z) = f^{-1}(Y) \cap f^{-1}(Z)$
4. $f^{-1}(Y \cup Z) = f^{-1}(Y) \cup f^{-1}(Z)$
5. $X \subseteq f^{-1}(f(X))$
6. $Y \subseteq f(f^{-1}(Y))$

Exercises

1. Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined as $f(x) = x^2 + 3$. Find $f([-3, 5])$ and $f^{-1}([12, 19])$.
   Ans: $f([-3, 5]) = [3, 28]$, $f^{-1}([12, 19]) = [-4, -3] \cup [3, 4]$

2. Consider the function $f : \{1, 2, 3, 4, 5, 6, 7\} \to \{0, 1, 23, 4\}$. How many such functions have the property that $|f^{-1}(\{3\})| = 3$?
   Ans: $4^4 \binom{7}{3}$

3. Problem from the text (Section 5.6).
   (a) Example 5.63 (page 285)
   (b) (page 288) 3, 9(a), 13, 17

Pigeonhole Principle
Section 5.4

Homework #7

Date due: April 2, 2014

The pigeonhole principle (PHP)

- If m pigeons occupy n pigeonholes, and m > n, then at least one pigeonhole has two or more pigeons roosting in it.
- The PHP is a powerful tool to solve combinatorial problems.
- The next slide discusses the main theorem and its proof. We will list a host of problems, categorized into two parts.
- Part A problems are for your practice.
- The homework questions are listed in Part B section.

Generalized pigeonhole principle

- If m objects are placed into n boxes, then there is at least one box containing $\lceil m/n \rceil$ objects
  - Proof by contradiction. Suppose each box contains less than $\lceil m/n \rceil$ objects, and there are m objects in total in n boxes. In this case the total number of objects n boxes can hold is at most $(\lceil m/n \rceil -1)*n$ which is less than $(((m/n)+1)-1)*n$, since $\lceil x \rceil < x+1$ always. This implies that there are less than m pigeons in n boxes. This is a contradiction.

Examples

- Given 9 integers whose prime factors lie in {2, 3, 7}, prove that there must be two whose product is a square.
  - All such integers can be expressed as $2^a3^b7^c$
  - Let two such integers be $2^a3^b7^c$ and $2^{a'}3^{b'}7^{c'}$
  - Their product is a square implies a+a', b+b' and c+c' are even.
  - Each exponent is either odd or even. Therefore, there are $2^3 = 8$ different ways the three exponents of a number may appear. These triplets are (even,even,even), (odd, odd,odd), (even,even,odd) ....
  - Each triplet is considered a group (bag).
  - If we select 9 integers, we get nine triplets. Two of these triplets must be in the same bag (Pigeonhole principle).
  - The corresponding two integers when multiplied will result in a perfect square.

Examples

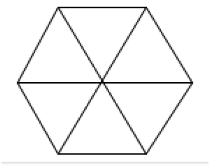
- How many times must we roll a single die in order to get the same score (a) at least twice? (b) at least thrice? (c) at least n times?
  - – A die has six sides. We need to throw 7 times to get the same score twice; need to throw 13 times to get the same score thrice; need to throw 6 (n-1) + 1, n > 0.

Examples

- During the first 6 weeks of his senior year in college, Brace sends out at least one resume each day, but no more than 60 resumes in total. Show that there is a period of consecutive days during which he sends out exactly 23 resumes.
  - Let x_i, i=1, 2, ..., 42 denote the number of resumes Brace has sent out from the start of his senior year to the end of the i-th day. Then $1 \leq x_1 < x_2 < .... < x_{42} \leq 60$. We can write $1 + 23 \leq x_1 + 23 < x_2 + 23 < .... < x_{42} + 23 \leq 60 + 23$. Thus we have 42 distict numbers x_1, x_2, ..., x_{42} and 42 distinct numbers x_1+23, x_2+23, ..., $x_{42}+23$. These 84 numbers can take values from 1 and 83 (inclusive).
  - By the pigeonhole principle, at least two of them must be equal.
  - We can then conclude that there exist i and j, $1 \leq j < i \leq 42$ such that $x_i = x_j + 23$, i.e. $x_i – x_j = 23$. Hence, from the start of day j+1 to the end of day i, Brace will send exactly 23 resumes.

PART A

1. Let S ⊂ Z$^+$, where |S|=12. Then S contains two elements that have the same remainder upon division by 11. (Discussed in the class)
2. Example 5.45 of the text is discussed in the class.
3. 19 darts are thrown onto a dartboard which is shaped as a regular hexagon with side length of 1 unit. Show that there are 4 darts within distance (√3)/3.



4. Show that among 200 people, there are at least 17 people who are born on the same month
5. How many students in a class must there be to ensure that 10 students get the same grade (one of A, B, C, D, F, or N)?

PART A (contd.)

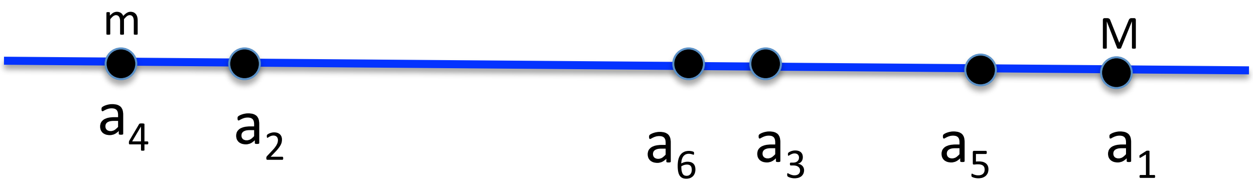
6. Suppose that there are 50 people in the room. Some of them are acquainted with each other, while some are not. Assume that each person has at least one acquaintance. Show that there are two persons in the room who have equal number of acquaintances.

   (Hints: Each individual can have acquaintances in the range [1 .. 49]. Why?)

7. Problem from the text:
   - **Section 5.5:** 4, 5(a), 7(a), 8(a), (b), 10, 14, 20
   - **Supplementary problem:** 14, 24

PART A (contd.)

7. Consider n distinct numbers $a_1, a_2, \ldots, a_m$. Let m = min $\{a_1, a_2, \ldots, a_n\}$ and M = max $\{a_1, a_2, \ldots, a_n\}$. We define the gap of of two elements a_i and a_j to be $|a_i – a_j|$ if there does not exist any other element a_k with $a_i < a_k < a_j$, otherwise it is 0. Show that there exist two elements in $\{a_1, a_2, \ldots, a_n\}$ whose gap is at least (M-m)/(n+1).



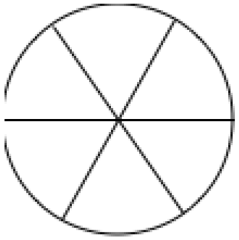
The gap between a_2 and a_6 is the largest; the gap between a_4 and a_6 is zero, since a_2 lies in between a_4 and a_6.

(Hint: Partition the interval [m .. M] into n+1 small sub-intervals, each of length (M-m)/(n+1).)

Discussed in the class.

PART B

1. Seven darts are thrown onto a circular dartboard of radius 10 units. Show that there will be two darts which are at most 10 units apart.



2. 6 computers on a network are connected to at least 1 other computer. Show there are at least two computers that have the same number of connections

PART B (contd.)

3. Consider 5 distinct points (x_i, y_i) with integer values, where i = 1, 2, 3, 4, 5. Show that the midpoint of at least one pair of these five points also has integer coordinates.
   - (Hints: We are looking for the midpoint of a segment from (a,b) to (c,d). The midpoint is ((a+c)/2, (b+d)/2). Note that the midpoint will be integers if a and c have the same parity: are either both even or both odd. The same is true for b and d.)
4. Suppose 49 points are placed, in a random way, into a square of side 1 unit. Prove that 4 of these points can be covered by a circle of radius ½. (Hints: The square should create 16 holes.)
5. Given m positive integers a_1, a_2, …, a_m, show that there exists k and l with 0 ≤ k <l ≤ m such that $a_{k+1} + a_{k+2} + \dots + a_l$ is divisible by m.

Relations

Sections 7.1,7.2,7.3,7.4

Relations

- Let A_1, A_2, … , A_n be sets. An n-ary relation on these sets (in this order) is a subset of $A_1 \times A_2 \times \ldots \times A_n$.
- Most of the time we consider n = 2 in which case have a binary relation and also say the the relation is "from A_1 to A_2".
- With this terminology, all functions are relations, but not vice versa.

Relations

- binary relations R defined on a set A
- R $\subseteq$ A x A : n = 2
- R $\subseteq$ **R** x **R : ** real plane
- R $\subseteq$ **R**$^{+}$ x **R**$^{+}$**:** Interior of the first quadrant
- (a,b) ε R is an element of R.
  - In the text infix notation aRb is also used.

Relations as Subsets

Question : Suppose we have relations on {1,2} given by R = {(1,1), (2,2)}, S = {(1,1),(1,2)}. Find:

- The union $R \cup S$
- The intersection $R \cap S$
- The symmetric difference $R \oplus S$
- The difference R-S
- The complement of R

Relations as Subsets

Answer: (R = {(1,1),(2,2)}, S = {(1,1),(1,2)})

- $R \cup S$ = {(1,1),(1,2),(2,2)}
- $R \cap S$ = {(1,1)}
- $R \oplus S$ = {(1,2),(2,2)}.
- R-S = {(2,2)}.
- $\overline{R}$ = {(1,2),(2,1)}

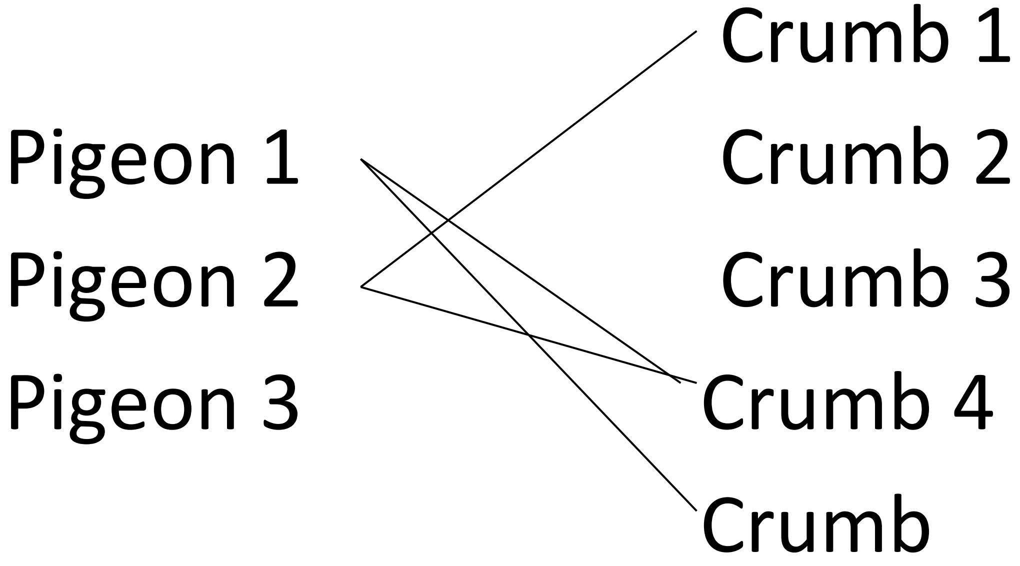
Composing Relations

- If R is a relation from A to B, and S is a relation from B to C then the ***composite*** of R and S is the relation $R \bullet S$ (or just SR) from A to C defined by setting (a,c) ε ($R \bullet S$) if and only if there is some b such that (a,b) ε R and (b,c) ε S.
- Notation is weird because generalizing functional composition: $f \bullet g\ (x) = f\ (g\ (x))$.

Representing Binary Relations -(0-1) Boolean Matrices

- Represent binary relations using (0,1)Boolean matrices, i.e. 2 dimensional tables consisting of 0's and 1's.
- For a relation R from A to B define matrix M_R by:
  - Rows –one for each element of A
  - Columns –one for each element of B
  - Value at i th row and j th column is
  - 1 if i th element of A is related to j th element of B
  - 0 otherwise

Representing Binary Relations -Boolean Matrices



Pigeon 1

Pigeon 2

Pigeon 3

Crumb 1

Crumb 2

Crumb 3

Crumb 4

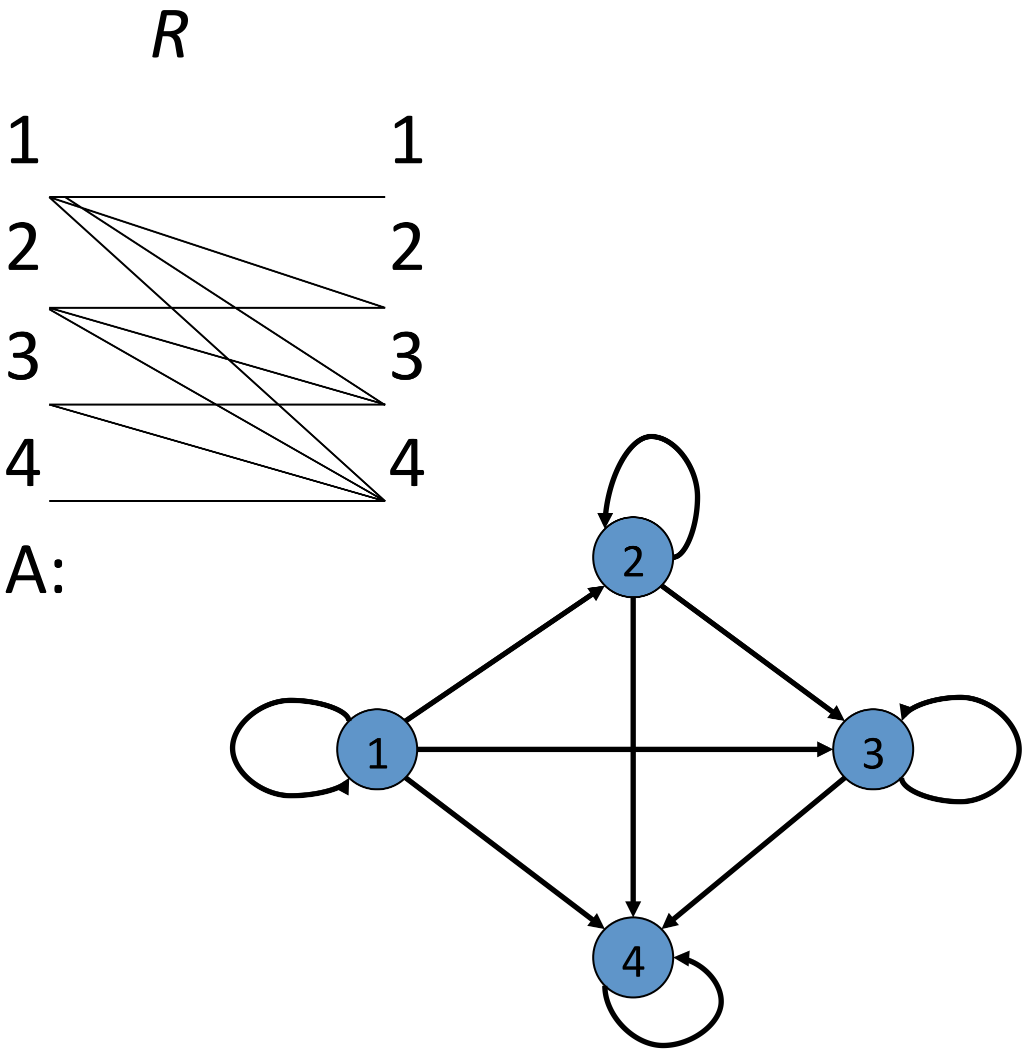
Crumb

M(R)= $\begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$

Digraph Representation

The another way of representing a relation R on a set A is with a **digraph** which stands for “**di**rected **graph**”. The set A is represented by **nodes** (or **vertices**) and whenever (a,b) ε R occurs, a **directed edge** (or **arrow**) a→b is created. Self pointing edges (or **loops**) are used to represent (a,a) ε R.

Digraph Representation



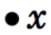
A:

Properties of Binary Relations

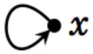
- Let R be a binary relation on A (i.e. R ⊆ A x A)
  - R is reflexive if for all a ε A, (a,a) ε R.
  - R is symmetric if (a,b) ε R, (b,a) ε R.
  - R is transitive if (a,b) ε R, (b,c) ε R, then (a,c) ε R.
  - R is antisymmetric if (a,b) ε R and (b,a) ε R, a = b.
- A relation R defined on A is an equivalence relation if R is reflexive, symmetric and transitive.
- A relation R is a partial order on A if R is reflexive, antisymmetric and transitive.

Spotting various properties of a relation from its diagram

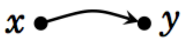
1. A relation is **reflexive** if for each point x ...



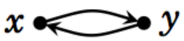
...there is a loop at x:



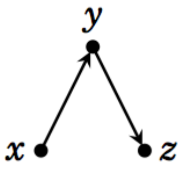
2. A relation is **symmetric** if whenever there is an arrow from x to y ...



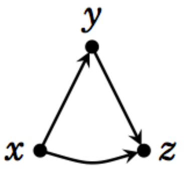
...there is also an arrow from y back to x:



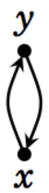
3. A relation is **transitive** if whenever there are arrows from x to y and y to z ...



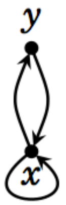
...there is also an arrow from x to z:



(If $x = z$, this means that if there are arrows from x to y and from y to x ...



...there is also a loop from x back to x.)



Properties of Binary Relations

Let R be a relation on $\mathbb{Z}^+$. The following table summarizes the properties of R when $R \in \{<, \leq, =, |, not(|), \neq\}$

Relation on $\mathbb{Z}^+$	$<$	$<=$	$=$	$\vert$	$not(\vert)$	$\neq$
reflexive	N	Y	Y	Y	N	N
symmetric	N	N	Y	N	N	Y
transitive	Y	Y	Y	Y	N	N

Visualizing the Properties

For relations R on a set A.

Q: What does M_R look like when when R is reflexive?

Visualizing the Properties

A: Reflexive. Upper-Left corner to Lower-Right corner diagonal is all 1's. EG:

$$M_R = \begin{pmatrix} 1 & * & * & * \\ * & 1 & * & * \\ * & * & 1 & * \\ * & * & * & 1 \end{pmatrix}$$

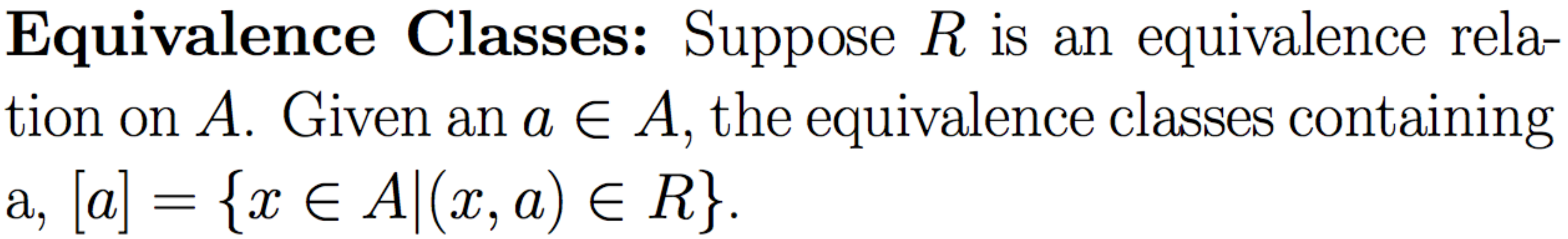
Q: How about if *R* is symmetric?

Visualizing the Properties

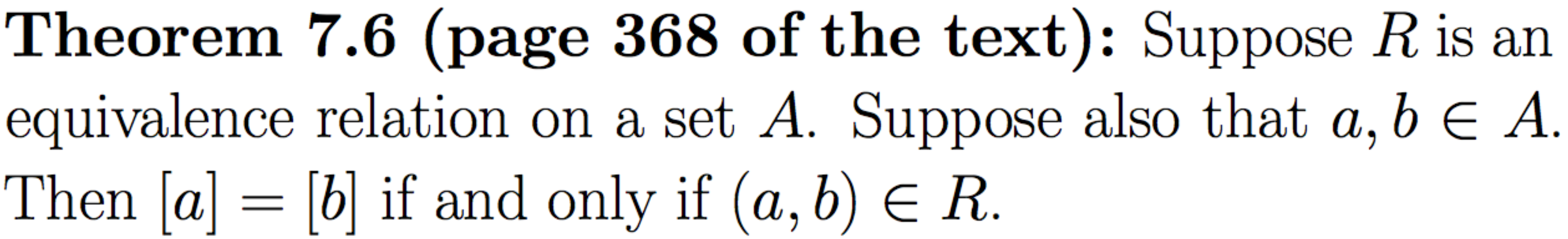
A: A ***symmetric matrix***. i.e., flipping across diagonal does not change matrix. EG:

$$M_R = \begin{pmatrix} * & 0 & 1 & 1 \\ 0 & * & 0 & 0 \\ 1 & 0 & * & 1 \\ 1 & 0 & 1 & * \end{pmatrix}$$

Equivalence classes and partition



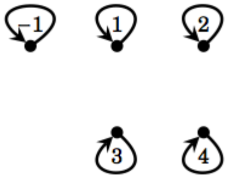
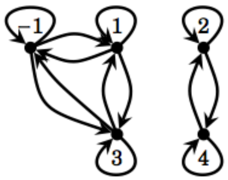
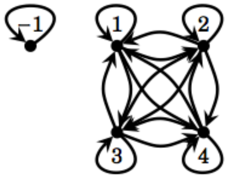
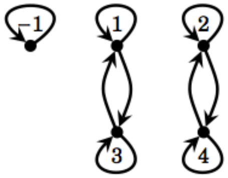
Equivalence Classes: Suppose R is an equivalence relation on A. Given an $a \in A$, the equivalence classes containing a, $[a] = \{x \in A | (x, a) \in R\}$.



Theorem 7.6 (page 368 of the text): Suppose R is an equivalence relation on a set A. Suppose also that $a, b \in A$. Then $[a] = [b]$ if and only if $(a, b) \in R$.

Equivalence classes and partition

R is defined on A = {-1, 1, 2, 3, 4}

Relation R	Diagram	Equivalence classes (see next page)
"is equal to" (=) $R_1 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4)\}$		$\{-1\}$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$
"has same parity as" $R_2 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4), (-1,1),(1,-1),(-1,3),(3,-1), (1,3),(3,1),(2,4),(4,2)\}$		$\{-1,1,3\}$, $\{2,4\}$
"has same sign as" $R_3 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4), (1,2),(2,1),(1,3),(3,1),(1,4),(4,1), (2,3),(3,2),(2,4),(4,2),(1,3),(3,1)\}$		$\{-1\}$, $\{1,2,3,4\}$
"has same parity and sign as" $R_4 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4), (1,3),(3,1),(2,4),(4,2)\}$		$\{-1\}$, $\{1,3\}$, $\{2,4\}$

Partition of a Set

- Given a set A, a collection $\{A_1, A_2, ..., A_k\}$ of non-empty, pair-wise disjoint subsets of A is a partition of A if the union of sets $A_1, A_2, ..., A_k$ is A.
  - Z = set of integers; Z_{even} = set of even integers

    Z_{odd} = set of odd integers.

  Clearly, $\{Z_{even}, Z_{odd}\}$ is a partition of Z.

- Theorem 7.7 (text page 369): If A is a set, then
  - any equivalence relation R on A partitions A into disjoint subsets $\{[a]: a \varepsilon A\}$.
  - Any partition of A gives rise to an equivalence relation R on A.

Partition of a Set

- Example: Consider R= ‘mod 3’ relation on the set of integers Z. We have shown in the class that R is an equivalence relation. The equivalence classes give the following partition of Z:

  {{…,-3,0,3,6,9, …},{…,-2,1,4,7,…},{…, -1,2,5,8, …}}

- We can write more compactly as {[0], [1], [2]}.

Partial Orders : Hasse Diagrams

Definition: Let R be a binary relation on a nonempty set A. R is a partial ordering if R is a reflexive, antisymmetric and transitive relation.

Example: If X is a set, then $\subseteq$ relation (R) on X is a partial ordering on the subsets of X $(\mathbb{P}(X))$.

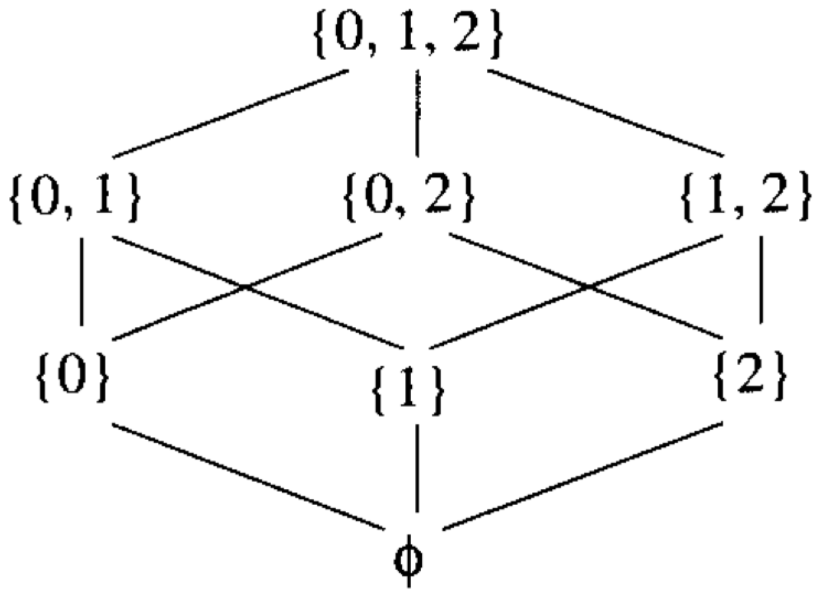
Proof: Let A, B be two arbitrary elements of $\mathbb{P}(X)$. Then R is

- reflexive: since A is a subset of itself, i.e. $A \subseteq A$.
- antisymmetric: since $A \subseteq B$ and $B \subseteq A$ implies $A = B$.
- is transitive: easy to see

Thus $(\mathbb{P}(X), \subseteq)$ is a poset.

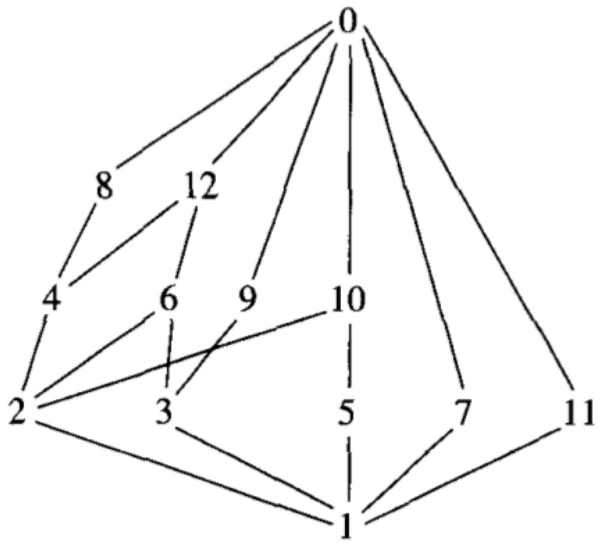
Partial Orders : Hasse Diagrams

- The Hasse diagram of the poset, (P(X), ⊆), is shown below where X = {0,1,2}. In Hasse diagram, x is drawn below y if (x,y) ε R; all the reflexive and transitive arcs are not included; the direction of the arcs are ignored (knowing that arcs are always pointed upwards).



Partial Orders : Hasse Diagrams

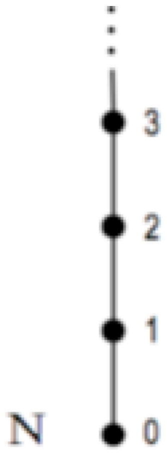
- The Hasse diagram of the poset ({0,1,2,3, …, 11,12}, ‘|’) below shows how the elements of the set are related.



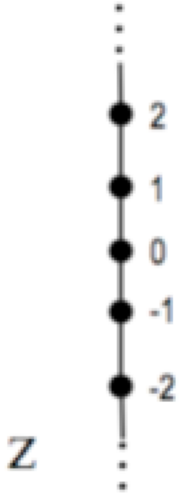
- A path from 1 to 0, say, <1,3,6,12,0> indicates that the elements on the path are related, i.e. for any a, b on the path, either (a,b) ε R or (b,a) ε R. Here R is the relation ‘|’.
- If a and b lie on two different paths (say 8 and 12), neither (a,b) nor (b,a) is in R.

Partial Orders : Hasse Diagrams

- Consider the posets (N, <=) and (Z,<=). Note that for any two elements a and b of N or Z, either (a <=b) or (b<= a). Therefore, elements a and b are related. The Hasse diagram of these posets looks like



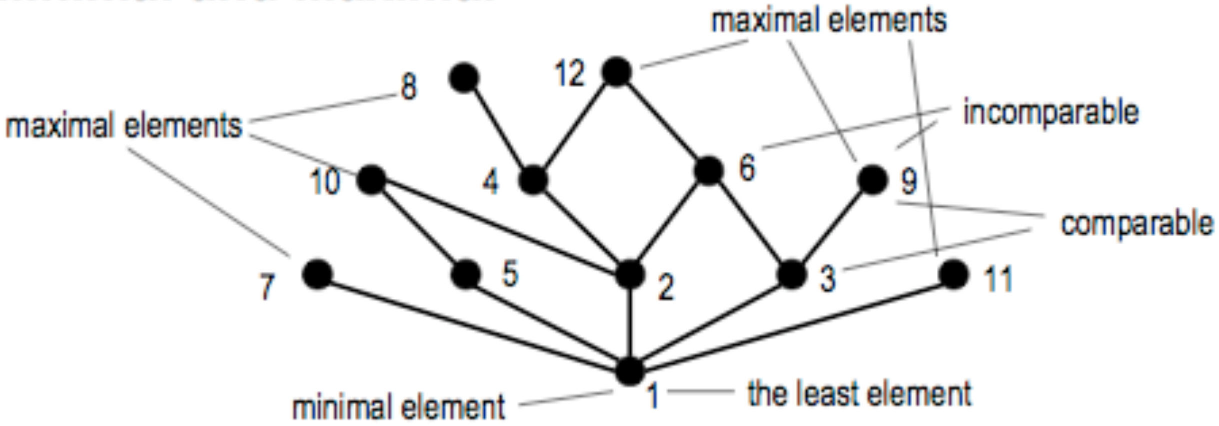
poset(N,<=)



poset(Z,<=)

- These posets realize total order of the elements of N and Z.

Minimal and Maximal



- Elements a,b are said to be comparable if (a,b) ∈ R or (b,a) ∈ R
- Otherwise they are called incomparable
- Element a is minimal if for any b if (b,a) ∈ R then a = b
- Element a is maximal if for any b if (a,b) ∈ R then a = b
- Element a is called the least element if for any b, (a,b) ∈ R
- Element a is called the greatest element if for any b, (b,a) ∈ R

Number Theory

Section 4.3, 4.4, 4.5

Importance of Number Theory

- Before the dawn of computers, many viewed number theory as last bastion of “pure math” which could not be useful and must be enjoyed only for its aesthetic beauty.
- Number theory is crucial for encryption algorithms.

Divisors

- Let a, b and c be integers such that $a = b \cdot c$.
  - b and c are **factors** of a, while a is said to be a **multiple** of b (as well as of c).
  - The pipe symbol "|" denotes "divides" so the situation is summarized by:

$$b \mid a \ \wedge \ c \mid a \, .$$

Divisors. Examples

- 77 | 7: false bigger number can’t divide smaller positive number
- 7 | 77: true because 77 = 7 · 11
- 24 | 24: true because 24 = 24 · 1
- 0 | 24: false, only 0 is divisible by 0
- 24 | 0: true, 0 is divisible by every number (0 = 24 · 0)
- **Question:** How many positive multiples of 15 are less than 100?

Divisor Theorem

Theorem: Let *a, b,* and *c* be integers. Then:

- $a|b \wedge a|c \rightarrow a|(b+c)$
- $a|b \rightarrow a|bc$
- $a|b \wedge b|c \rightarrow a|c$
- Let x = y + z for some integers x, y and z.
  - If a divides two of the three integers, a divides the third integer.
- If $a|b \wedge b|c \rightarrow a \mid sb + tc$ for all integers s and t.
  - sb + tc is known as the linear combination of a and b

Prime Numbers

- Definition: A number n ≥ 2 **prime** if it is only divisible by 1 and itself.
- A number n ≥ 2 which isn't prime is called **composite**.
- Question: Which of the following are prime?

  0,1,2,3,4,5,6,7,8,9,10

  – Note that 0 and 1 are not prime.

Fundamental Theorem of Arithmetic

Theorem:

Any number $n > 1$ is expressible as a unique product of 1 or more prime numbers.

Primality testing

- Prime numbers are very important in encryption. Essential to be able to verify if a number is prime or not.
- Testing if n is a prime.
  - Consider all integers greater than 1 and less than n to see if nis a composite.
  - Don't try number bigger than $\sqrt{n}$
  - After trying 2, don't try any other even numbers.
  - In general try only smaller prime numbers.

Division

- Theorem: Let a be an integer, and b be a positive integer. There are unique integers q, r with $r \in \{0,1,2,\ldots,b\text{-}1\}$ satisfying

$$a = qb + r$$

- a is called the **dividend**; q is called the **quotient** and r is called the **remainder**.
- The theorem is called the ***division algorithm***.

Greatest Common Divisor Relatively Prime

- Definition: Let *a*,*b* be integers, not both zero. The ***greatest common divisor*** of *a* and *b* (or gcd(*a*,*b*)) is the biggest number *d* which divides both *a* and *b*.
- Equivalently: gcd(*a*,*b*) is smallest number which divisibly by any *x* dividing both *a* and *b*.
- Definition: *a* and *b* are said to be ***relatively prime*** if gcd(*a*,*b*) = 1, so no prime common divisors.

Greatest Common Divisor

Question: Find the following gcd' s

- gcd(11,77)
- gcd(33,77)
- gcd(24,36)
- gcd(24,25)
- gcd(12,0)
- gcd(77,33)

Greatest Common Divisor

Theorem: For all $a, b \in \mathbb{Z}^+$, there exists a unique $c \in \mathbb{Z}^+$ that is the greatest common divisor of a and b.

Proof: Theorem 4.6 of the text (page 231).

Lemma: Let $a, b \in \mathbb{Z}^+$ where $a = qb + r$ where q and r are integers, and $0 \leq r < b$. Show that $gcd(a, b) = gcd(b, r)$.

Proof

- Let $d|a$ and $d|b$. Then $d|(a - bq)$. Therefore, $d|r$. Thus any divisor of a and b is also a divisor of r.

- Let $d|b$ and $d|r$. Thus $d|(bq + r)$. Therefore, $d|a$. Thus any divisor of b and r is also a divisor of a.

Therefore, $gcd(a, b) = gcd(b, r)$.

Greatest Common Divisor Algorithm

- Let a and b be positive integers with $a \geq b$. Set $r_0 = a$ and $r_1 = b$ Successively apply the division algorithm until the remainder is 0

$$\begin{array}{ll} r_0 = r_1 q_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 = r_2 q_2 + r_3 & 0 \leq r_3 < r_2 \\ \vdots & \\ r_{k-2} = r_{k-1} q_{k-1} + r_k & 0 \leq r_k < r_{k-1} \\ r_{k-1} = r_k q_k & \end{array}$$

- Eventually, the remainder is zero, because the sequence of remainders $a = r_0 > r_1 > r_2 > \ldots \geq 0$ cannot contain more than a elements.
- Furthermore, $\gcd(a,b) = \gcd(r_0, r_1) = \cdots = \gcd(r_{k-2}, r_{k-1})$

$$= \gcd(r_{k-1}, r_k) = \gcd(r_k, 0) = r_k$$

- Hence $\gcd(a,b)$ is the last nonzero remainder in the sequence

Greatest Common Divisor Relatively Prime

- ***Pairwise relatively prime***: the numbers a, b, c, d, … are said to be pairwise relatively prime if any two distinct numbers in the list are relatively prime.
- Q: Find a maximal pairwise relatively prime subset of

$$\{ 44, 28, 21, 15, 169, 17 \}$$

  - {17, 169, 28, 15} is one answer.
  - {17, 169, 44, 15} is another answer.