SYDDANSK UNIVERSITET

MM524 / DM527 Mathematical Tools (for Computer Science)

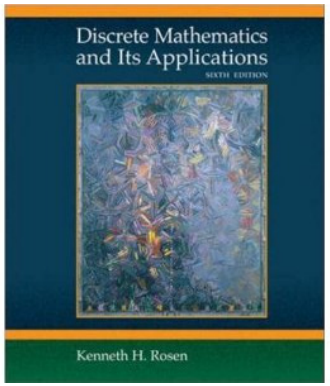
Fall 2010
Daniel Merkle

Instructor, TA, Office Hours

- Instructor
  - Daniel Merkle, daniel(at)imada.sdu.dk
- Teaching Assistants
  - Tikva Kathja Bøgh Fugløe, tifug09(at)student.sdu.dk
  - Christian Kudahl, kudahl(at)gmail.com
  - Magnus Find, magnus(at)gausdalfind.dk
- Hours
  - Lecture: Tuesdays 8-10, Thursday 10-12
  - Discussion sections: see online

Textbook

- Discrete Mathematics and Its Applications,
  - Rosen
  - 6th Edition
  - McGraw Hill
  - 2006



Overview

- Much of the basic mathematical machinery useful in computer science / mathematics will be presented, with applications.
- Students will learn actively the art of creating real-world proofs in these areas,
  - preparing them for diverse regions of computer science / mathematics such as cryptography, algorithmics, automata, programming languages, …, and
  - increasing their general problem-solving abilities in all areas.

Why study Discrete Maths?

- Proof
  - Ability to understand and create mathematical argument
- Gateway to more advanced math/CS courses
  - Data structures, algorithms, automata theory, formal languages
  - Database, networks, operating system, security

Course content

- Ch. 1: Logic and Proofs
- Ch. 2: Sets, Functions, Sequences and Sums
- Ch. 3: Algorithms, the Integers, and Matrices
- Ch. 4: Induction and Recursion
- Ch. 8: Relations

Due dates and Submission

- Due dates for all assignments are strict.
- There will be three mandatory assignments.
- Count for 30% of the final grade.
- First mandatory assignment is available already. Deadline: Sept. 17th, 13:00

SYDDANSK UNIVERSITET

ch1.1
Propositional Logic

Teaser

- There are two doors. One door leads in the right direction, the other one leads in the wrong direction. There are two people standing in front of the doors. One always lies, and one always tells the truth. You don't know which one is the liar, and you don't know which door is the wrong door. What one question can you ask that will tell you which door you should take?

(from the movie "Labyrinth")

Propositions

- A proposition is a statement that can be either true or false
  - "Anders has an Apple laptop."
  - "Anders is a professor."
  - "3 = 2 + 1"
  - "3 = 2 + 2"
- Not propositions:
  - "Are you Bob?"
  - "x + y = 7"
  - "Read this carefully."

Propositional variables

- We use propositional variables to refer to propositions
  - Usually are lower case letters starting with p (i.e. *p, q, r, s*, etc.)
  - A propositional variable can have one of two values: true (T) or false (F)
- A proposition can be…
  - A single variable: p
  - An operation of multiple variables: $p \wedge (q \vee \neg r)$

Introduction to Logical Operators

- About a dozen logical operators
  - Similar to algebraic operators + * - /
- In the following examples,
  - p = "Today is Friday"
  - q = "Today is my birthday"

Logical operators: Not

- A "not" operation switches (negates) the truth value
- Symbol: ¬ or ~
- ¬p = "Today is not Friday"

p	¬p
T	F
F	T

Logical operators: And

- An "and" operation is true if both operands are true
- Symbol: ∧
  - It's like the 'A' in And
- p∧q = "Today is Friday and today is my birthday"

p	q	p∧q
T	T	T
T	F	F
F	T	F
F	F	F

Logical operators: Or

- An "or" operation is true if either operands are true
- Symbol: ∨
- p∨q = "Today is Friday or today is my birthday (or possibly both)"

p	q	p∨q
T	T	T
T	F	T
F	T	T
F	F	F

Logical operators: Exclusive Or

- An exclusive or operation is true if one of the operands are true, but false if both are true
- Symbol: ⊕
- Often called XOR
- p⊕q ≡ (p ∨ q) ∧ ¬(p ∧ q)
- p⊕q = "Today is Friday or today is my birthday, but not both"

p	q	p⊕q
T	T	F
T	F	T
F	T	T
F	F	F

Inclusive Or versus Exclusive Or

- Do these sentences mean inclusive or exclusive or?
  - Experience with C++ or Java is required
  - Lunch includes soup or salad
  - To enter the country, you need a passport or a driver's license

Logical operators: Conditional 1

- A conditional means "if p then q"
- Symbol: $\rightarrow$
- $p \rightarrow q$ = "If today is Friday, then today is my birthday"
- $p \rightarrow q = \neg p \vee q$

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

the antecedent/ hypothesis

the consequence/ conclusion

Logical operators: Conditional 2

- Let p = "I am elected" and q = "I will lower taxes"
- I state: $p \rightarrow q$ = "If I am elected, then I will lower taxes"
- Consider all possibilities
- Note that if p is false, then the conditional is true regardless of whether q is true or false

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Logical operators: Conditional 3

- Alternate ways of stating a conditional:
  - p implies q
  - If p, q
  - p only if q
  - p is sufficient for q
  - q if p
  - q whenever p
  - q is necessary for p
  - q unless $\neg p$

Logical operators: Conditional 4

				Conditional	Inverse	Converse	Contrapositive
p	q	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg p \rightarrow \neg q$	$q \rightarrow p$	$\neg q \rightarrow \neg p$
T	T	F	F	T	T	T	T
T	F	F	T	F	T	T	F
F	T	T	F	T	F	F	T
F	F	T	T	T	T	T	T

Logical operators: Bi-conditional 1

- A bi-conditional means "p if and only if q"
- Symbol: $\leftrightarrow$
- Alternatively, it means "(if p then q) and (if q then p)"
- Note that a bi-conditional has the opposite truth values of the exclusive or

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Logical operators: Bi-conditional 2

- Let p = "You take this class" and q = "You get a grade"
- Then $p \leftrightarrow q$ means "You take this class if and only if you get a grade"
- Alternatively, it means "If you take this class, then you get a grade and if you get a grade then you take (took) this class"

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Boolean operators summary

		not	not	and	or	xor	conditional	Bi-conditional
p	q	$\neg p$	$\neg q$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	F	F	T	T	F	T	T
T	F	F	T	F	T	T	F	F
F	T	T	F	F	T	T	T	F
F	F	T	T	F	F	F	T	T

- Learn what they mean, don't just memorize the table!

Precedence of operators

- Just as in algebra, operators have precedence
  - 4+3*2 = 4+(3*2), not (4+3)*2
- Precedence order (from highest to lowest):
  $\neg \wedge \vee \rightarrow \leftrightarrow$
  - The first three are the most important
- This means that $p \vee q \wedge \neg r \rightarrow s \leftrightarrow t$ yields: $(p \vee (q \wedge (\neg r)) \rightarrow s) \leftrightarrow (t)$
- Not is *always* performed before any other operation

Translating English Sentences

- Question 7 from Rosen, p. 17
  - p = "It is below freezing"
  - q = "It is snowing"

- It is below freezing and it is snowing $p \wedge q$
- It is below freezing but not snowing $p \wedge \neg q$
- It is not below freezing and it is not snowing $\neg p \wedge \neg q$
- It is either snowing or below freezing (or both) $p \vee q$
- If it is below freezing, it is also snowing $p \rightarrow q$
- It is either below freezing or it is snowing, but it is not snowing if it is below freezing $(p \vee q) \wedge (p \rightarrow \neg q)$
- That it is below freezing is necessary and sufficient for it to be snowing $p \leftrightarrow q$

Translation (related) Example 2

- A study showed that there is a positive correlation between "chance of being bitten by a snake" and "frequency of ice eating".
- Conclusions: (???)
  - If you eat more ice, then you will more often be bitten by a snake. ???
  - If you are bitten often by a snake, then you more frequently eat ice. ???
- Sleeping with one's shoes on is strongly correlated with waking up with a headache. Therefore, sleeping with one's shoes on causes headache.

- NO!
  Correlating data vs. cause and effect
  http://en.wikipedia.org/wiki/Correlation_does_not_imply_causation

Translation Example 3

- "I have neither given nor received help on this exam"
- Let p = "I have given help on this exam"
- Let q = "I have received help on this exam"

- $\neg p \wedge \neg q$

Translation Example 4

- You can access the Internet from campus only if you are a computer science major or you are not a freshman.
- $a \rightarrow (c \vee \neg f)$

Boolean Searches

(MM524 OR DM527) AND "merkle" AND "computer science"

- Note that Google requires you to capitalize Boolean operators
- Google defaults to AND; many others do not

Bit Operations

- Boolean values can be represented as 1 (true) and 0 (false)
- A bit string is a series of Boolean values. Length of the string is the number of bits.
  - 10110100 is eight Boolean values in one string
- We can then do operations on these Boolean strings
  - Each column is its own Boolean operation

$$\begin{array}{r} 01011010 \\ \oplus 10110100 \\ \hline 11101110 \end{array}$$

ch1.2
Propositional Equivalence

Tautology, Contradiction, Equivalence

- **Tautology**: a compound proposition that's always true
  - $p \vee \neg p$ will always be true
- **Contradiction**: a compound proposition that's always false
  - $p \wedge \neg p$ will always be false
- **Contingency**: neither a tatology nor a contradiction
- A logical equivalence means that the two sides always have the same truth values
  - Symbol is $\equiv$ or $\Leftrightarrow$ (we'll use $\equiv$)

Examples

- Identity law $p \wedge T \equiv p$

p	T	$p \wedge T$
T	T	T
F	T	F

- Commutative law $p \wedge q \equiv q \wedge p$

p	q	$p \wedge q$	$q \wedge p$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	F

Examples

- Associative law $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

p	q	r	$p \wedge q$	$(p \wedge q) \wedge r$	$q \wedge r$	$p \wedge (q \wedge r)$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	F	F	F
T	F	F	F	F	F	F
F	T	T	F	F	T	F
F	T	F	F	F	F	F
F	F	T	F	F	F	F
F	F	F	F	F	F	F

How to prove equivalence?

- Two methods:
  - Using truth tables
    - Not good for long formula
    - In this course, only allowed if specifically stated!
  - Using the logical equivalences
    - The preferred method
- $(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

Truth Table Solution

- $(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

p	q	r	p→r	q →r	(p→r)∨(q →r)	p∧q	(p∧q) →r
T	T	T	T	T	T	T	T
T	T	F	F	F	F	T	F
T	F	T	T	T	T	F	T
T	F	F	F	T	T	F	T
F	T	T	T	T	T	F	T
F	T	F	T	F	T	F	T
F	F	T	T	T	T	F	T
F	F	F	T	T	T	F	T

Logical Equivalences

$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity Laws	$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination Law	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent Laws	$\neg (p \wedge q) \equiv \neg p \vee \neg q$ $\neg (p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$\neg(\neg p) \equiv p$	Double negation law	$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative Laws	$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	Negation laws
$p \rightarrow q \equiv \neg p \vee q$	Definition of Implication	$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$	Definition of Biconditional

Proof using Logical Equivalence

$(p \rightarrow r) \vee (q \rightarrow r)$

$\equiv (\neg p \vee r) \vee (\neg q \vee r)$ Definition of implication

$\equiv \neg p \vee r \vee \neg q \vee r$ Associative

$\equiv \neg p \vee \neg q \vee r \vee r$ Commutative

$\equiv (\neg p \vee \neg q) \vee (r \vee r)$ Associative

$\equiv \neg (p \wedge q) \vee r$ De Morgan, Idempotent

$\equiv (p \wedge q) \rightarrow r$ Definition of implication

Example

- Show that $(p \wedge q) \rightarrow (p \vee q)$ is a Tautology. (Proof)

$(p \wedge q) \rightarrow (p \vee q)$

$\equiv \neg (p \wedge q) \vee (p \vee q)$ Def. of implication

$\equiv (\neg p \vee \neg q) \vee (p \vee q)$ De Morgan

$\equiv (\neg p \vee p) \vee (\neg q \vee q)$ Commutative, Associative

$\equiv T \vee T$ Negation

$\equiv T$ Identity

Example

- At a trial:
  - Bill says: "Sue is guilty and Fred is innocent."
  - Sue says: "If Bill is guilty, then so is Fred."
  - Fred says: "I am innocent, but at least one of the others is guilty."
- Let b = Bill is innocent, f = Fred is innocent, and s = Sue is innocent
- Statements are:
  - $\neg s \wedge f$
  - $\neg b \rightarrow \neg f$
  - $f \wedge (\neg b \vee \neg s)$
- Can all of their statements be true???

Example (cnt)

- $(\neg s \wedge f) \wedge (\neg b \rightarrow \neg f) \wedge (f \wedge (\neg b \vee \neg s)) \equiv T$
  $(\neg s \wedge f) \wedge (b \vee \neg f) \wedge (f \wedge (\neg b \vee \neg s))$
  $\equiv ((\neg s \wedge f) \wedge (f \wedge (\neg b \vee \neg s))) \wedge (b \vee \neg f)$
  $\equiv (\neg s \wedge f \wedge (\neg b \vee \neg s)) \wedge (b \vee \neg f)$
  $\equiv ((\neg s \wedge f \wedge \neg b) \vee (\neg s \wedge f)) \wedge (b \vee \neg f)$
  $\equiv (\neg s \wedge f) \wedge (b \vee \neg f)$
  $\equiv (\neg s \wedge f \wedge b) \vee (\neg s \wedge f \wedge \neg f)$
  $\equiv (\neg s \wedge f \wedge b) \vee F$
  $\equiv \neg s \wedge f \wedge b$
- So what is the conclusion?

Syddansk Universitet

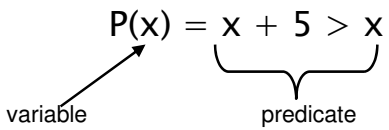
ch1.3
Predicates and Quantifiers

- How can we express
  - "every computer in CS department is protected by intrusion detection system"
  - "There exists at least one student who has a red hair".
- "x is greater than 3"
  - x: subject/variable
  - "is greater than 3": predicate
  - P(x): propositional function P at x

Propositional Functions

- Consider P(x) = x < 5
  - P(x) has no truth values (x is not given a value)
  - P(1) is true: The proposition 1<5 is true
  - P(10) is false: The proposition 10<5 is false
- P(x) will create a proposition when given a value
- Let P(x) = "x is a multiple of 5"
  - For what values of x is P(x) true?
- Let P(x) = (x + 3 == 0)
  - For what values of x is P(x) true?

Anatomy of a propositional function



Propositional functions 3

- Functions with multiple variables:
  - P(x,y) = x + y == 0
    - P(1,2) is false, P(1,-1) is true
  - P(x,y,z) = x + y == z
    - P(3,4,5) is false, P(1,2,3) is true
  - $P(x_1,x_2,x_3 \ldots x_n) = \ldots$

Quantifiers

- Why quantifiers?
  - Many things (in this course and beyond) are specified using quantifiers
    - In some cases, it's a more accurate way to describe things than Boolean propositions
- Quantification expresses the extend to which a predicate is true over a range of elements.
- Two types:
  - Universal
  - Existential

Universal quantifiers 1

- Represented by an upside-down A: ∀
  - It means "for all"
  - Let P(x) = x+1 > x
- We can state the following:
  - ∀x P(x)
  - English translation: "for all values of x, P(x) is true"
  - English translation: "for all values of x, x+1>x is true"

Universal quantifiers 2

- But is that always true?
  - ∀x P(x)
- Let x = the character 'a'
  - Is 'a'+1 > 'a'?
- Let x = the state of Minnesota
  - Is Minnesota+1 > Minnesota?
- You need to specify your universe!
  - What values x can represent
  - Called the "domain" or "universe of discourse"

Universal quantifiers 3

- Let the universe be the real numbers.
- Let P(x) = x/2 < x
  - Not true for the negative numbers!
  - Thus, ∀x P(x) is false
    - When the domain is all the real numbers
- In order to prove that a universal quantification is true, it must be shown for ALL cases
- In order to prove that a universal quantification is false, it must be shown to be false for only ONE case

Universal quantification 4

- Given some propositional function P(x)
- And values in the universe x_1 .. x_n
- The universal quantification ∀x P(x) is the same as the following conjunction:

$$P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n)$$

Existential quantification 1

- Represented by an backwards E: ∃
  - It means "there exists"
  - Let P(x) = x+1 > x
- We can state the following:
  - ∃x P(x)
  - English translation: "there exists (a value of) x such that P(x) is true"
  - English translation: "for at least one value of x, x+1>x is true"

Existential quantification 2

- Note that you still have to specify your universe
- Let P(x) = x+1 < x
  - Let the universe be all real numbers
  - There is no numerical value x for which x+1<x
  - Thus, ∃x P(x) is false

Existential quantification 3

- Let P(x) = x+1 > x
  - Let the universe be all real numbers
  - There is a numerical value for which x+1>x
  - In fact, it's true for all of the values of x!
  - Thus, ∃ x P(x) is true
- In order to show an existential quantification is true, you only have to find ONE value
- In order to show an existential quantification is false, you have to show it's false for ALL values

Existential quantification 4

- Given some propositional function P(x)
- And values in the universe x_1 .. x_n
- The existential quantification ∃x P(x) is equivalent to:

$$P(x_1) \vee P(x_2) \vee \ldots \vee P(x_n)$$

A note on quantifiers

- Recall that P(x) is a propositional function
  - Let P(x) be "x == 0"
- Recall that a proposition is a statement that is either true or false
  - P(x) is not a proposition
- There are two ways to make a propositional function into a proposition:
  - Supply it with a value
    - For example, P(5) is false, P(0) is true
  - Provide a quantification
    - For example, $\forall x$ P(x) is false and $\exists x$ P(x) is true
      - Let the universe of discourse be the real numbers

Binding variables

- Let P(x,y) be $x > y$
- Consider: $\forall x$ P(x,y)
  - This is not a proposition!
  - Universe: all real numbers.
  - What is y?
    - If it's 5, then $\forall x$ P(x,y) is false
- Note that y is not "bound" by a quantifier
- Scope of binding: the part of the logical expression to which a quantifier is applied
- Precedence of quantifiers: higher then all logical operatos

Binding variables 2

- $\exists x$ P(x) $\vee$ Q(x)
  - The x in Q(x) is not bound; thus not a proposition
- $\exists x$ P(x) $\vee \forall x$ Q(x)
  - Both x values are bound; thus it is a proposition
- $\exists x$ (P(x) $\wedge$ Q(x)) $\vee$ ($\forall y$ R(y))
  - All variables are bound; thus it is a proposition
- $\exists x$ (P(x) $\wedge$ Q(y)) $\vee$ ($\forall y$ R(y))
  - The y in Q(y) is not bound; this not a proposition

Negating quantifications

- Consider the statement:
  - All students in this class have red hair
- What is required to show the statement is false?
  - There exists a student in this class that does NOT have red hair
- To negate a universal quantification:
  - You negate the propositional function
  - AND you change to an existential quantification
  - $\neg\forall x$ P(x) = $\exists x \neg$P(x)

Negating quantifications 2

- Consider the statement:
  - There is a student in this class with red hair
- What is required to show the statement is false?
  - All students in this class do not have red hair
- Thus, to negate an existential quantification:
  - To negate the propositional function
  - AND you change to a universal quantification
  - $\neg\exists x\, P(x) = \forall x\, \neg P(x)$

TABLE 2 De Morgan's Laws for Quantifiers.

Negation	*Equivalent Statement*	*When Is Negation True?*	*When False?*
$\neg\exists x\, P(x)$	$\forall x \neg P(x)$	For every x, $P(x)$ is false.	There is an x for which $P(x)$ is true.
$\neg\forall x\, P(x)$	$\exists x \neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x.

Translating from English

- What about if the universe of discourse is all students (or all people?)
  - Every student in this class has studied calculus.
  - $\forall x\, (S(x) \wedge C(x))$
    - This is wrong! Why?
  - $\forall x\, (S(x) \rightarrow C(x))$

Translating from English 3

- Consider:
  - "Some students have visited Mexico"
  - "Every student in this class has visited Canada or Mexico"
- Let:
  - S(x) be "x is a student in this class"
  - M(x) be "x has visited Mexico"
  - C(x) be "x has visited Canada"

Translating from English 4

- Consider: "Some students have visited Mexico"
  - Rephrasing: "There exists a student who has visited Mexico"
- $\exists x\ M(x)$
  - True if the universe of discourse is all students
- What about if the universe of discourse is all people?
  - $\exists x\ (S(x) \rightarrow M(x))$
    - This is wrong! Why?
  - $\exists x\ (S(x) \wedge M(x))$

Translating from English 5

- Consider: "Every student in this class has visited Canada or Mexico"
- $\forall x\ (M(x) \vee C(x))$
  - When the universe of discourse is all students
- $\forall x\ (S(x) \rightarrow (M(x) \vee C(x))$
  - When the universe of discourse is all people

A Teaser: Logic Programming

- Prolog: PROgramming in LOGic
- **Prolog facts** define predicates by specifying elements that satisfy these predicates.
- **Prolog rules** define new predicates using already defined facts.
- http://www.csse.monash.edu.au/~lloyd/tildeLogic/Prolog.toy/Examples/Aunt/

SYDDANSK UNIVERSITET

ch1.4
Nested Quantifiers

Multiple quantifiers

- You can have multiple quantifiers on a statement
- $\forall x \exists y\ P(x, y)$
  - "For all x, there exists a y such that P(x,y)"
  - Example: $\forall x \exists y\ (x+y == 0)$
- $\exists x \forall y\ P(x,y)$
  - There exists an x such that for all y P(x,y) is true"
  - Example: $\exists x \forall y\ (x*y == 0)$

Order of quantifiers

- $\exists x \forall y\ P(x,y)$ and $\forall x \exists y\ P(x,y)$ are not equivalent!
- $\exists x \forall y\ P(x,y)$
  - $P(x,y) = (x+y == 0)$ is false (Note: Universe!)
- $\forall x \exists y\ P(x,y)$
  - $P(x,y) = (x+y == 0)$ is true (Again! Universe?)

Negating multiple quantifiers

- Recall negation rules for single quantifiers:
  - $\neg\forall x\ P(x) = \exists x\ \neg P(x)$
  - $\neg\exists x\ P(x) = \forall x\ \neg P(x)$
  - Essentially, you change the quantifier(s), and negate what it's quantifying
- Examples:
  - $\neg(\forall x \exists y\ P(x,y)) = \exists x\ \neg\exists y\ P(x,y) = \exists x \forall y\ \neg P(x,y)$
  - $\neg(\forall x \exists y \forall z\ P(x,y,z)) = \exists x \neg\exists y \forall z\ P(x,y,z)$
    $= \exists x \forall \neg y \forall z\ P(x,y,z) = \exists x \forall y \exists z\ \neg P(x,y,z)$

Negating multiple quantifiers 2

- Consider $\neg(\forall x \exists y\ P(x,y)) = \exists x \forall y\ \neg P(x,y)$
  - The left side is saying "for all x, there exists a y such that P is true"
  - To disprove it (negate it), you need to show that "there exists an x such that for all y, P is false"
- Consider $\neg(\exists x \forall y\ P(x,y)) = \forall x \exists y\ \neg P(x,y)$
  - The left side is saying "there exists an x such that for all y, P is true"
  - To disprove it (negate it), you need to show that "for all x, there exists a y such that P is false"

Translating between English and quantifiers

- The product of two negative integers is positive
  - $\forall x \forall y ((x<0) \wedge (y<0) \rightarrow (xy > 0))$
  - Why conditional instead of and?
- The average of two positive integers is positive
  - $\forall x \forall y ((x>0) \wedge (y>0) \rightarrow ((x+y)/2 > 0))$
- The difference of two negative integers is not necessarily negative
  - $\exists x \exists y ((x<0) \wedge (y<0) \wedge (x-y \geq 0))$
  - Why and instead of conditional?
- The absolute value of the sum of two integers does not exceed the sum of the absolute values of these integers
  - $\forall x \forall y (|x+y| \leq |x| + |y|)$

Translating between English and quantifiers

- $\exists x \forall y (x+y = y)$
  - There exists an additive identity for all real numbers
- $\forall x \forall y (((x \geq 0) \wedge (y<0)) \rightarrow (x-y > 0))$
  - A non-negative number minus a negative number is greater than zero
- $\exists x \exists y (((x \leq 0) \wedge (y \leq 0)) \wedge (x-y > 0))$
  - The difference between two non-positive numbers is not necessarily non-positive (i.e. can be positive)
- $\forall x \forall y (((x \neq 0) \wedge (y \neq 0)) \leftrightarrow (xy \neq 0))$
  - The product of two non-zero numbers is non-zero if and only if both factors are non-zero

Syddansk Universitet

ch1.5
Rules of Inference

Valid Arguments

- Assume you are given the following two statements:
  - "if you are in this class, you will get a grade"
  - "you are in this class"
  - Therefore,
  - "You will get a grade"

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore\ q \end{array}$$

Definitions

- An argument in propositional logic is a sequence of propositions.
- All but the final proposition are called premises.
- The final proposition is called conclusion.
- An argument is valid if the truth of all premises implies that the conclusion is true.
  - i.e. $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$ is a tautology.

Modus Ponens (Law of Detachment)

- Consider $(p \wedge (p \rightarrow q)) \rightarrow q$

p	q	p→q	p∧(p→q))	(p∧(p→q)) → q
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

$$\begin{array}{l} p \\ \underline{p \rightarrow q} \\ \therefore q \end{array}$$

Modus Ponens example

- Assume you are given the following two statements:
  - "you are in this class"
  - "if you are in this class, you will get a grade"
- Let p = "you are in this class"
- Let q = "you will get a grade"
- By Modus Ponens, you can conclude that you will get a grade

Another example

"If all integers are even, then the difference of any two integers is even".

"All integer are even".

Consequently,
" The difference of any two arbitrary integers is even".

Valid Arument?
Premises True?

Modus Tollens

- Assume that we know: $\neg q$ and $p \rightarrow q$
  - Recall that $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- Thus, if we know $\neg q$ and $(\neg q \rightarrow \neg p)$
- We can conclude $\neg p$

$$\begin{array}{l} \neg q \\ \underline{p \rightarrow q} \\ \therefore \neg p \end{array}$$

Modus Tollens example

- Assume you are given the following two statements:
  - "you will not get a grade"
  - "if you are in this class, you will get a grade"
- Let p = "you are in this class"
- Let q = "you will get a grade"
- By Modus Tollens, you can conclude that you are not in this class

Addition & Simplification

- Addition: If you know that p is true, then $p \vee q$ will ALWAYS be true

$$\begin{array}{l} \underline{p} \\ \therefore p \vee q \end{array}$$

- Simplification: If $p \wedge q$ is true, then p will ALWAYS be true

$$\begin{array}{l} \underline{p \wedge q} \\ \therefore p \end{array}$$

Example Proof

- We have the hypotheses:
  - "It is not sunny this afternoon and it is colder than yesterday" $(\neg p \wedge q)$
  - "We will go swimming only if it is sunny this afternoon" $(r \rightarrow p)$
  - "If we do not go swimming, then we will take a canoe trip" $(\neg r \rightarrow s)$
  - "If we take a canoe trip, then we will be home by sunset" $(s \rightarrow u)$
- Does this imply that "we will be home by sunset"? u
- $((\neg p \wedge q) \wedge (r \rightarrow p) \wedge (\neg r \rightarrow s) \wedge (s \rightarrow u)) \rightarrow u$???
  - When
    - p = "It is sunny this afternoon"
    - q = "it is colder than yesterday"
    - r = "We will go swimming"
    - s = "we will take a canoe trip"
    - u = "we will be home by sunset"

Example of proof

1.	$\neg p \wedge q$	1st hypothesis
2.	$\neg p$	Simplification using step 1
3.	$r \rightarrow p$	2nd hypothesis
4.	$\neg r$	Modus tollens using steps 2 & 3
5.	$\neg r \rightarrow s$	3rd hypothesis
6.	s	Modus ponens using steps 4 & 5
7.	$s \rightarrow u$	4th hypothesis
8.	u	Modus ponens using steps 6 & 7

More Rules of Inference

- **Conjunction**: if p and q are true separately, then $p \wedge q$ is true
- **Disjunctive syllogism**: If $p \vee q$ is true, and p is false, then q must be true
- **Resolution**: If $p \vee q$ is true, and $\neg p \vee r$ is true, then $q \vee r$ must be true
- **Hypothetical syllogism**: If $p \rightarrow q$ is true, and $q \rightarrow r$ is true, then $p \rightarrow r$ must be true

Summary: Rules of Inference

Modus ponens	p $p \rightarrow q$ $\therefore q$	Modus tollens	$\neg q$ $p \rightarrow q$ $\therefore \neg p$
Hypothetical syllogism	$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$	Disjunctive syllogism	$p \vee q$ $\neg p$ $\therefore q$
Addition	p $\therefore p \vee q$	Simplification	$p \wedge q$ $\therefore p$
Conjunction	p q $\therefore p \wedge q$	Resolution	$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$

Example Proof

- Example
  - "If it does not rain or if it is not foggy, then the sailing race will be held and the lifesaving demonstration will go on"
    - $(\neg r \vee \neg f) \rightarrow (s \wedge l)$
  - "If the sailing race is held, then the trophy will be awarded"
    - $s \rightarrow t$
  - "The trophy was not awarded"
    - $\neg t$
- Can you conclude: "It rained"?

Example of proof

1.	¬t	3rd hypothesis
2.	s → t	2nd hypothesis
3.	¬s	Modus tollens using steps 2 & 3
4.	(¬r∨¬f)→(s∧l)	1st hypothesis
5.	¬(s∧l)→¬(¬r∨¬f)	Contrapositive of step 4
6.	(¬s∨¬l)→(r∧f)	DeMorgan's law and double negation law
7.	¬s∨¬l	Addition from step 3
8.	r∧f	Modus ponens using steps 6 & 7
9.	r	Simplification using step 8

Rules of inference for the universal quantifier

- Assume that we know that ∀x P(x) is true
  - Then we can conclude that P(c) is true
    - Here c stands for some specific constant
  - This is called "**universal instantiation**"
- Assume that we know that P(c) is true for any value of c
  - Then we can conclude that ∀x P(x) is true
  - This is called "**universal generalization**"

Rules of inference for the existential quantifier

- Assume that we know that ∃x P(x) is true
  - Then we can conclude that P(c) is true for some value of c
  - This is called "**existential instantiation**"
- Assume that we know that P(c) is true for some value of c
  - Then we can conclude that ∃x P(x) is true
  - This is called "**existential generalization**"

Example of proof (ch1.5, 14a)

- Given the hypotheses:
  - "Linda, a student in this class, owns a red convertible."
  - "Everybody who owns a red convertible has gotten at least one speeding ticket"
- Can you conclude: "Somebody in this class has gotten a speeding ticket"?

C(Linda)
R(Linda)
∀x (R(x)→T(x))

∃x (C(x)∧T(x))

Example of proof

1.	$\forall x\ (R(x) \rightarrow T(x))$	3rd hypothesis
2.	$R(Linda) \rightarrow T(Linda)$	Universal instantiation using step 1
3.	$R(Linda)$	2nd hypothesis
4.	$T(Linda)$	Modes ponens using steps 2 & 3
5.	$C(Linda)$	1st hypothesis
6.	$C(Linda) \wedge T(Linda)$	Conjunction using steps 4 & 5
7.	$\exists x\ (C(x) \wedge T(x))$	Existential generalization using step 6

Thus, we have shown that "Somebody in this class has gotten a speeding ticket"

Example of proof (ch1.5, 14d)

- Given the hypotheses:
  - "There is someone in this class who has been to France"
  - "Everyone who goes to France visits the Louvre"
- Can you conclude: "Someone in this class has visited the Louvre"?

$\exists x\ (C(x) \wedge F(x))$
$\forall x\ (F(x) \rightarrow L(x))$

$\exists x\ (C(x) \wedge L(x))$

Example of proof

1.	$\exists x\ (C(x) \wedge F(x))$	1st hypothesis
2.	$C(y) \wedge F(y)$	Existential instantiation using step 1
3.	$F(y)$	Simplification using step 2
4.	$C(y)$	Simplification using step 2
5.	$\forall x\ (F(x) \rightarrow L(x))$	2nd hypothesis
6.	$F(y) \rightarrow L(y)$	Universal instantiation using step 5
7.	$L(y)$	Modus ponens using steps 3 & 6
8.	$C(y) \wedge L(y)$	Conjunction using steps 4 & 7
9.	$\exists x\ (C(x) \wedge L(x))$	Existential generalization using step 8

Thus, we have shown that "Someone in this class has visited the Louvre"

How do you know which one to use?

- Experience!

SYDDANSK UNIVERSITET

ch1.6
Introduction to Proofs
ch1.7
Proof Methods and Strategy

Proof methods

We will discuss ten proof methods:

1. Direct proofs
2. Indirect proofs
   - by Contraposition
   - by Contradiction
3. Vacuous proofs
4. Trivial proofs
5. Proof by cases
6. Proofs of equivalence
7. Existence proofs
8. Uniqueness proofs
9. Counterexamples

Terminology

- Theorem: a statement that can be shown true. Sometimes called facts.
  - Proposition: less important theorem
- Proof: Demonstration that a theorem is true.
- Axiom: A statement that is assumed to be true.
- Lemma: a less important theorem that is useful to prove a theorem.
- Corollary: a theorem that can be proven directly from a theorem that has been proved.
- Conjecture: a statement that is being proposed to be a true statement.

Formal Proofs vs. Informal Proofs

Direct proofs

- Consider an implication: $p \rightarrow q$
  - If p is false, then the implication is always true
  - Thus, show that if p is true, then q is true
- To perform a direct proof, assume that p is true, and show that q must therefore be true
- Show that the square of an even integer is an even integer
  - Rephrased: if n is even, then n^2 is even

(Proof) Assume n is even
Thus, $n = 2k$, for some k (definition of even numbers)
$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$
As n^2 is 2 times an integer, n^2 is thus even

Proof by Contraposition

- Consider an implication: $p \rightarrow q$
  - It's contrapositive is $\neg q \rightarrow \neg p$
    - Is logically equivalent to the original implication!
  - If the hypothesis ($\neg q$) is false, then the contrapositive is always true
  - Thus, show that if $\neg q$ is true, then $\neg p$ is true

- To perform an proof by contraposition, do a direct proof on the contrapositive

Proof by Contraposition Example

- If n^2 is an odd integer then n is an odd integer
- Prove the contrapositive: If n is an even integer, then n^2 is an even integer
- Proof:
  - Assume $n=2k$ for some integer k (definition of even numbers)
  - $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$
  - Since n^2 is 2 times an integer, it is even
- When do you use a direct proof versus an indirect proof?

Example of which to use

- Prove that if n^3+5 is an odd integer, then n is even
- Via direct proof
  - $n^3+5 = 2k+1$ for some integer k (definition of odd numbers)
  - $n^3 = 2k-4$
  - Umm… $n = \sqrt[3]{2k-4}$???
- So direct proof didn't work out. So: indirect proof
  - Contrapositive: If n is odd, then n^3+5 is even
  - Assume n is odd, and show that n^3+5 is even
  - $n=2k+1$ for some integer k (definition of odd numbers)
  - $n^3+5 = (2k+1)^3+5 = 8k^3+12k^2+6k+6 = 2(4k^3+6k^2+3k+3)$
  - As $2(4k^3+6k^2+3k+3)$ is 2 times an integer, it is even

Proof by Contradiction

- Given a statement p, assume it is false
  - Assume $\neg p$ is true
- Prove that $\neg p$ cannot occur as a contradiction exists.
- Formally show $\neg p \rightarrow (\neg r \wedge r)$ for some proposition r.
- As $(\neg r \wedge r)$ is false, we can conclude that $\neg p$ is false, i.e. p is true.

Pigeonhole Principle

The pigeonhole principle states that if n items are put into m pigeonholes with n > m, then at least one pigeonhole must contain more than one item.

Proof by contradiction example 1

- Show: **At least 4 of 22 different chosen days must fall on the same day of the week.**

Proof:

- Assume: ¬p is true, i.e., at most 3 days of any 22 different chosen days fall on the same day of the week.
- As there are only 7 days a week, maximally 21 days were chosen (because for each of the days of the week at most 3 of the chosen days could fall on that weekday)
- This contradicts that 22 days were chosen.

Q.E.D.

We showed:
¬p →("22 days are chosen" ∧"maximally 21 days were chosen")

Proof by contradiction example 2

- Theorem (by Euclid):
  There are infinitely many prime numbers.

- Proof. Assume there are a finite number of primes
- List them sorted as follows: $p_1, p_2 \ldots, p_n$.
- Consider the number $k = p_1 p_2 \ldots p_n + 1$
  - This number is not divisible by any of the listed primes (If we divided p_i into q, there would result a remainder of 1)
  - We must conclude that
    - k is either a prime number, or
    - k is divisible by a prime larger number than p_n
  - This contradicts our assumption that all primes are in the list $p_1, p_2 \ldots, p_n$.

We showed:
¬p → ("There is no prime larger than p_n." ∧ "There IS a prime larger than p_n.")

Proof by contradiction example 3

- Prove that if n is an integer and n^3+5 is odd, then n is even
- Rephrased: If n^3+5 is odd, then n is even

$p \equiv (q \rightarrow r)$

$\neg p \equiv \neg(q \rightarrow r)$
$\equiv \neg(\neg q \vee r)$
$\equiv q \wedge \neg r$

- Assume q is true and r is false, i.e.,
- assume that n^3+5 is odd, and n is odd
- $n=2k+1$ for some integer k (definition of odd numbers)
- $n^3+5 = (2k+1)^3+5 = 8k^3+12k^2+6k+6 = 2(4k^3+6k^2+3k+3)$
- As $2(4k^3+6k^2+3k+3)$ is 2 times an integer, n^3+5 must be even
- Contradiction!

We showed ¬p → ("n^3+5 is odd" ∧ "n^3+5 is even")

Vacuous and Trivial proofs

- Vacuous proof
  - Consider an implication: $p \rightarrow q$
  - If it can be shown that p is false, then the implication is always true (by the definition of implication)
- Trivial Proof
  - Consider an implication: $p \rightarrow q$
  - If it can be shown that q is true, then the implication is always true (by the definition of implication)

Vacuous proof example

- Consider the statement:
  All criminology majors in MM524 / DM527 are female.
- Rephrased:
  If you are a criminology major and you are in MM524 / DM527, then you are female.
- Proof:
  Since there are no criminology majors in this class, the hypothesis is false, and the implication is true!

Trivial proof example

- Consider the statement:
  If you are tall, then you are a student.
  (universe of discourse: all MM524 / DM527 students)
- Proof:
  Since all people in MM524 / DM527 are students, the implication is true regardless the hypothesis.

Exhaustive Proof /Proof by Cases

- Show a statement is true by showing all possible cases are true
- A statement of the form $(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$ is true iff $p_i \rightarrow q$ is true for all $i=1,2,\ldots,n$ individually

Reason:

$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \equiv [\ (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)\ ]$

- Make sure you get ALL the cases
  - The biggest mistake is to leave out some of the cases

Proof by cases example

- Prove that $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$ (b ≠ 0)

- Cases:
  - Case 1: a ≥ 0 and b > 0
    - Then |a| = a, |b| = b, and
  - Case 2: a ≥ 0 and b < 0
    - Then |a| = a, |b| = −b, and
  - Case 3: a < 0 and b > 0
    - Then |a| = −a, |b| = b, and
  - Case 4: a < 0 and b < 0
    - Then |a| = −a, |b| = −b, and

$$\left|\frac{a}{b}\right| = \frac{a}{b} = \frac{|a|}{|b|}$$

$$\left|\frac{a}{b}\right| = -\frac{a}{b} = \frac{a}{-b} = \frac{|a|}{|b|}$$

$$\left|\frac{a}{b}\right| = -\frac{a}{b} = \frac{-a}{b} = \frac{|a|}{|b|}$$

$$\left|\frac{a}{b}\right| = \frac{a}{b} = \frac{-a}{-b} = \frac{|a|}{|b|}$$

Proofs of equivalences

- This is showing the definition of a bi-conditional

- Given a statement of the form "p if and only if q"
  - Show it is true by showing (p→q)∧(q→p) is true

Proofs of equivalence example

- Show that $m^2=n^2$ if and only if m=n or m=−n
- Rephrased: $(m^2=n^2) \leftrightarrow [(m=n)\vee(m=-n)]$
  - $[(m=n)\vee(m=-n)] \rightarrow (m^2=n^2)$
    - Proof by cases!
    - Case 1: $(m=n) \rightarrow (m^2=n^2)$
      - $m^2 = (n)^2 = n^2$, so this case is proven
    - Case 2: $(m=-n) \rightarrow (m^2=n^2)$
      - $m^2 = (-n)^2 = n^2$, so this case is proven
  - $(m^2=n^2) \rightarrow [(m=n)\vee(m=-n)]$
    - Subtract n^2 from both sides to get $m^2-n^2=0$
    - Factor to get (m+n)(m−n) = 0
    - Since that equals zero, one of the factors must be zero
    - Thus, either m+n=0 (which means m=−n)
      or m−n=0 (which means m=n)

Existence proofs

- Given a statement: ∃x P(x)
- We only have to show that a P(c) exists for some value of c

- Two types:
  - Constructive: Find a specific value of c for which P(c) is true.
  - Nonconstructive: Show that such a c exists, but don't actually find it
    - Assume it does not exist, and show a contradiction

Constructive existence proof example

- Show that a square exists that is the sum of two other squares
  - Proof: $3^2 + 4^2 = 5^2$
- Show that a cube exists that is the sum of three other cubes
  - Proof: $3^3 + 4^3 + 5^3 = 6^3$

Non-constructive existence proof example

- Prove that either $2*10^{500}+15$ or $2*10^{500}+16$ is not a perfect square
  - A perfect square is a square of an integer
  - Rephrased: Show that a non-perfect square exists in the set $\{2*10^{500}+15, 2*10^{500}+16\}$
- Proof:
  - The only two perfect squares that differ by 1 are 0 and 1
  - Thus, any other numbers that differ by 1 cannot both be perfect squares
  - Thus, a non-perfect square must exist in any set that contains two numbers that differ by 1

  (Note that we didn't specify which one it was!)

Proof by Counterexample

- Every positive integer is the sum of two squares of integers. TRUE?
- Every positive integer is the sum of three squares of integers. TRUE?
- Every positive integer is the sum of four squares of integers. TRUE?

Uniqueness proofs

- A theorem may state that only one such value exists
- To prove this, you need to show:
  - Existence: that such a value does indeed exist
    - Either via a constructive or non-constructive existence proof
  - Uniqueness: that there is only one such value

Uniqueness proof example

- If a and b are real numbers and $a \neq 0$, the there is a unique real number r, such that $ar+b=0$
- Existence
  - $r=-b/a$ is a solution of $ar+b=0$. Consequently, a real number r exists for which $ar+b=0$
- Uniqueness
  - Suppose s is a real number such that $as+b=0$
  - Then $ar+b=as+b$, where $r=-b/a$
  - therefore, $ar=as$, and consequently
  - $s=r$
  - Thus, the one solution is unique!

Proof methods

- We discussed ten proof methods:
  1. Direct proofs
  2. Indirect proofs
     1. Proof by showing the Contrapositive
     2. Proof by Contradiction
  3. Vacuous proofs
  4. Trivial proofs
  5. Proof by cases
  6. Proofs of equivalence
  7. Existence proofs
  8. Uniqueness proofs
  9. Counterexamples

Syddansk Universitet

ch2.1 Sets

What is a set?

- A set is a unordered collection of "objects"
  - People in a class: {Alice, Bob, Chris }
  - States in the US: {Alabama, Alaska, Virginia, … }
  - Sets can contain non-related elements: {3, a, Virginia}
  - All positive numbers less than or equal to 5: {1, 2, 3, 4, 5}
- Properties
  - Order does not matter
    - {1, 2, 3, 4, 5} is equivalent to {3, 5, 2, 4, 1}
  - Sets do not have duplicate elements
    - Consider the list of students in this class
      - It does not make sense to list somebody twice

Specifying a set

- A set "contains" the various "members" or "elements" that make up the set
  - If an element a is a member of (or an element of) a set S, we use then notation $a \in S$
    - $4 \in \{1, 2, 3, 4\}$
  - If not, we use the notation $a \notin S$
    - $7 \notin \{1, 2, 3, 4\}$

Often used sets

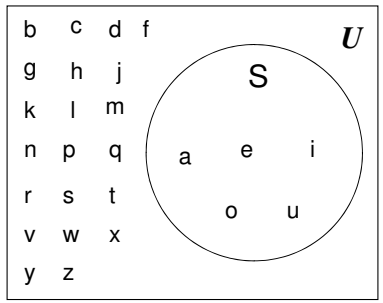
- **N** = {0, 1, 2, 3, …} is the set of natural numbers
- **Z** = {…, −2, −1, 0, 1, 2, …} is the set of integers
- $\mathbf{Z}^+$ = {1, 2, 3, …} is the set of positive integers (a.k.a whole numbers)
  - Note that people disagree on the exact definitions of whole numbers and natural numbers
- **Q** = $\{p/q \mid p \in \mathbf{Z}, q \in \mathbf{Z}, q \neq 0\}$ is the set of rational numbers
  - Any number that can be expressed as a fraction of two integers (where the bottom one is not zero)
- **R** is the set of real numbers

The universal set

- U is the **universal set** – the set of all of elements (or the "universe") from which given any set is drawn
  - For the set {−2, 0.4, 2}, U could be the real numbers
  - For the set {0, 1, 2}, U could be the **N**, **Z**, **Q**, **R** depending on the context
  - For the set of the vowels of the alphabet, U could be all the letters of the alphabet

Venn diagrams

- Represents sets graphically
  - The box represents the universal set
  - Circles represent the set(s)
- Consider set S, which is the set of all vowels in the alphabet
- The individual elements are usually not written in a Venn diagram



Sets of sets

- Sets can contain other sets
  - S = { {1}, {2}, {3} }
  - T = { {1}, {{2}}, {{{3}}} }
  - V = { {{1}, {{2}}}, {{{3}}}, { {1}, {{2}}, {{{3}}} } }
    - V has only 3 elements!
- Note that $1 \neq \{1\} \neq \{\{1\}\} \neq \{\{\{1\}\}\}$
  - They are all different

The Empty Set

- If a set has zero elements, it is called the empty (or null) set
  - Written using the symbol ∅
  - Thus, ∅ = { } ← IMPORTANT
- It can be a element of other sets
  - { ∅, 1, 2, {3}, x } is a valid set
- $\emptyset \neq \{ \emptyset \}$
  - The first is a set of zero elements
  - The second is a set of 1 element (namely the empty set)
- Replace ∅ by { }, and you get: { } ≠ {{ }}
  - It's easier to see that they are not equal that way

Set Equality, Subsets

- Two sets are equal if they have the same elements
  - {1, 2, 3, 4, 5} = {5, 4, 3, 2, 1}
  - {1, 2, 3, 2, 4, 3, 2, 1} = {4, 3, 2, 1}
  - Two sets are not equal if they do not have the same elements
    - {1, 2, 3, 4, 5} ≠ {1, 2, 3, 4}
- If all the elements of a set S are also elements of a set T, then S is a subset of T
  - If S = {2, 4, 6}, T = {1, 2, 3, 4, 5, 6, 7}, S is a subset of T
  - This is specified by $S \subseteq T$ meaning that $\forall x (x \in S \rightarrow x \in T)$
  - For any set S, $S \subseteq S$ ($\forall S \ \ S \subseteq S$)
  - For any set S, $\emptyset \subseteq S$ ($\forall S \ \ \emptyset \subseteq S$)

Proper Subsets

- If S is a subset of T, and S is not equal to T, then S is a proper subset of T
  - Can be written as: $S \subseteq T$ and $S \neq T$
  - Let T = {0, 1, 2, 3, 4, 5}
  - If S = {1, 2, 3}, S is a subset of T,and S is not equal to T
  - A proper subset is written as $S \subset T$
  - Let Q = {4, 5, 6}. Q is neither a subset or T nor a proper subset of T
  - $\forall x (x \in S \rightarrow x \in T) \wedge \exists x (x \in T \wedge x \notin S)$

Set cardinality

- The cardinality of a set is the number of elements in a set, written as |A|
- Examples
  - Let R = {1, 2, 3, 4, 5}. Then |R| = 5
  - |∅| = 0
  - Let S = {∅, {a}, {b}, {a, b}}. Then |S| = 4

Power Sets

- Given S = {0, 1}. All the possible subsets of S?
  - ∅ (as it is a subset of all sets), {0}, {1}, and {0, 1}
  - The power set of S (written as P(S), or $\wp(S)$) is the set of all the subsets of S
  - P(S) = { ∅, {0}, {1}, {0,1} }
    - Note that |S| = 2 and |P(S)| = 4
- Let T = {0, 1, 2}. The P(T) = { ∅, {0}, {1}, {2}, {0,1}, {0,2}, {1,2}, {0,1,2} }
  - Note that |T| = 3 and |P(T)| = 8
- P(∅) = { ∅ }
  - Note that |∅| = 0 and |P(∅)| = 1
- If a set has *n* elements, then the power set will have 2^n elements

- Cartesian product
- Set notation with quantifiers
- Truth set of quantifiers

SYDDANSK UNIVERSITET

2.2
Set Operations

Set operations: Union

- Formal definition for the union of two sets:
  $A \cup B = \{ x \mid x \in A \text{ or } x \in B \}$
- Examples
  - $\{1, 2, 3\} \cup \{3, 4, 5\} = \{1, 2, 3, 4, 5\}$
  - $\{a, b\} \cup \{3, 4\} = \{a, b, 3, 4\}$
  - $\{1, 2\} \cup \varnothing = \{1, 2\}$
- Properties of the union operation

$A \cup \varnothing = A$	Identity law
$A \cup \boldsymbol{U} = \boldsymbol{U}$	Domination law
$A \cup A = A$	Idempotent law
$A \cup B = B \cup A$	Commutative law
$A \cup (B \cup C) = (A \cup B) \cup C$	Associative law

Set operations: Intersection

- Formal definition for the intersection of two sets:
  $A \cap B = \{ x \mid x \in A \text{ and } x \in B \}$
- Examples
  - $\{1, 2, 3\} \cap \{3, 4, 5\} = \{3\}$
  - $\{a, b\} \cap \{3, 4\} = \varnothing$
  - $\{1, 2\} \cap \varnothing = \varnothing$
- Properties of the intersection operation

$A \cap \boldsymbol{U} = A$	Identity law
$A \cap \varnothing = \varnothing$	Domination law
$A \cap A = A$	Idempotent law
$A \cap B = B \cap A$	Commutative law
$A \cap (B \cap C) = (A \cap B) \cap C$	Associative law

Disjoint sets

- Formal definition for disjoint sets: two sets are **disjoint** if their intersection is the empty set
- Examples:
  - $\{1, 2, 3\}$ and $\{3, 4, 5\}$ are not disjoint
  - $\{a, b\}$ and $\{3, 4\}$ are disjoint
  - $\{1, 2\}$ and $\varnothing$ are disjoint
    - Their intersection is the empty set
  - $\varnothing$ and $\varnothing$ are disjoint!
    - Their intersection is the empty set

Set operations: Difference

- Formal definition for the **difference** of two sets:
  $A - B = \{ x \mid x \in A \wedge x \notin B \}$
- Examples:
  - $\{1, 2, 3\} - \{3, 4, 5\} = \{1, 2\}$
  - $\{a, b\} - \{3, 4\} = \{a, b\}$
  - $\{1, 2\} - \varnothing = \{1, 2\}$
  - The difference of any set S with the empty set will be the set S

Complement sets

- Formal definition for the **complement** of a set: $\overline{A} = \{ x \mid x \notin A \} = A^c$
  - Or U – A, where U is the universal set
- Further examples (assuming $U = Z$)
  - $\{1, 2, 3\}^c = \{ \ldots, -2, -1, 0, 4, 5, 6, \ldots \}$
- Properties of complement sets
  - $(A^c)^c = A$ Complementation law
  - $A \cup A^c = U$ Complement law
  - $A \cap A^c = \varnothing$ Complement law

Set Identities

$A\cup\varnothing = A$ $A\cap U = A$	Identity Law	$A\cup U = U$ $A\cap\varnothing = \varnothing$	Domination law
$A\cup A = A$ $A\cap A = A$	Idempotent Law	$(A^c)^c = A$	Complement Law
$A\cup B = B\cup A$ $A\cap B = B\cap A$	Commutative Law	$(A\cup B)^c = A^c\cap B^c$ $(A\cap B)^c = A^c\cup B^c$	De Morgan's Law
$A\cup(B\cup C)$ $= (A\cup B)\cup C$ $A\cap(B\cap C)$ $= (A\cap B)\cap C$	Associative Law	$A\cap(B\cup C) =$ $(A\cap B)\cup(A\cap C)$ $A\cup(B\cap C) =$ $(A\cup B)\cap(A\cup C)$	Distributive Law
$A\cup(A\cap B) = A$ $A\cap(A\cup B) = A$	Absorption Law	$A \cup A^c = U$ $A \cap A^c = \varnothing$	Complement Law

How to prove a set identity

- For example: A∩B=A−(A−B)
- Four methods:
  - Use the basic set identities
  - Use membership tables
  - Prove each set is a subset of each other
  - Use set builder notation and logical equivalences

Proof by Set Identities

- $A \cap B = A - (A - B)$

Proof: $A - (A - B) = A - (A \cap B^c)$
$= A \cap (A \cap B^c)^c$
$= A \cap (A^c \cup B)$
$= (A \cap A^c) \cup (A \cap B)$
$= \varnothing \cup (A \cap B)$
$= A \cap B$

Showing each is a subset of the others

$(A \cap B)^c = A^c \cup B^c$
Proof:
Show that $(A \cap B)^c \subseteq A^c \cup B^c$ and $(A \cap B)^c \supseteq A^c \cup B^c$

$x \in (A \cap B)^c$
$\Rightarrow x \notin (A \cap B)$
$\Rightarrow \neg (x \in A \cap B)$
$\Rightarrow \neg (x \in A \wedge x \in B)$
$\Rightarrow \neg (x \in A) \vee \neg (x \in B)$
$\Rightarrow x \notin A \vee x \notin B$
$\Rightarrow x \in A^c \vee x \in B^c$
$\Rightarrow x \in A^c \cup B^c$

Still to be shown: $(A \cap B)^c \supseteq A^c \cup B^c$ (left as exercise)

Examples

- Let *A*, *B*, and *C* be sets. Show that:

a) $(A \cup B) \subseteq (A \cup B \cup C)$
b) $(A \cap B \cap C) \subseteq (A \cap B)$
c) $(A-B)-C \subseteq A-C$
d) $(A-C) \cap (C-B) = \varnothing$

Blackboard:

- Russels's Paradox (if time allows)
- Generalized union/intersection of collections of sets

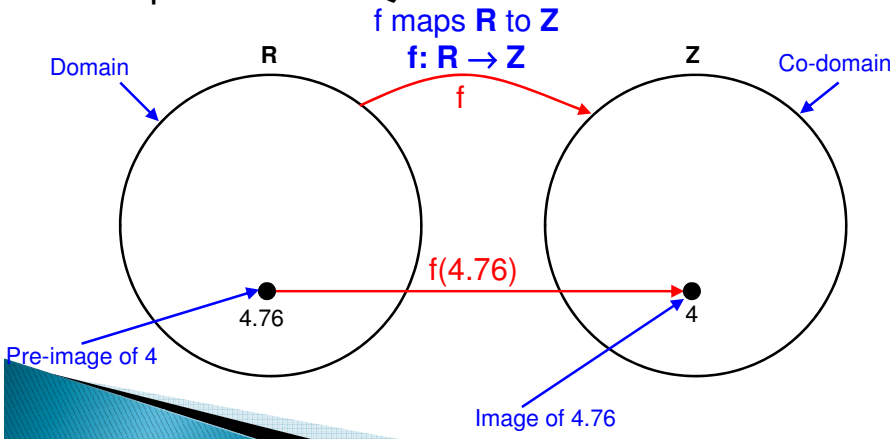
„ Einem wissenschaftlichen Schriftsteller kann kaum etwas Unerwünschteres begegnen, als daß ihm nach Vollendung einer Arbeit eine der Grundlagen seines Baues erschüttert wird. In diese Lage wurde ich durch einen Brief des Herrn Bertrand Russell versetzt, als der Druck dieses Bandes sich seinem Ende näherte." [Frege, 1903]

SYDDANSK UNIVERSITET

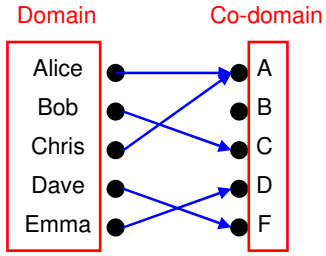
ch2.3 Functions

Definition of a function

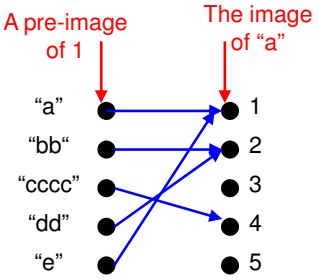
- A function takes an element from a set and maps it to a UNIQUE element in another set



More functions

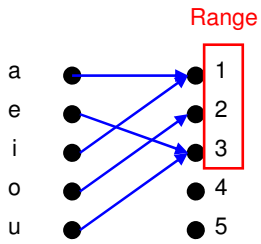


A class grade function

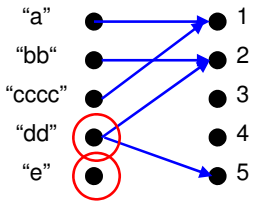


A string length function

Even more functions



Some function…



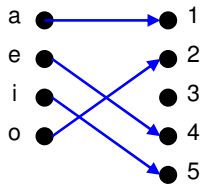
Not a valid function!
Also not a valid function!

Function arithmetic

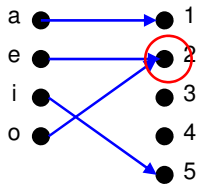
- Let $f_1(x) = 2x$
- Let $f_2(x) = x^2$
- $(f_1+f_2)(x) = f_1(x)+f_2(x) = 2x+x^2$
- $(f_1*f_2)(x) = f_1(x)*f_2(x) = 2x*x^2 = 2x^3$

Injective ("One-to-one") functions

- A function is **injective** (or "one-to-one") if each element in the co-domain has a unique pre-image



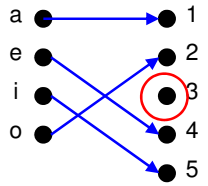
An injective function



A function that is not injective

More on injective functions

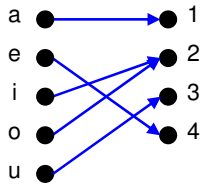
- A function is an injection if it is injective.
- Note that there can be un-used elements in the co-domain



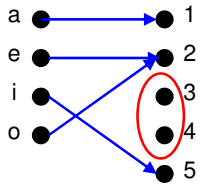
A one-to-one function

Surjective / ("Onto") functions

- A function is **surjective** if each element in the co-domain is an image of some pre-image



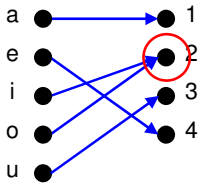
A surjective function



A function that is not surjective

More on "onto"

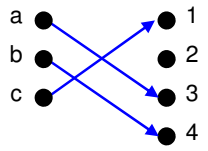
- A function is an surjection if it is surjective
- Note that there can be multiply used elements in the co-domain



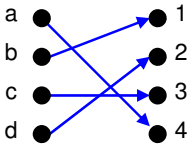
An onto function

Surjective, injective

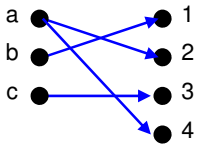
- Are the following functions surjective, injective, both, or neither?



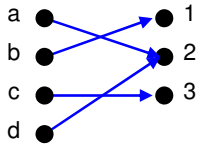
injective, not surjective



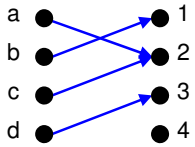
Both injective and surjective



Not a valid function



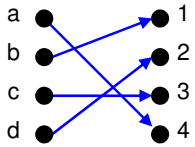
surjective, not injective



Neither injective nor surjective

Bijections

- Consider a function that is both injective and surjective:
- Such a function is a one-to-one correspondence, or a **bijection**

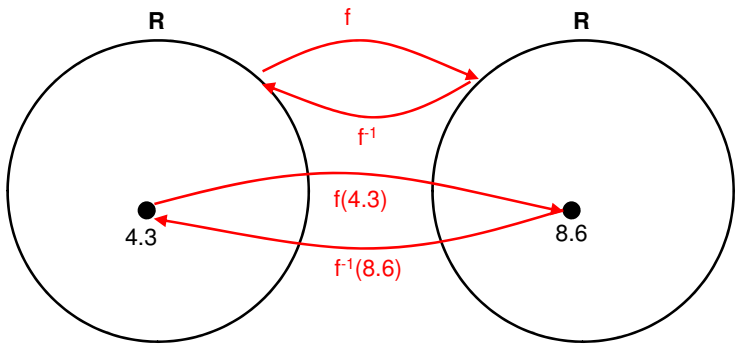


Identity functions

- A function such that the image and the pre-image are ALWAYS equal
- $f(x) = 1*x$
- $f(x) = x + 0$
- The domain and the co-domain must be the same set

Inverse functions

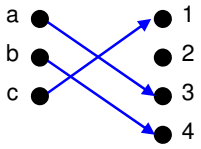
Let f(x) = 2*x



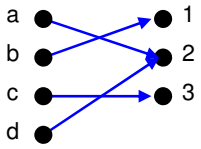
Then $f^{-1}(x) = x/2$

More on inverse functions

- Can we define the inverse of the following functions?



What is $f^{-1}(2)$?
Not surjective!



What is $f^{-1}(2)$?
Not injective!

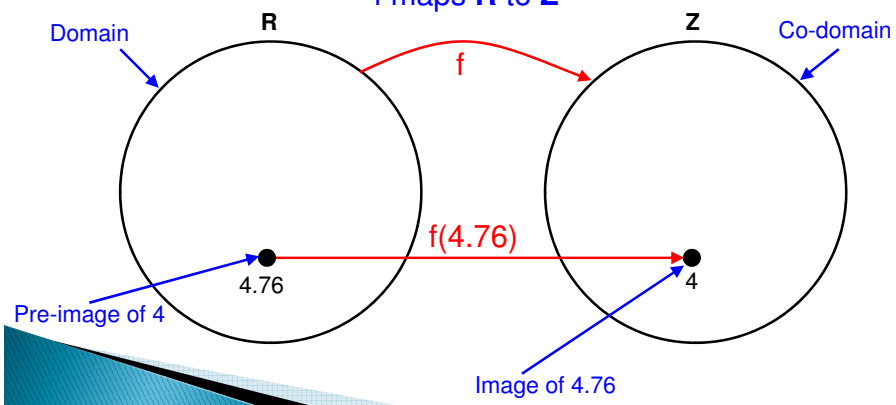
- An inverse function can ONLY be defined on a bijection

Few Examples

- f: $Z \rightarrow Z$
  - $f(x) = x$
  - $f(x) = 2x$
  - $f(x) = x+1$
- f: $R \rightarrow R$
  - $f(x) = 2x$
  - $f(x) = x^2$
  - $f(x) = x^3$
- f: $R \rightarrow R^+ \cup \{0\}$
  - $f(x) = x^2$

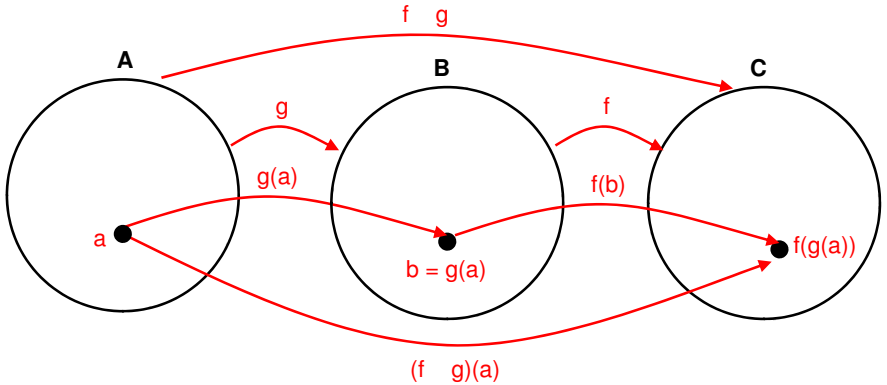
Definition of a function

- A function takes an element from a set and maps it to a UNIQUE element in another set



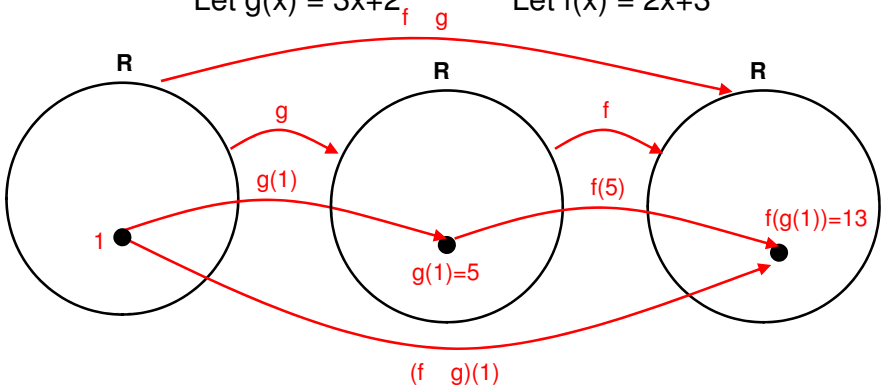
Compositions of functions

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



Compositions of functions

Let g(x) = 3x+2 Let f(x) = 2x+3



f(g(x)) = 2(3x+2)+3 = 6x+7

Compositions of functions

Does f(g(x)) = g(f(x))?

Let f(x) = 2x+3 Let g(x) = 3x+2

f(g(x)) = 2(3x+2)+3 = 6x+7
g(f(x)) = 3(2x+3)+2 = 6x+11

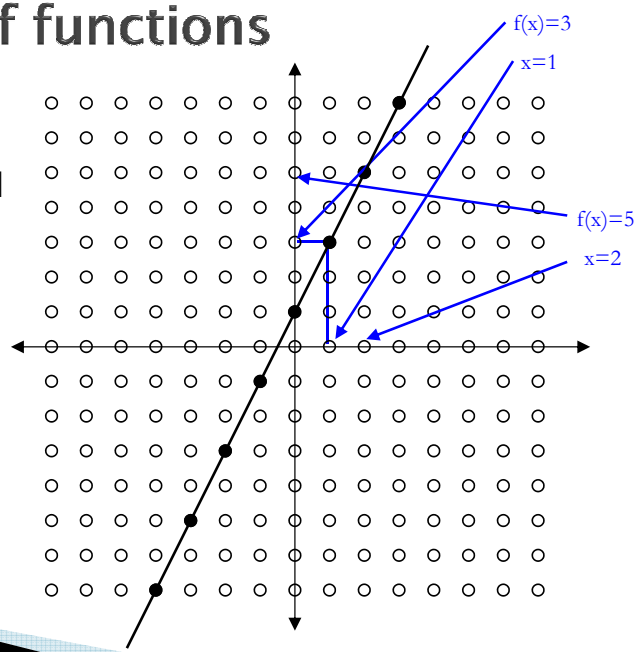
Not equal!

Function composition is not commutative!

Graphs of functions

Let f(x)=2x+1

Plot (x, f(x))



This is a plot of f(x)

Useful functions

- Floor: $\lfloor x \rfloor$ means take the greatest integer less than or equal to the number
- Ceiling: $\lceil x \rceil$ means take the lowest integer greater than or equal to the number
- round(x) = $\lfloor x+0.5 \rfloor$

Floor, Ceiling Examples

- Find these values

$\lfloor 1.1 \rfloor$	1
$\lceil 1.1 \rceil$	2
$\lfloor -0.1 \rfloor$	-1
$\lceil -0.1 \rceil$	0

Ceiling and floor properties

Let n be an integer

(1a) $\lfloor x \rfloor = n$ if and only if $n \le x < n+1$
(1b) $\lceil x \rceil = n$ if and only if $n-1 < x \le n$
(1c) $\lfloor x \rfloor = n$ if and only if $x-1 < n \le x$
(1d) $\lceil x \rceil = n$ if and only if $x \le n < x+1$
(2) $x-1 < \lfloor x \rfloor \le x \le \lceil x \rceil < x+1$
(3a) $\lfloor -x \rfloor = -\lceil x \rceil$
(3b) $\lceil -x \rceil = -\lfloor x \rfloor$
(4a) $\lfloor x+n \rfloor = \lfloor x \rfloor + n$
(4b) $\lceil x+n \rceil = \lceil x \rceil + n$

Ceiling property proof

- Prove rule 4a: $\lfloor x+n \rfloor = \lfloor x \rfloor + n$
  - Where n is an integer
  - Will use rule 1a: $\lfloor x \rfloor = n$ if and only if $n \le x < n+1$
- Direct proof!
  - Let $m = \lfloor x \rfloor$
  - Thus, $m \le x < m+1$ (by rule 1a)
  - Add n to both sides: $m+n \le x+n < m+n+1$
  - $m+n = \lfloor x+n \rfloor$ (by rule 1a)
  - Since $m = \lfloor x \rfloor$, $m+n$ also equals $\lfloor x \rfloor + n$
  - Thus, $\lfloor x \rfloor + n = m+n = \lfloor x+n \rfloor$

Factorial

- Factorial is denoted by n!
- n! = n * (n-1) * (n-2) * … * 2 * 1
- Thus, 6! = 6 * 5 * 4 * 3 * 2 * 1 = 720
- Note that 0! is defined to equal 1

Proving Function problems

- Let f be an invertible function from Y to Z
- Let g be an invertible function from X to Y
- Show that the inverse of f○g is:
  - $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$

Proof: We want to show, for all $x \in X$ (resp. for all $z \in Z$)
$((f \circ g) \circ (g^{-1} \circ f^{-1}))\ (x) = x$ (and $((f^{-1} \circ g^{-1}) \circ (g \circ f))\ (z) = z$)

$$\begin{aligned}((f \circ g) \circ (g^{-1} \circ f^{-1}))\ (x) &= (f \circ g)\ ((g^{-1} \circ f^{-1})\ (x)) \\ &= (f \circ g)\ (g^{-1}\ (f^{-1}(x))) \\ &= (f\ (g\ (g^{-1}\ (f^{-1}(x))))) \\ &= (f\ (f^{-1}(x)) \\ &= x\end{aligned}$$

The second equality can be shown similar.

SYDDANSK UNIVERSITET

ch2.4
Sequences and Summations

Definitions

- Sequence: an ordered list of elements
  - Similar to a set, but:
    - Elements can be duplicated
    - Elements are ordered
- A sequence is a function from a subset of **Z** to a set S
- a_n is a term of the sequence
- $\{a_n\}$ means the entire sequence
  - The same notation, but different meaning as for sets!

Sequence examples

- $a_n = 3n$
  - The terms in the sequence are a_1, a_2, a_3, …
  - The sequence $\{a_n\}$ is 3, 6, 9, 12, …
- **Arithmetic Progression**
  - $a, a+d, a+2d, \ldots, a+nd, \ldots$
  - $a_n = a + (n-1)\,d$

- $b_n = 2^n$
  - The terms in the sequence are b_1, b_2, b_3, …
  - The sequence $\{b_n\}$ is 2, 4, 8, 16, 32, …
- **Geometric Progression**
  - $a, ar, ar^2, ar^3, \ldots, ar^{n-1}, \ldots$
  - $a_n = ar^{n-1}$

Determining the sequence formula

- Given values in a sequence, how do you determine the formula?
- Steps to consider:
  - Is it an arithmetic progression?
  - Is it a geometric progression?
  - Does the sequence repeat (or cycle)?
  - Does the sequence combine previous terms?
  - Are there runs of the same value?

Determining the sequence formula

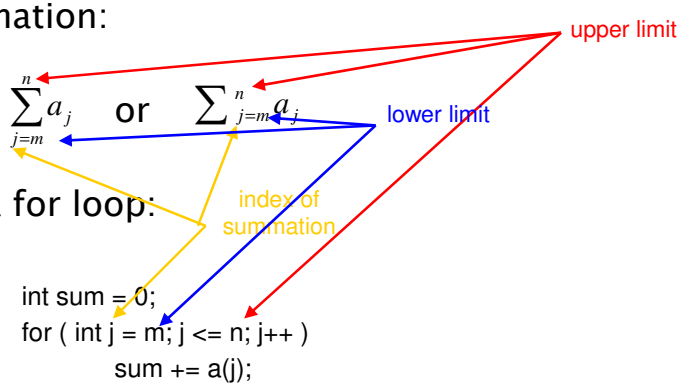
- 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, …
  - The sequence alternates 1's and 0's, increasing the number of 1's and 0's each time
- 1, 2, 2, 3, 4, 4, 5, 6, 6, 7, 8, 8, …
  - This sequence increases by one, but repeats all even numbers once
- 1, 0, 2, 0, 4, 0, 8, 0, 16, 0, …
  - The non-0 numbers are a geometric sequence (2^n) interspersed with zeros
- 3, 6, 12, 24, 48, 96, 192, …
  - Each term is twice the previous: geometric progression
  - $a_n = 3*2^{n-1}$

Determining the sequence formula

- 15, 8, 1, -6, -13, -20, -27, …
  - Each term is 7 less than the previous term
  - $a_n = 22 - 7n$
- 3, 5, 8, 12, 17, 23, 30, 38, 47, …
  - The difference between successive terms increases by one each time
  - $a_1 = 3$, $a_n = a_{n-1} + n$
  - $a_n = n(n+1)/2 + 2$
- 2, 16, 54, 128, 250, 432, 686, …
  - Each term is twice the cube of n
  - $a_n = 2*n^3$
- 2, 3, 7, 25, 121, 721, 5041, 40321
  - Each successive term is about n times the previous
  - $a_n = n! + 1$

Summations

- A summation:



- is like a for loop:

Evaluating Summations

- $\Sigma^{5}_{k=1}\ (k+1) = 2 + 3 + 4 + 5 + 6 = 20$
- $\Sigma^{4}_{k=0}\ (-2)^k = (-2)^0 + (-2)^1 + (-2)^2 + (-2)^3 + (-2)^4 = 11$
- $\Sigma^{10}_{k=1}\ 3 = 3 + 3 + 3 + 3 + 3 + 3 + 3 + 3 + 3 + 3 = 30$
- $\Sigma^{10}_{k=1}\ (2^k - 2^{k-1}) = (2^1-2^0) + (2^2-2^1) + (2^3-2^2) + \ldots (2^{10}-2^9) = 511$
  - Note that each term (except the first and last) is cancelled by another term

Summation

- $1 + 2 + 3 + \ldots + n = n(n+1)/2$
- $1 + 2 + 3 + \ldots + (n-1) = ?$
- $1 + 3 + 5 + \ldots + 21 = ?$
- $a_i = a_1 + (i-1)\,d$
- $\sum_{i=1}^{n} a_i = ?$

Summation of a geometric series

- Sum of a geometric series:

$$\sum_{j=0}^{n} ar^j = \begin{cases} \frac{ar^{n+1}-a}{r-1} & \text{if } r \neq 1 \\ (n+1)a & \text{if } r = 1 \end{cases}$$

Proof

- If $r = 1$, then the sum is:

$$\boxed{S = \sum_{j=0}^{n} a = (n+1)a}$$

$$\begin{aligned} S &= \sum_{j=0}^{n} ar^j \\ rS &= r\sum_{j=0}^{n} ar^j \\ &= \sum_{j=0}^{n} ar^{j+1} \\ &= \sum_{k=1}^{n+1} ar^k \\ &= \sum_{k=0}^{n} ar^k + \left(ar^{n+1} - a\right) \\ rS &= S + \left(ar^{n+1} - a\right) \\ rS - S &= \left(ar^{n+1} - a\right) \\ S(r-1) &= \left(ar^{n+1} - a\right) \\ S &= \frac{\left(ar^{n+1} - a\right)}{r-1} \end{aligned}$$

Double summations

- Like a nested for loop

$$\sum_{i=1}^{4}\sum_{j=1}^{3} ij$$

- Is equivalent to:

```
int sum = 0;
for ( int i = 1; i <= 4; i++ )
        for ( int j = 1; j <= 3; j++ )
                sum += i*j;
```


Cardinality

- For finite (only) sets, cardinality is the number of elements in the set
- For finite and infinite sets, two sets *A* and *B* have the same cardinality if there is a bijection (one-to-one correspondence) from *A* to *B*
- An infinite set S that is **countable** has the cardinality "aleph null" ($|S| = \aleph_0$)

Cardinality

- Example on finite sets:
  - Let $S = \{ 1, 2, 3, 4, 5 \}$
  - Let $T = \{ a, b, c, d, e \}$
  - There is a bijection between the sets
- Example on infinite sets:
  - Let $S = \mathbf{Z}^+$
  - Let $T = \{ x \mid x = 2k \text{ and } k \in \mathbf{Z}^+ \}$
  - Bijection:

    $1 \leftrightarrow 2$ $\quad 2 \leftrightarrow 4$ $\quad 3 \leftrightarrow 6$ $\quad 4 \leftrightarrow 2$

    $5 \leftrightarrow 10$ $\quad 6 \leftrightarrow 12$ $\quad 7 \leftrightarrow 14$ $\quad 8 \leftrightarrow 16$

    Etc.
    - Note that here the '↔' symbol means that there is a correspondence between them, not the biconditional

More definitions

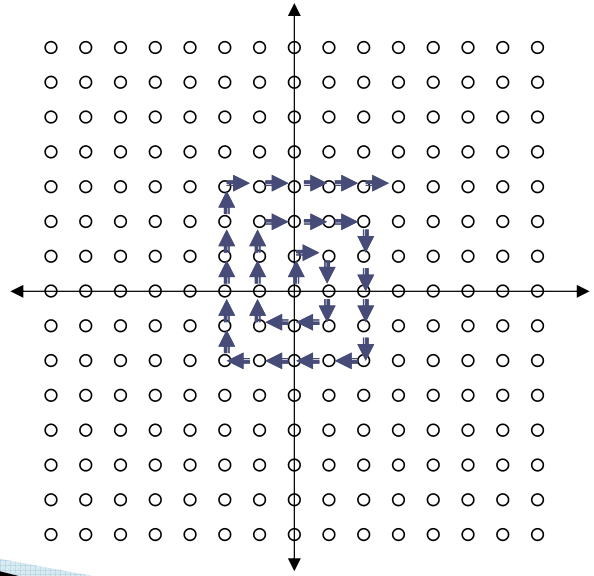
- Countably infinite: elements can be listed
  - Anything that has the same cardinality as the integers
  - Example: rational numbers, ordered pairs of integers
- Uncountably infinite: elements cannot be listed
  - Example: real numbers

Showing a set is countably infinite

- Done by showing there is a one-to-one correspondence (bijection) between the set and the integers
- Examples
  - Even numbers
    - Shown two slides ago
  - Rational numbers
    - Shown in Rosen, page 159
  - Ordered pairs of integers
    - Shown next slide

Ordered pairs of integers: countably infinite

A bijection



Cantor Diagonilization

- The set of real number is uncountable (-> blackboard: Proof by contradiction)

SYDDANSK UNIVERSITET

ch 3.4
Integers and Division

Division

- Def: **a (a≠0) divides b if ∃ c such that b = ac.**
  - a | b: a divides b
- 3 | 7? 3 | 12?
- 3 | 0? 0 | 3?

- Theorem: Let a, b, c be integers. Then
  - a | b and a | c ⇒ a | (b + c).
  - a | b ⇒ a | bc for all integer c.
  - a | b and b | c ⇒ a | c.

Division

- Let a, b, c be integers. Then
  - a | b and a | c ⇒ a | (b + c).

Division

- Let a, b, c be integers. Then
  - a | b ⇒ a | bc ∀ integer c.

Division

- Let a, b, c be integers. Then
  - a | b, b | c ⇒ a | c.

Division

- a | b and a | c $\Rightarrow$ a | (mb + nc) for all integer m, n.

Division "Algorithm"

- *Theorem*: Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$.

- Definition
  - q = a **div** d, quotient
  - r = a **mod** d, remainder

- $101 = 7 \cdot 14 + 3$
- $-11 = 7 \cdot (-2) + 3$

Modular Arithmetic

- Definiton:
  If a and b are integers, and m is a positive integer, then

  "a is **congruent** to b modulo m"

  if m divides (a−b).

  We use the notation $a \equiv b \pmod{m}$.

Modular Arithmetic

- Theorem:
  Let m be a positive integer.
  $a \equiv b \pmod{m}$ iff $\exists$ k such that $a = b + km$.

More…

- Theorem:
  Let m be a positive integer.
  If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then
  - $a + c \equiv b + d \pmod m$, and
  - $ac \equiv bd \pmod m$.

More…

- Prove or Disprove
  - If $ac \equiv bc \pmod m$, where $a, b, c, m \in \mathbf{Z}$ (with $m \geq 2$), then $a \equiv b \pmod m$.
  - $a, b, c, d, m \in \mathbf{Z}$, $c, d > 0$, $m \geq 2$, then $a^c \equiv b^d \pmod m$.
    - $a = 2, b = 5, c = 4, d = 1, m = 3$

Cryptology

"Caesar cipher"

- Alphabet to number: a~0, b~1, … , z~25.
- Encryption: $E_K(x) = (x + K)$ **mod** 26.
- Decryption: $D_K(x) = (x - K)$ **mod** 26.

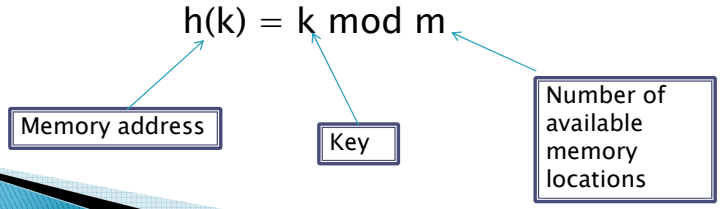
- Caesar used K = 3.

"RSA Cryptosystem"

Further Applications

- Pseudorandom numbers:
  Linear congruential method $x_{n+1} = (ax_n + c) \mod m$
  Example: a=7, c=4, x_0=3, m=9
  3,7,8,6,1,2,0,4,5,3,7,8,6…

- Hashing Functions:



SYDDANSK UNIVERSITET

ch 3.5
Primes and GCD

Prime numbers

- Def: A positive integer p is prime if the only positive factors of p are 1 and p
  - If there are other factors, it is composite
  - Note that 1 is not prime!
    - It's not composite either – it's in its own class
- Def: An integer n is composite if and only if there exists an integer a such that $a \mid n$ and $1 < a < n$

Fundamental theorem of arithmetic

- Every positive integer greater than 1 can be uniquely written as a prime or as the product of two or more primes where the prime factors are written in order of non-decreasing size
- Examples
  - 100 = 2 * 2 * 5 * 5
  - 182 = 2 * 7 * 13
  - 29820 = 2 * 2 * 3 * 5 * 7 * 71

Composite factors

- If n is a composite integer, then n has a prime divisor less than or equal to the square root of n

Showing a number is prime

- Show that 113 is prime
- Solution
  - The only prime factors less than $\sqrt{113} \approx 10.63$ are 2, 3, 5, and 7
  - Neither of these divide 113
  - Thus, by the fundamental theorem of arithmetic, 113 must be prime

Again: Number of Primes is infinite

- **Theorem (Euclid): There are infinitely many prime numbers**

Proof: Proof by contradiction
Assume there are a finite number of primes
List them as follows: $p_1, p_2 \ldots, p_n$.
Consider the number $q = p_1 p_2 \ldots p_n + 1$

Since we have only a finite number of primes and q is not one of them, p_i divides q for some i.
Obviously $p_i \mid p_1 p_2 \ldots p_n$
Recall that a | b, a | c $\Rightarrow$ a | b + c.

Therefore, $p_i \mid (q - p_1 p_2 \ldots p_n)$. Therefore, $p_i \mid 1$.
Therefore, $p_i = 1$. Contradtiction.

The prime number theorem

- **The radio of**
  the number of primes not exceeding x and $x/\ln(x)$
  approaches 1 as x grows without bound

Rephrased: the number of prime numbers less than x is approximately $x/\ln(x)$

When $x = 2^{512}$, # of primes $= 2^{512}/512 \approx 2^{503}$

Greatest common divisor

- The greatest common divisor of two integers a and b (gcd(a,b)) is the largest integer d such that $d \mid a$ and $d \mid b$
- Examples
  - gcd (24, 36) = 12
  - gcd (17, 22) = 1
  - gcd (100, 17) = 1

Relative primes

- Two numbers are *relatively prime* if they don't have any common factors (other than 1)
  - Rephrased: *a* and *b* are relatively prime if gcd (a,b) = 1
- gcd (25, 39) = 1, so 25 and 39 are relatively prime

Pairwise relative prime

- The integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if, for all pairs of numbers, they are relatively prime
  - Formally: The integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \le i < j \le n$.
- Example: are 10, 17, and 21 pairwise relatively prime?
  - gcd(10,17) = 1, gcd (17, 21) = 1, and gcd (21, 10) = 1
  - Thus, they are pairwise relatively prime
- Example: are 10, 19, and 24 pairwise relatively prime?
  - Since gcd(10,24) ≠ 1, they are not

More on gcd's

- Given two integers *a* and *b*, rewrite them as:

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$$

  - Example: gcd (120, 500)
    - $120 = 2^3 * 3 * 5 = 2^3 * 3^1 * 5^1$
    - $500 = 2^2 * 5^3 = 2^2 * 3^0 * 5^3$
- Then compute the gcd by the following formula:

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \ldots p_n^{\min(a_n,b_n)}$$

  - Example: gcd(120,500) $= 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)}$
    $= 2^2 3^0 5^1 = 20$

Least common multiple

- The **least common multiple** of the positive integers *a* and *b* is the smallest positive integer that is divisible by both *a* and *b*.
  - Denoted by lcm (*a*, *b*)

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_n^{\max(a_n,b_n)}$$

- Example: lcm(10, 25) = 50
- What is lcm (95256, 432)?
  - $95256 = 2^3 3^5 7^2$, $432 = 2^4 3^3$
  - lcm $(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^4 3^5 7^2$ = 190512

lcm and gcd theorem

- Let *a* and *b* be positive integers. Then $a*b = \gcd(a,b) * \text{lcm}(a, b)$
- Example:
  gcd (10,25) = 5,
  lcm (10,25) = 50,
  10*25 = 5*50
- Example:
  gcd (95256, 432) = 216,
  lcm (95256, 432) = 190512,
  95256*432 = 216*190512

Example Proof

- Prove or disprove that $n^2 - 79n + 1601$ is prime, whenever n is a positive integer.
- For all integers n<=79,
  $n^2 - 79n + 1601$ IS prime

  but… (Disprove by counter example)
  When n = 1601,
  $n^2 - 79n + 1601 = 1601\ (1601 - 79 + 1)$

Syddansk Universitet

ch 3.6
Integers and Algorithms

Representation of Integers

- Any positive integer n can be uniquely written as
  $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$
  (k is a positive integer, $0 < a_i < b$, and $a_k \neq 0$)
- The **base b expansion of n** is denoted by
  $(a_k a_{k-1} \ldots a_1 a_0)_b$
  - b = 2 : Binary representation
  - b = 16 : Hexadecimal representation
- $(245)_8 = 2 * 8^2 + 4 * 8^1 + 5 * 8^0 = 165$
  $= (10100101)_2$
  $= (A5)_{16}$

Euclidean Algorithm

- Example: gcd(287, 91)=… (blackboard)
- Let a = b q + r, where a, b, q, r be integers. Then gcd (a, b) = gcd (b, r).
- Proof: blackboard.

Euclidean Algorithm

- procedure gcd (a, b: positive integer)

```
x := a
y := b
while y ≠ 0
   r := x mod y
   x := y
   y := r
return x
```


Euclidean Algorithm Example

- gcd(120,23) = ???

Dividend	Divisor	Quotient	Remainder
120	23	5	5
23	5	4	3
5	3	1	2
3	2	1	1
2	1	2	0

Modular Exponentiation : a^k mod n

- 3^{13} mod 17 = $3^{2^3+2^2+1}$ mod 17 = $3^8 * 3^4 * 3^1$ mod 17
- INPUT: integers a, n, and k < n where $k = (k_{t-1}k_{t-2}\ldots k_0)_2 = \sum_{i=0}^{t-1} k_i 2^i$
- OUTPUT: a^k mod n.
- **Algorithm**

```
set b = 1.
if k = 0 then
   return b.
set A = a.
if k0 = 1 then set b = a.
for i from 1 to t-1 do the following:
   set A = A² mod n.
   if ki = 1 then set b = Ab mod n.
return b.
```

Modular Exponentiation

- a = 3
- k = 13 = $(1101)_2$ (i.e. t=4)
- n = 17

set b=1.
set A = a.
if k_0 = 1 then set b = a.
for i from 1 to t-1
  set A = A^2 mod n.
  if k_i = 1 then set b = Ab mod n.

i	k_i	b	A
		1	3
	1	3	3
1	0		3^2
2	1		3^4
		3 3^4	
3	1		3^8
		3 3^4 3^8	

(all numbers mod 17)

Modular Exponentiation

- a = 3
- k = 13 = $(1101)_2$ (i.e. t=4)
- n = 17

set b=1.
set A = a.
if k_0 = 1 then set b = a.
for i from 1 to t-1
  set A = A^2 mod n.
  if k_i = 1 then set b = Ab mod n.

i	k_i	b	A
		1	3
	1	3	3
1	0		9
2	1		81 mod 17 =13
		3*13 mod 17=5	
3	1		169 mod 17 = 16
		5*16 mod 17=**12**	

SYDDANSK UNIVERSITET

ch 3.7 Applications of Number Theory

Some Useful Results

- Theorem 1:
  If a and b are positive integers, then there exists s and t such that gcd(a, b) = s a + t b.

  (Proof): Try it!

Some Useful Results

- Lemma 1
  If a, b, c are positive integers such that gcd(a, b) = 1 and a | bc, then a | c.

  Proof:
  Since gcd(a, b) = 1, there exist integer s, t such that as + bt = 1. By multiplying c on both sides, we get asc + btc = c.
  Since a | bc, a | btc holds. Also a | asc holds.
  Therefore, a | c.

Some Useful Results

- We can divide both sides of a congruence by an integer relatively prime to the modulus.
- Formally:
  $m \in \mathbf{Z}^+$, a, b, $c \in \mathbf{Z}$.
  $ac \equiv bc \pmod m$ and $\gcd(c,m)=1 \Rightarrow a \equiv b \pmod m$

  Proof:
  m | ac – bc
  Then ∃ t such that c(a–b) = mt.
  By Lemma 1, since gcd(c, m)=1 it follows m | a–b.
  Then $a \equiv b \pmod m$.

Some useful results

- Definition:
  a^{-1} is the (multiplicative) inverse of a modulo m if $a*a^{-1} \equiv 1 \pmod m$.
- Does this always exist? No! (example: blackboard)
- An inverse of a modulo m exists, if a and m are relatively prime and m>0.
- Formally:
  If gcd (a, m) = 1 and m > 1, then a^{-1} exists.
  Proof: Using Theorem 1.

Extended Eucledean Algorithm

- gcd(120,23)?
- multiplicative inverse of 120 modulo 23?
- multiplicative inverse of 23 modulo 120?
- http://imada.sdu.dk/~svalle/courses/dm527-2007/examples/euclid.php

Step	Quotient	Remainder	Substitute	Combine terms
1		120		120 = 120 × 1 + 23 × 0
2		23		23 = 120 × 0 + 23 × 1
3	5	5 = 120 − 23 × 5	5 = (120 × 1 + 23 × 0) − (120 × 0 + 23 × 1) × 5	5 = 120 × 1 + 23 × −5
4	4	3 = 23 − 5 × 4	3 = (120 × 0 + 23 × 1) − (120 × 1 + 23 × −5) × 4	3 = 120 × −4 + 23 × 21
5	1	2 = 5 − 3 × 1	2 = (120 × 1 + 23 × −5) − (120 × −4 + 23 × 21) × 1	2 = 120 × 5 + 23 × −26
6	1	1 = 3 − 2 × 1	1 = (120 × −4 + 23 × 21) − (120 × 5 + 23 × −26) × 1	1 = 120 × **−9** + 23 × **47**
7	2	0	*End of algorithm*	

Linear Congruential Equation

- A congruence of the form $ax \equiv b \pmod{m}$ where a and b are positive integers, and x is a variable, is called a linear congruence.
- Find x such that $3x \equiv 4 \pmod{7}$.

$3x \equiv 4 \pmod{7}$.
$3^{-1}\ 3x \equiv 3^{-1}\ 4 \pmod{7}$.
$x \equiv (-2)\ 4 \pmod{7}$ (since $3^{-1} \equiv -2 \pmod{7}$)
$x \equiv 6 \pmod{7}$

i.e., …,-15,-8,-1,6,13,20,… are solutions

Chinese Remainder Theorem

- Imagine that you're a commander in the Chinese Army about two-thousand years ago. When you went out into battle, you had 208 soldiers with you. You're back from battle now, but there surely aren't still 208 soldiers there. How many do you have?

Groups of 3: 2 soldiers left.
Groups of 5: 3 soldiers left.
Groups of 7: 2 soldiers left.

Chinese Remainder Theorem

- Given integers $m_1, m_2, \ldots, m_n$, which are pairwise relatively prime, then
  $x \equiv a_1 \pmod{m_1}$,
  $x \equiv a_2 \pmod{m_2}$,
  $x \equiv a_3 \pmod{m_3}$,
  …,
  $x \equiv a_n \pmod{m_n}$
  has the unique solution :
  $$x \equiv y_1 a_1 M_1 + \ldots + y_n a_n M_n \pmod{m}$$
  where $m = m_1 * m_2 * \ldots * m_r$, $M_i = m/m_i$, $y_i M_i \equiv 1 \pmod{m_i}$.

Proof: Check x is a solution.

Special case of the CRT

- Given integers $m_1, m_2, \ldots, m_n$, which are pairwise relatively prime. If

  $x \equiv a \pmod{m_1}$,
  $x \equiv a \pmod{m_2}$,
  …
  $x \equiv a \pmod{m_n}$

  then

  $x \equiv a \pmod{m * m_2 * \ldots * m_r}$

(Shown in Exercise 23 of Chapter 3.7)

CRT Example

- Find x satisfying
  $x \equiv 1 \pmod 3$ and
  $x \equiv 4 \pmod 5$.
  - $m_1 = 3$, $m_2 = 5$, $a_1 = 1$, $a_2 = 4$
  - $m = 3 * 5 = 15$
  - $M_1 = 5$, $M_2 = 3$
  - $y_1 * 5 \equiv 1 \pmod 3 \Rightarrow y_1 = 2$
  - $y_2 * 3 \equiv 1 \pmod 5 \Rightarrow y_2 = 2$
  - $x = 2 * 1 * 5 + 2 * 4 * 3 \equiv 4 \pmod{15}$.

You can use the Extended Eucledian Algorithm to find the inverse!

Fermat's Little Theorem

If p is a prime and a is an integer, then $a^p \equiv a \pmod p$.

Variant: If p is a prime, and a is an integer coprime to p, then $a^{p-1} \equiv 1 \pmod p$.

Sketch of Proof:

Step 1) If a is not divisible by p, no two of the integers $1 \cdot a$, $2 \cdot a$, …, $(p-1) \cdot a$ are congruent modulo p.

Step 2) $1 \cdot 2 \cdots (p-1) \equiv 1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a \pmod p$

Step 3) $(p-1)! \equiv a^{p-1} (p-1)! \pmod p$

Application of Fermat's little theorem

- 541: prime
  - $2^{540} \pmod{541} \equiv 1$
  - $2^{20098261} \pmod{541}$
    $\equiv 2^{(540 * 37219) + 1} \pmod{541}$
    $\equiv (2^{540})^{37219} 2^1 \pmod{541}$
    $\equiv 2 \pmod{541}$
- **Compute $x \equiv 2^{60} \pmod{899}$**
  - Note, that $899 = 29 * 31$
  - First compute $2^{60} \equiv 16 \pmod{29}$ and $2^{60} \equiv 1 \pmod{31}$.
  - Since $x \equiv 16 \pmod{29}$ and $x \equiv 1 \pmod{31}$, using CRT find $x \equiv 683 \bmod 899$.

HOW?

RSA Encryption

- Key Generation
  - two **large** random primes p and q, each roughly the same size
  - $n = pq$
  - e, $1 < e < (p-1)(q-1)$, such that $\gcd((p-1)(q-1), e) = 1$
  - $ed \equiv 1 \pmod{(p-1)(q-1)}$
  - Public key is (n, e); Private key is (n, d)
- **Encryption:** compute $c = m^e \bmod n$
- **Decryption:** $m = c^d \bmod n$
- Why does it work?

Why RSA works?

as $ed \equiv 1 \pmod{(p-1)(q-1)}$

- $c^d \pmod n$
  $\equiv m^{ed} \pmod n$
  $\equiv m^{1 + k(p-1)(q-1)} \pmod n$
  $\equiv m$

Now let's apply Fermat's Little Theorem

- Last equivalence:
  - $m^{1+k(p-1)(q-1)} \pmod p \equiv m \cdot (m^{(p-1)})^{k(q-1)} \pmod p \equiv m \pmod p$
  - $m^{1+k(p-1)(q-1)} \pmod q \equiv m \cdot (m^{(q-1)})^{k(p-1)} \pmod q \equiv m \pmod q$
  - Using (the special case of) the Chinese remainder theorem, the conclusion follows.

Matrices (blackboard)

Notation: $A = [a_{ij}]$ with $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$

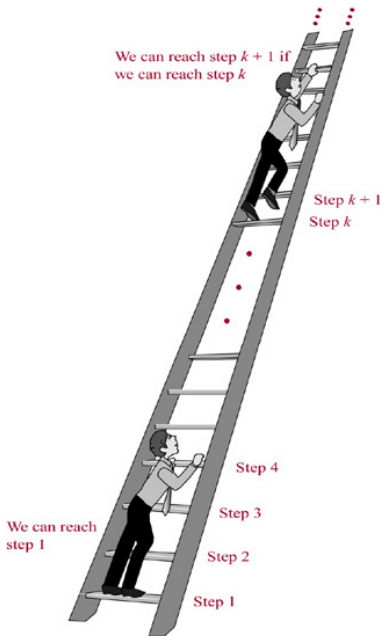
- Sum of matrices $A + B = [a_{ij} + b_{ij}]$
- Product of matrices $AB = \left[\sum_k a_{ik} b_{kj}\right]$

$$A = \begin{pmatrix} 1 & -2 & 2 \\ 1 & 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 1 \\ 3 & -1 & 5 \\ 4 & 2 & 0 \end{pmatrix} \quad AB = \begin{pmatrix} 3 & 6 & -9 \\ 9 & 4 & 1 \end{pmatrix}$$

- Identity Matrix I_n
- Transpose of Matrices A^T
- Powers of Matrices A^k
- Zero-One Matrices (join, meet, boolean product)

SYDDANSK UNIVERSITET

ch 4.1, 4.2, 4.3
Mathematical Induction, Strong Induction, Recursion



What is induction?

- A method of proof
- Three parts:
  - **Base case(s) / basis step:**
    Show P(k) is true for k=1
  - **Inductive hypothesis:**
    Assume P(k) is true for an arbitrary positive integer k
  - **Inductive step:**
    Show that if P(k) is true, then P(k+1) is true

Mathematical Induction

- A powerful technique for proving that a predicate $P(n)$ is true for *every* natural number n, no matter how large.
- Based on a predicate-logic inference rule:

$$\frac{P(1) \quad \forall n \geq 1\ (P(n) \rightarrow P(n+1))}{\therefore \forall n \geq 1\ P(n)}$$

"The First Principle of Mathematical Induction"

Induction example

- Show that the sum of the first n odd integers is n^2
  - Example: If $n = 5$, $1+3+5+7+9 = 25 = 5^2$
  - Formally, Show $\forall$ n P(n) where P(n) is the proposition $\sum^{n}_{i=1}(2i-1) = n^2$
- Base case: Show that P(1) is true
  - P(1) is true, because $(2*1-1) = 1^2$
- Inductive hypothesis: assume P(k) is true for an arbitrary positive integer *k*
  - Thus, we assume that P(*k*) is true, or that $\sum^{k}_{i=1}(2i-1) = k^2$
  - Note: we don't yet know if this is true or not!
- Inductive step: show P(k+1) is true
  - i.e., we need to show that $\sum^{k+1}_{i=1}(2i-1) = (k+1)^2$

Induction Example

- Induction hypothesis:
  - Assume P(k) is true, i.e. $\sum^{k}_{i=1}(2i-1) = k^2$
- Inductive step:
  - $\sum^{k+1}_{i=1}(2i-1) = \sum^{k}_{i=1}(2i-1) + (2(k+1)-1)$
    $= k^2 + (2k+1)$
    $= (k+1)^2$

    i.e. P(k+1) is true

because P(k) is true

What did we show

- Base case: P(1)
- If P(k) is true, then P(k+1) is true
  - i.e., P(k) → P(k+1) (for all positive integers k)
- We know P(1) is true
- Because of P(k) → P(k+1), it holds : if P(1) is true, then P(2) is true
- Because of P(k) → P(k+1), it holds : if P(2) is true, then P(3) is true
- Because of P(k) → P(k+1), it holds : if P(3) is true, then P(4) is true
- Because of P(k) → P(k+1), it holds : if P(4) is true, then P(5) is true
- And onwards to infinity
- Thus, it P(k) is true for all possible values of k
- Using first order logic:
  - $[P(1) \wedge \forall k\ (P(k) \rightarrow P(k+1))] \rightarrow \forall n\ P(n)$

Second induction example

- Show the sum of the first n positive even integers is $n^2 + n$
  - Rephrased: $\forall$ n P(n) is true where P(n) is the proposition $\sum_{i=1}^{n} (2\ i) = n^2 + n$ for the integer n
- The three parts:
  - Base case
  - Inductive hypothesis
  - Inductive step

Induction example

- Show that $n! < n^n$ for all $n > 1$
- Base case: $n = 2$

  $2! < 2^2$

  $2 < 4$
- Inductive hypothesis: assume $k! < k^k$ for an arbitrary positive integer k>1 is true
- Inductive step: show that $(k+1)! < (k+1)^{k+1}$
  - $(k+1)! = (k+1) \cdot k!$

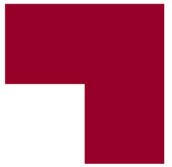
    $< (k+1)\ k^k$

    $< (k+1)\ (k+1)^k$

    $= (k+1)^{k+1}$

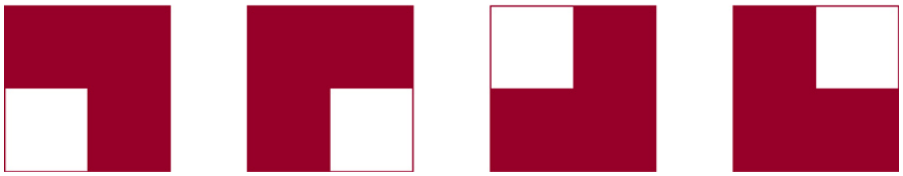
Another one…

Let n be a positive integer. Let P(n) be the proposition that any 2^n x 2^n checkerboard with one square removed can be tiled using pieces like the following:



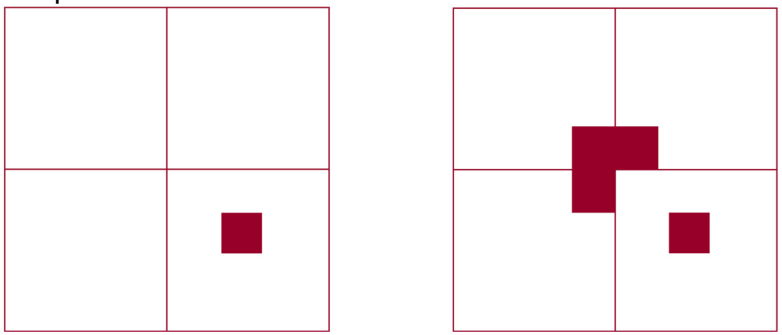
Basis step:

P(1) is true :



Inductive Step:

Assume P(k) is true for the positive integer k. We want to show that P(k+1) is true, i.e., it must be shown that any 2^{k+1} x 2^{k+1} checkerboard with one square removed can be tiles with the given piece:



The Well-Ordering Property

- The validity of the inductive inference rule can also be proved using the **well-ordering property**, which says:
  - Every non-empty set of non-negative integers has a least (smallest) element.

Why the induction is valid?

- $P(0) \wedge \forall n \geq 0\ (P(n) \rightarrow P(n+1))$
  $\therefore \forall n \geq 0\ P(n)$
- Suppose that $S = \{n \mid \neg P(n)\}$ is non-empty.

  By the well-ordering property, S has a least element m such that $P(m)$ is false.

  Then $m \neq 0$ (since $P(0)$ is true) and $P(m-1)$ is false (since $\forall n \geq 0\ (P(n) \rightarrow P(n+1))$).

  This contradicts to m is the least element.

Outline of an Inductive Proof

- Want to prove $\forall n\ P(n)$…
  - **Basis step:** Prove $P(0)$ is true.
  - **Inductive step:** Prove $\forall n\ P(n) \rightarrow P(n+1)$.

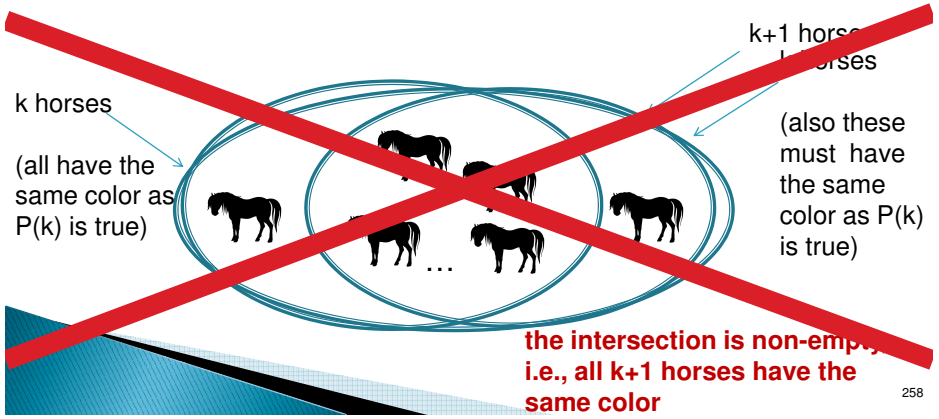
All horses have the same color

Let P(n) be the proposition that all horses in a set of n horses have the same color.

Basis step: Clearly, P(1) is true.

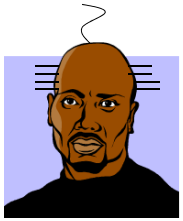
Hypothesis: P(k) is true for an arbitrary positive integer k.

Inductive step:



Interesting Induction

- Someone with zero hairs is bald.
- Someone with one more hair than a bald person is bald.
- .
- . turn the inductive crank……
- .
- Therefore, someone with 1,000, 000 hairs is bald.



- What's wrong with this induction?

More Examples

- Prove that if $h > -1$, then $1+nh \leq (1+h)^n$ for all non-negative integer n.
- Prove that $n^2 \equiv 1 \pmod 8$ for all odd integer n.

More Examples

- Suppose that $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$

  Show that $A^n = \begin{pmatrix} a^n & 0 \\ 0 & b^n \end{pmatrix}$

Strong mathematical induction

- **Weak mathematical induction** assumes P(*k*) is true, and uses that (and only that!) to show P(*k*+1) is true
- **Strong mathematical induction** assumes P(1), P(2), …, P(*k*) are all true, and uses that to show that P(*k*+1) is true.

  $[P(1) \wedge P(2) \wedge p(3) \wedge \ldots \wedge P(k)] \rightarrow P(k+1)$

Strong mathematical induction

- Characterized by another inference rule:

$$\frac{P(0) \quad \forall n \geq 0: ((\forall 0 \leq k \leq n : P(k)) \rightarrow P(n+1))}{\therefore \forall n \geq 0: P(n)}$$

P is true in all previous cases

"The Second Principle of Mathematical Induction"

Strong induction example 1

- Show that any number > 1 can be written as the product of primes
- Base case: P(2)
  - 2 is the product of 2 (remember that 1 is not prime!)
- Inductive hypothesis: P(2), P(3), P(4), …, P(*k*) are all true
- Inductive step: Show that P(*k*+1) is true

Strong induction example 1

- Inductive step: Show that P(k+1) is true
- There are two cases:
  - k+1 is prime
    - It can then be written as the product of k+1
  - k+1 is composite
    - It can be written as the product of two composites, a and b, where $2 \le a \le b < k+1$
    - By the inductive hypothesis, both P(a) and P(b) are true

Strong Induction Examples 2

- Prove that every amount of 12 cents or more can be formed using just 4-cent and 5-sent stamps.
- Base case:
  - 12 = 3 * 4 cent stamp
  - 13 = 2 * 4 + 1 * 5
  - 14 = 1 * 4 + 2 * 5
  - 15 = 3 * 5
- Inductive step: Suppose P(j) is true for $12 \le j \le k$ ($k \ge 15$). It is sufficient to show that P(k+1) is true. We know that P(k-3) is true since $k \ge 15$. To form postage of k+1 cents, we just need to add 1 4-cent postage to the stamps we used to form k-3 cents.

4.3 Recursive Definitions.

The process of defining an object in terms of itself is called recursion. Recursion can be used to define sequences, functions, sets, …

e.g. We can specify the terms of a sequence using

(1) an explicit formula:

$$a_n = 2^n, \quad n = 0,1,2,\ldots$$

(2) or using a recursive form:

$$a_0 = 1,$$
$$a_{n+1} = 2a_n, \quad n = 0,1,2,\ldots$$

Example. Suppose that f is defined recursively by $f(0)=3$, $f(n+1)=2f(n)+3$

Find $f(1), f(2), f(3), f(4)$.

Example. Give an inductive (recursive) definition of the factorial function $F(n) = n!$

Sol :

initial value : $F(0) = 1$

recursive form : $F(n+1) = (n+1)! = n! \cdot (n+1)$
$= F(n) \cdot (n+1)$

Example. The Fibonacci numbers $f_0, f_1, f_2 \ldots$, are defined by : $f_0 = 0$,
$f_1 = 1$,
$f_n = f_{n-1} + f_{n-2}$, for $n = 2,3,4,\ldots$

what is f_4 ?

Solution :

$$f_4 = f_3 + f_2 = (f_2 + f_1) + (f_1 + f_0) = f_2 + 2$$
$$= (f_1 + f_0) + 2 = 3$$

Example 6. Show that $f_n > \varphi^{n-2}$, where $\varphi = \frac{1+\sqrt{5}}{2}, n \geq 3$

Proof: (By Strong Induction)

Let $P(n)$ be the statement $f_n > \varphi^{n-2}$.

Base case $f_3 = 2 > \varphi$

$$f_4 = 3 > \varphi^2 = \frac{3+\sqrt{5}}{2}$$

so $P(3)$ and $P(4)$ are true.

Inductive step:

Assume that $P(3)$, $P(4)$, …, $P(n)$ are true.

We must show that $P(n+1)$ is true.

$$f_{n+1} = f_n + f_{n-1} > \varphi^{n-2} + \varphi^{n-3}$$
$$= \varphi^{n-3}(\varphi+1)$$

(using $\varphi+1 = \varphi^2$)

$$f_{n+1} > \varphi^{n-3} \cdot \varphi^2 = \varphi^{n-1}$$

We get that $P(n+1)$ is true. By Strong MI, $P(n)$ is true for all $n \geq 3$

Syddansk Universitet

ch 8.1 Relations

What is a relation

- Relation generalizes the notion of functions.
- Recall: A function takes EACH element from a set and maps it to a UNIQUE element in another set
  - f: X → Y
    - ∀ x ∈ X, ∃ y such that f(x) = y
- Let *A* and *B* be sets.
  A binary relation *R* from A to B is a subset of $A \times B$
  - Recall: A x B = {(a, b) | a ∈ A, b ∈ B}

aRb: (a, b) ∈ R.

What is a relation

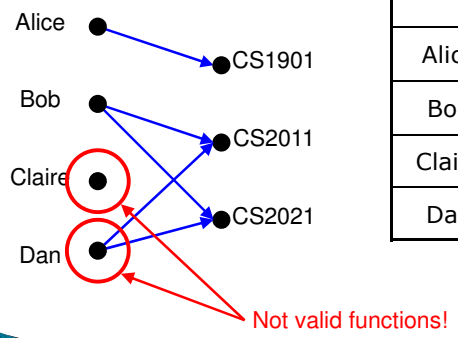
- Example
  - Let *A* be the students in a the CS major
    - *A* = {Alice, Bob, Claire, Dan}
  - Let *B* be the courses the department offers
    - *B* = {CS1901, CS2011, CS2021}
  - We specify relation $R \subseteq A \times B$ as the set that lists all students $a \in A$ enrolled in class $b \in B$
  - R = {(Alice, CS1011), (Bob, CS2011), (Bob, CS2021), (Dan, CS2011), (Dan, CS2021)}

More relation examples

- Another relation example:
  - Let A be the cities in Europe
  - Let B be the countries in Europe
  - We define R to mean a is a city in country b
  - Thus, the following are in our relation:
    - (Paris, France)
    - (Lion, France)
    - (Copenhagen, Denmark)
    - (Berlin, Germany)
    - etc…

Representing relations

We can represent relations graphically:



We can represent relations in a table:

	CS1901	CS2011	CS2021
Alice	X		
Bob		X	X
Claire			
Dan		X	X

Relations vs. functions

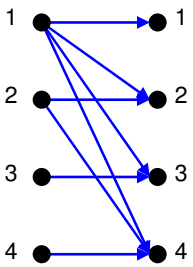
- If $R \subseteq X \times Y$ is a relation, then is R (the graph of) a function?
- If $f: X \to Y$ is a function, then is (the graph of) f a relation?

Relations on a set

- A relation on the set A is a relation from A to A

Relations on a set

- Let A be the set { 1, 2, 3, 4 }
- Which ordered pairs are in the relation
  R = { (a,b) | a divides b }
- R = {(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)}



R	1	2	3	4
1	X	X	X	X
2		X		X
3			X	
4				X

More examples

- Consider some relations on the set **Z**
- Are the following ordered pairs in the relation?

	(1,1)	(1,2)	(2,1)	(1,−1)	(2,2)
R_1 = { (a,b) | $a \le b$ }	X	X			X
R_2 = { (a,b) | $a > b$ }			X	X	
R_3 = { (a,b) | $a = \|b\|$ }	X			X	X
R_4 = { (a,b) | $a = b$ }	X				X
R_5 = { (a,b) | $a = b+1$ }			X		
R_6 = { (a,b) | $a+b \le 3$ }	X	X	X	X	

Relation properties

- Six properties of relations we will study:
  - Reflexive
  - Irreflexive
  - Symmetric
  - Asymmetric
  - Antisymmetric
  - Transitive

Reflexivity vs. Irreflexivity

- Reflexivity
  - Definition: A relation is reflexive if
    - $(a,a) \in R$ *for all* $a \in A$
- Irreflexivity
  - Definition: A relation is irreflexive if
    - $(a,a) \notin R$ *for all* $a \in A$

	=	<	>	≤	≥
reflexive	o	x	x	o	o
irreflexive	x	o	o	x	x

- Examples
  - Is the "divides" relation on $\mathbf{Z}^+$ reflexive?
  - Is the "$\subset$" (not $\subseteq$) relation on a P(A) irreflexive?

Reflexivity vs. Irreflexivity

- A relation can be neither reflexive nor irreflexive
- Example?
  - A = {1, 2}, R = {(1, 1)}
  - It is not reflexive, since (2, 2) $\notin R$,
  - It is not irreflexive, since (1, 1) $\in R$.

Symmetry, Asymmetry, Antisymmetry

- A relation is symmetric if
  - for all a, b $\in$ A, $(a,b) \in R \Rightarrow (b,a) \in R$
- A relation is asymmetric if
  - for all a, b $\in$ A, $(a,b) \in R \Rightarrow (b,a) \notin R$
- A relation is antisymmetric if
  - for all a, b $\in$ A, $((a,b) \in R \wedge (b,a) \in R) \Rightarrow a=b$
  - (Second definition) for all a, b $\in$ A, $((a,b) \in R \wedge a \neq b) \Rightarrow (b,a) \notin R$

	<	>	=	≤	≥	isTwinOf
symmetric	x	x	o	x	x	o
asymmetric	o	o	x	x	x	x
antisymmetric	o	o	o	o	o	x

Notes on *symmetric relations

- A relation can be neither symmetric or asymmetric
  - R = { (a,b) | a=|b| }
  - This is not symmetric
    - -4 is not related to itself
  - This is not asymmetric
    - 4 is related to itself
  - Note that it is antisymmetric

Transitivity

- A relation is transitive if
  - for all a, b, c $\in$ A, $((a,b) \in R \wedge (b,c) \in R) \Rightarrow (a,c) \in R$
- If $a < b$ and $b < c$, then $a < c$
  - Thus, $<$ is transitive
- If $a = b$ and $b = c$, then $a = c$
  - Thus, $=$ is transitive

Transitivity examples

- Consider isAncestorOf()
  - Let Alice be Bob's parent, and Bob be Claire's parent
  - Thus, Alice is an ancestor of Bob, and Bob is an ancestor of Claire
  - Thus, Alice is an ancestor of Claire
  - Thus, isAncestorOf() is a transitive relation
- Consider isParentOf()
  - Let Alice be Bob's parent, and Bob be Claire's parent
  - Thus, Alice is a parent of Bob, and Bob is a parent of Claire
  - However, Alice is *not* a parent of Claire
  - Thus, isParentOf() is *not* a transitive relation

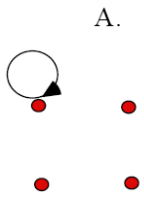
Summary of properties of relations

reflexive	$\forall a\ (a, a) \in R$
irreflexive	$\forall a\ (a, a) \notin R$
symmetric	$\forall\ a, b \in A, (a,b) \in R \Rightarrow (b,a) \in R$
asymmetric	$\forall\ a, b \in A, (a,b) \in R \Rightarrow (b,a) \notin R$
antisymmetric	$\forall\ a, b \in A, ((a,b) \in R \wedge (b,a) \in R) \Rightarrow a=b$ (*)for all $a, b \in A, ((a,b) \in R \wedge a \neq b) \Rightarrow (b,a) \notin R)$
transitive	$\forall\ a, b, c \in A, ((a,b) \in R \wedge (b,c) \in R) \Rightarrow (a,c) \in R$

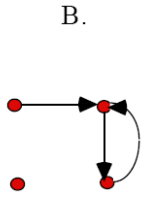
(*) Alternative definition…

Properties of Relations

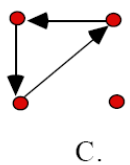
A:
not reflexive
not irreflexive
symmetric
not asymmetric
antisymmetric
transitive



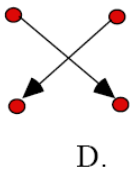
B:
not reflexive
irreflexive
not symmetric
not asymmetric
not antisymmetric
not transitive



C:
not reflexive
irreflexive
not symmetric
asymmertric
antisymmetric
not transitive



D:
not reflexive
irreflexive
not symmetric
asymmetric
antisymmetric
transitive



Combining relations

- There are two ways to combine relations R_1 and R_2
  - Via set operators
  - Via relation "composition"
- Example (blackboard)
  R_1 : „smaller than"
  R_2 : „greater than"

Combining via relational composition

- Similar to function composition
- Let R be a relation from A to B, and S be a relation from B to C
  - Let $a \in A$, $b \in B$, and $c \in C$
  - Let $(a,b) \in R$, and $(b,c) \in S$
  - The composite of R and S consists of the ordered pairs (a,c)
    - We denote the relation by $S \circ R$
    - Note that S comes first when writing the composition!
  - (a, c) $\in S \circ R$ if $\exists$ b such that (a, b) $\in R$, and $(b,c) \in S$

Combining via relational composition

- Let M be the relation "is mother of"
- Let F be the relation "is father of"
- What is $M \circ F$? (the composite of F and M!)
  - If $(a,b) \in F$, then a is the father of b
  - If $(b,c) \in M$, then b is the mother of c
  - Thus, $M \circ F$ denotes the relation "maternal grandfather"
- What is $F \circ M$?
  - If $(a,b) \in M$, then a is the mother of b
  - If $(b,c) \in F$, then b is the father of c
  - Thus, $F \circ M$ denotes the relation "paternal grandmother"
- What is $M \circ M$?
  - If $(a,b) \in M$, then a is the mother of b
  - If $(b,c) \in M$, then b is the mother of c
  - Thus, $M \circ M$ denotes the relation "maternal grandmother"

Combining via relational composition

- Given relation R
  - $R \circ R$ can be denoted by R^2
  - $R^2 \circ R = (R \circ R) \circ R = R^3$
  - Example: M^3 is your mother's mother's mother

SYDDANSK UNIVERSITET

ch 8.2
n-ary Relations (blackboard)

8.3 Representing Relations

Connection Matrices

- Let R be a relation from

  $A = \{a_1, a_2, \ldots, a_m\}$ to $B = \{b_1, b_2, \ldots, b_n\}$.
- **Definition:** A_n *m× n connection matrix M* for *R is* defined by $M_{ij} = 1$ if (a_i, b_j) is in R, $= 0$ otherwise.
- Example: We assume the rows are labeled with the elements of A and the columns are labeled with the elements of B. Let $A = \{a, b, c\}$, $B = \{e, f, g, h\}$; $R = \{(a, e), (c, g)\}$
- Then the connection matrix M for R is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

(Note: the order of the elements of A and B matters)

Representing Relations

- **Theorem:** Let R be a binary relation on a set A and let M be its connection matrix. Then
  - R is reflexive iff $M_{ii} = 1$ for all i.
  - R is symmetric iff M is a symmetric matrix: $M = M^T$
  - R is antisymetric if $M_{ij} = 0$ or $M_{ji} = 0$ for all $i \neq j$.

$$\begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ & & & & & 1 \end{bmatrix}$$

The Zero-One Matrix for a Reflexive Relation.

$$\begin{bmatrix} & & 1 \\ & 0 & \\ 1 & & \end{bmatrix} \qquad \begin{bmatrix} 1 & & \\ & 0 & \\ & & 1 \end{bmatrix}$$

(a) Symmetric (b) Antisymmetric

The Zero-One Matrices for Symmetric and Antisymmetric Relations.

The Composition

- **Definition:** Let

  M_R be the connection matrix for R

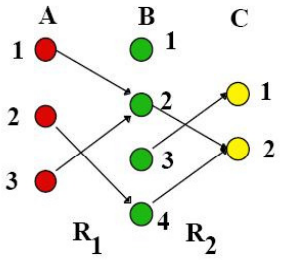
  M_S be the connection matrix for S.

  The boolean product of two connection matrices M_R and M_S, denoted $M_R \odot M_S$, is the connection matrix for the composite of R and S, $S \circ R$.

$$M_{R^n} = M_{R \circ R \circ \ldots \circ R} = M_R \odot M_R \odot \ldots \odot M_R = M_R^{[n]}$$

The Composition

Example :



$$M_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \qquad M_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$M_1 \odot M_2 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$$

$$(M_1 \odot M_2)_{12} = [(M_1)_{11} \wedge (M_2)_{12}] \vee [(M_1)_{12} \wedge (M_2)_{22}] \vee [(M_1)_{13} \wedge (M_2)_{32}] \vee [(M_1)_{14} \wedge (M_2)_{42}]$$
$$= [0 \wedge 0] \vee [1 \wedge 1] \vee [0 \wedge 0] \vee [0 \wedge 1] = 1$$

The Composition

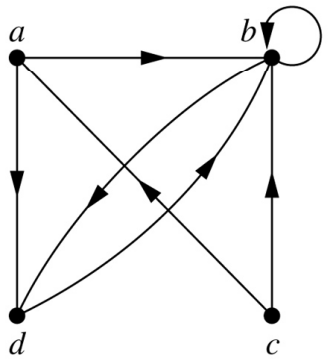
- Note:
  there is an arc in R_1 *from node 1 in A to node 2 in B*
  there is an arc in R_2 *from node 2 in B to node 2 in* C
  hence there is an arc in $R_2 \circ R_1$ *from node 1 in A to* node 2 in C.

Representing Relations Using Digraphs

- Definition 1: A *directed graph*, or *digraph*, consists of a set V of *vertices* (or *nodes*) together with a set E of ordered pairs of elements of V called *edges* (or *arcs*).
- The vertex *a* is called the *initial vertex* of the edge (a, b), and the vertex b is called the *terminal vertex* of this edge.
- An edge of the form (*a*, *a*) is represented using an arc from the vertex a back to itself. Such an edge is called a **loop**.

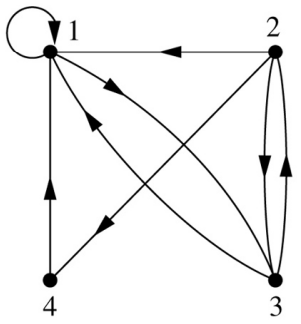
Representing Relations Using Digraphs

- Example: The directed graph with vertices a, b, c, and d, and edges (a, b), (a, d), (b, b), (b, d), (c, a), (c, b), and (d, b) :



Representing Relations Using Digraphs

- Example: The directed graph of the relation R={(1, 1), (1, 3), (2, 1), (2, 3), (2, 4), (3, 1), (3, 2), (4, 1)} on the set {1, 2, 3, 4}:



8.4 Closures of Relations

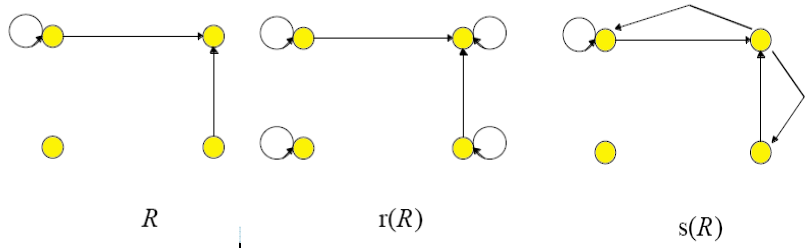
- Definition: The *closure* of a relation R with respect to property P is the relation obtained by adding the minimum number of ordered pairs to R to obtain property P.
- In terms of the digraph representation of *R*
  --To find the reflexive closure – add loops.
  --To find the symmetric closure – add arcs in the opposite direction.
  --To find the transitive closure – if there is a path from a to b, and a path from b to c, add an arc from a to c.
- Note: Reflexive and symmetric closures are easy. Transitive closures can be more complicated.

Symmetric and Reflexive Closure

Let *R be a relation on A. The* ***symmetric closure*** *of R, is denoted s(R), the* ***reflexive closure*** *is denoted r(R).*

Example: What is the symmetric / reflexive closure of the relation R={(a, b) | a> b} on the set of positive integers?

Example:



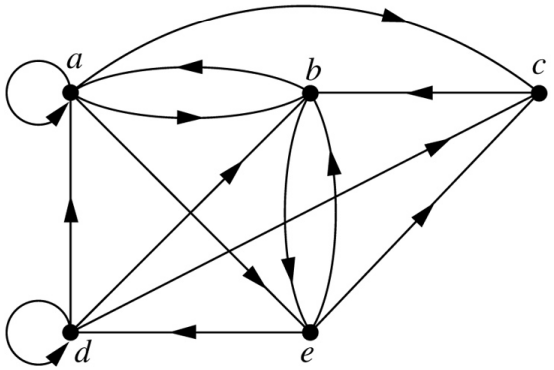
Paths in Directed Graphs

- Definition: A **path** from a to b in the directed graph G is a sequence of edges $(x_0, x_1), (x_1, x_2), (x_2, x_3), \ldots, (x_{n-1}, x_n)$ in G, where n is a nonnegative integer, and $x_0 = a$ and $x_1 = b$.
- This path is (often) denoted by $x_0, x_1, x_2, \ldots, x_{n-1}, x_n$ and has *length* n.

Example: blackboard / next slide

Paths in Directed Graphs

- Examples:
  Which of the following are paths in the directed graph show below? What are the lengths of those that are paths? Which of the paths in this list are circuits?
  - a,b,e,d;
  - a,e,c,d,b;
  - *b,a,c,b,a,a,b;*
  - *d,c;*
  - *c,b,a;*
  - *e,b,a,d,a,b,e;*



Paths in Directed Graphs

- **Theorem:** Let R be a relation on A. There is a path of length *n from a to b iff* $(a, b) \in R^n$

  Proof: (by induction -> book)

Transitive Closure

- **Definition:** The ***connectivity relation*** or the ***star closure*** of the relation *R,* denoted *R*,* is the set of ordered pairs (a, b) such that there is a path (in R) from a to b:

$$R^* = \bigcup_{n=1}^{\infty} R^n$$

Theorem: The transitivity closure of a relation R, denoted t(R), equals the connectivity relation *R**

Example: blackboard (graphs for Ex. 7 from book)

Transitive Closure

- **Theorem:** Let M_R be the zero-one matrix of the relation R on the relation R on a set with n elements. Then the zero-one matrix of the transitive closure R* is

$$M_{R^*} = M_R \vee M_R^{[2]} \vee M_R^{[3]} \vee \cdots \vee M_R^{[n]}$$

- **Example:** Find the zero-one matrix of the transitive closure of the relation R where

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

Transitive Closure

- **Algorithm :** A Procedure for Computing the Transitive Closure

procedure *transitive_closure* (M_R :zero-one *nxn* matrix)

A := M_R
B := A
for i :=2 **to** n
begin
A := A⊙M_R
B := B ∨ A
end {B is the zero-one matrix for R* }

ch 8.5
Equivalence Relations

Equivalence Relations

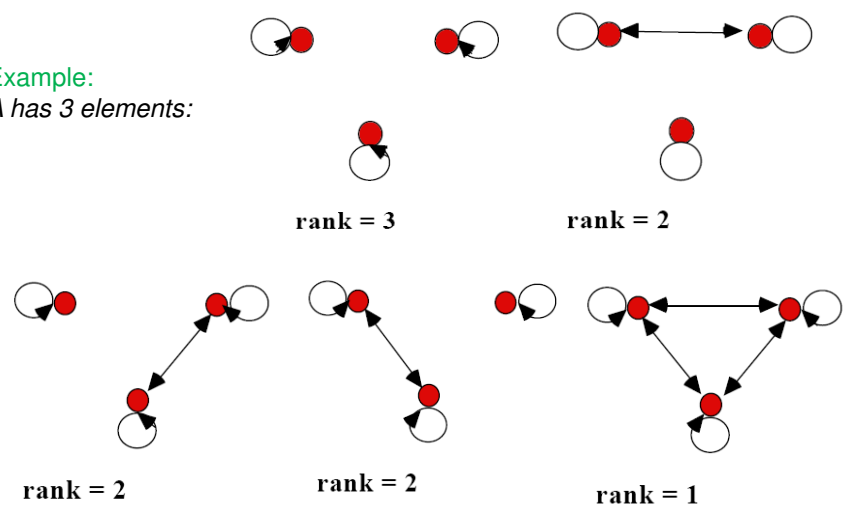
- Now we group properties of relations together to define new types of important relations.
- Definition: A relation *R on a set A is an equivalence relation iff R is*
  - reflexive
  - symmetric
  - transitive

Equivalence Relations

- It is easy to recognize equivalence relations using digraphs.
- The subset of all elements related to a particular element forms a universal relation (contains all possible arcs) on that subset.
- The (sub)digraph representing the subset is called a *complete (sub)digraph. All arcs are* present.
  (The number of such subsets is called the *rank of the* equivalence relation.)

Equivalence Relations

Example:
A has 3 elements:



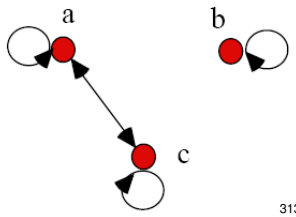
Equivalence Relations

- Each of the subsets is called an *equivalence class*.
- A bracket around an element means the equivalence class in which the element lies.

$$[x]_R = [x] = \{y \mid (x, y) \text{ is in } R\}$$

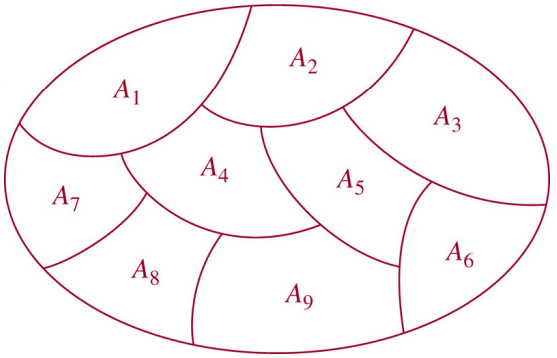
- The element in the bracket is called a *representative* of the equivalence class. We could have chosen any one.

- Example:
  [a] = {a, c}, [c] = {a, c}, [b] = {b}.
  rank = 2



Equivalence Relations

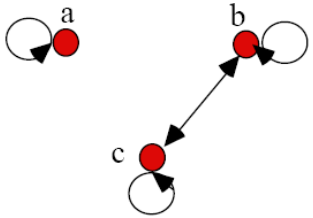
- **Definition:** Let $S_1, S_2, \ldots, S_n$ be a collection of subsets of A. Then the collection forms a ***partition*** of A if the subsets are **nonempty**, **disjoint** and ***exhaust*** A:
- $S_i \neq \varnothing$
- $S_i \cap S_j = \varnothing$ if $i \neq j$
- $\cup S_i = A$



A Partition of a Set.

Equivalence Relations

- **Theorem:** The equivalence classes of an equivalence relation R partition the set A into disjoint nonempty subsets whose union is the entire set.
- This partition is (often denoted A/R and) called
  -- the *quotient set*, *or*
  -- *the partition of A induced by R, or,*
  -- *A modulo R.*
- Example :
  $A/R = \{[a], [b]\}$
  $= \{[a], [c]\}$
  $= \{\{a\}, \{b,c\}\}$



Equivalence relations

- Example: Consider the relation
  $R = \{ (a,b) \mid len(a) = len(b) \}$
  where *len*(*a*) means the length of string *a*
  - It is reflexive: *len*(*a*) = *len*(*a*)
  - It is symmetric: if *len*(*a*) = *len*(b), then *len*(*b*) = *len*(*a*)
  - It is transitive: if *len*(*a*) = *len*(b) and *len*(b) = *len*(c), then *len*(a) = *len*(c)
  - Thus, *R* is a equivalence relation

Equivalence relation example

- Consider the relation $R = \{ (a,b) \mid a \equiv b \pmod{m} \}$
  - Remember that this means that $m \mid a-b$
- Is it reflexive: (a,a) $\in R$ means that $m \mid a-a$
  - $a-a = 0$, which is divisible by m
- Is it symmetric: if $(a,b) \in R$ then $(b,a) \in R$
  - (a,b) means that $m \mid a-b$
  - Or that $km = a-b$. Negating that, we get $b-a = -km$
  - Thus, $m \mid b-a$, so (b,a) $\in R$
- Is it transitive: if $(a,b) \in R$ and $(b,c) \in R$ then $(a,c) \in R$
  - (a,b) means that $m \mid a-b$, or that $km = a-b$
  - (b,c) means that $m \mid b-c$, or that $lm = b-c$
  - (a,c) means that $m \mid a-c$, or that $nm = a-c$
  - Adding these two, we get $km+lm = (a-b) + (b-c)$
  - Or $(k+l)m = a-c$
  - Thus, m divides $a-c$, where $n = k+l$
- Thus, congruence modulo m is an equivalence relation

Rosen, section 8.5, question 1

- Which of these relations on {0, 1, 2, 3} are equivalence relations? Determine the properties of an equivalence relation that the others lack
  - { (0,0), (1,1), (2,2), (3,3) }
    - Has all the properties, thus, is an equivalence relation
  - { (0,0), (0,2), (2,0), (2,2), (2,3), (3,2), (3,3) }
    - Not reflexive: (1,1) is missing
    - Not transitive: (0,2) and (2,3) are in the relation, but not (0,3)
  - { (0,0), (1,1), (1,2), (2,1), (2,2), (3,3) }
    - Has all the properties, thus, is an equivalence relation
  - { (0,0), (1,1), (1,3), (2,2), (2,3), (3,1), (3,2) (3,3) }
    - Not transitive: (1,3) and (3,2) are in the relation, but not (1,2)
  - { (0,0), (0,1) (0,2), (1,0), (1,1), (1,2), (2,0), (2,2), (3,3) }
    - Not symmetric: (1,2) is present, but not (2,1)
    - Not transitive: (2,0) and (0,1) are in the relation, but not (2,1)

Rosen, section 8.5, question 5

- Suppose that A is a non-empty set, and f is a function that has A as its domain. Let R be the relation on A consisting of all ordered pairs (x,y) where $f(x) = f(y)$
  - Meaning that x and y are related if and only if $f(x) = f(y)$
- Show that R is an equivalence relation on A
- Reflexivity: $f(x) = f(x)$
  - True, as given the same input, a function always produces the same output
- Symmetry: if $f(x) = f(y)$ then $f(y) = f(x)$
  - True, by the definition of equality
- Transitivity: if $f(x) = f(y)$ and $f(y) = f(z)$ then $f(x) = f(z)$
  - True, by the definition of equality

Rosen, section 8.5, question 8

- Show that the relation R, consisting of all pairs (x,y) where x and y are bit strings of length three or more that agree except perhaps in their first three bits, is an equivalence relation on the set of all bit strings
- Let $f(x)$ = the bit string formed by the last $n-3$ bits of the bit string x (where n is the length of the string)
- Thus, we want to show: let R be the relation on A consisting of all ordered pairs (x,y) where $f(x) = f(y)$
- This has been shown in question 5 on the previous slide

Partitions

- Consider the relation $R = \{ (a,b) \mid a \equiv b \pmod 2 \}$
- This splits the integers into two equivalence classes: even numbers and odd numbers
- In this example, the partition is { [0], [1] }
  - Or { {…, −3, −1, 1, 3, …}, {…, −4, −2, 0, 2, 4, …} }

Rosen, section 8.5, question 44

- Which are partitions of the set of integers?
  - The set of even integers and the set of odd integers
    - Yes, it's a valid partition
  - The set of positive integers and the set of negative integers
    - No: 0 is in neither set
  - The set of integers divisible by 3, the set of integers leaving a remainder of 1 when divided by 3, and the set of integers leaving a remaineder of 2 when divided by 3
    - Yes, it's a valid partition
  - The set of integers less than −100, the set of integers with absolute value not exceeding 100, and the set of integers greater than 100
    - Yes, it's a valid partition
  - The set of integers not divisible by 3, the set of even integers, and the set of integers that leave a remainder of 3 when divided by 6
    - The first two sets are not disjoint (2 is in both), so it's not a valid partition

8.6 Partial Orderings (not or only briefly covered in 2010)

- **Definition:** Let R be a relation on A. Then R is a *partial order* *iff* *R is*
- reflexive
- antisymmetric
- transitive
- *(A, R) is called a partially ordered set or a poset.*

Partial Orderings

- Note: It is not required that two things be related under a partial order. That's the *partial* part of it.
- If two objects are always related in a *poset*, it is called a total order or linear order or simple order.
- In this case (A, R) is called a *chain*.

Partial Orderings

- Examples:
  (Z, ≤) is a poset. In this case either $a \leq b$ *or* $b \leq a$ *so*
  two things are always related. Hence, ≤ is a total order and *(Z, ≤)* is a *chain.*
- If *S* is a set then *(P(S), ⊆) is a poset. It may not be* the case that $A \subseteq B$ *or* $B \subseteq A$. *Hence,* ⊆ *is not a total* order.
- *(Z+, 'divides') is a poset which is not a chain.*

Partial Orderings

- Definition: The elements a and b of a poset (S, $\preccurlyeq$) are called ***comparable*** if either $a \preccurlyeq b$ or $b \preccurlyeq a$.
- When *a* and b are elements of S such that neither $a \preccurlyeq b$ nor $b \preccurlyeq a$, *a* and b are called ***incomparable***.
- Example: In the poset (Z^+, |), are the integers 3 and 9 comparable? Are 5 and 7 are incomparable, because $5 \nmid 7$ and $7 \nmid 5$.

Partial Orderings

- Definition: Let *R* be a total order on *A* and suppose $S \subseteq A$. An element *s in S* is a least element of *S iff* *sRb* for every b in *S.*
- Similarly for *greatest element.*

Partial Orderings

- A Chain (A,R) is **well-ordered** iff every subset of A has a least element.
- Examples:
  (Z, ≤) is a chain but not well-ordered. Z does not have least element.
  (N, ≤) is well-ordered.
  (N, ≥) is not well-ordered.
- Theorem: **The Principle of Well-Ordered Induction**
  Suppose that S is a well-ordered set. Then P(x) is true for all $x \in S$, if
- Inductive Step: For every $y \in S$, if P(x) is true for all $x \in S$ with $x \prec y$, then P(y) is true.

Lexicographic Order

- Given two posets (A_1, R_1) and (A_2, R_2) we construct an *induced* partial order R on $A_1 \times A_2$:

$$(x_1, y_1)\ R\ (x_2, y_2) \quad \text{iff}$$

$$x_1\ R_1\ x_2 \text{ , or } x_1 = x_2 \text{ and } y_1\ R_2\ y_2.$$

- Example:

  Let $A_1 = A_2 = Z^+$ and $R_1 = R_2 =$ 'divides'. Then

- (2, 4) R (2, 8) since $x_1 = x_2$ and $y_1\ R_2\ y_2$.
- (2, 4) is not related under R to (2, 6) since $x_1 = x_2$ but 4 does not divide 6.
- (2, 4) R (4, 5) since $x_1\ R_1\ x_2$. (Note that 4 is not related to 5).

Lexicographic Order

- This definition extends naturally to multiple Cartesian products of partially ordered sets:

$$A_1 \times A_2 \times A_3 \times \ldots \times A_n.$$

- Example: Using the same definitions of A_i and R_i as above,
- (2, 3, 4, 5) R (2, 3, 8, 2) since $x_1 = x_2$, $y_1 = y_2$ and 4 divides 8.
- (2, 3, 4, 5) is not related to (3, 6, 8, 10) since 2 does not divide 3.

Lexicographic Order

- In the following Figure the ordered pairs in $Z^+ \times Z^+$ that are less than (3, 4) are highlighted.

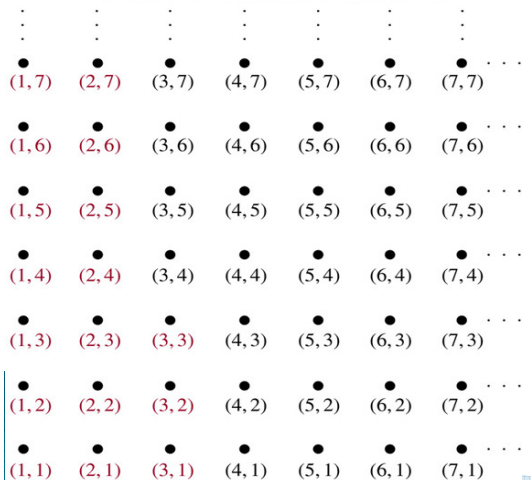


FIGURE The Ordered Pairs Less Than (3,4) in Lexicographic Order.

Strings

- We apply this ordering to strings of symbols where there is an underlying 'alphabetical' or partial order (which is a total order in this case).
- Example:

  Let $A = \{a, b, c\}$ and suppose R is the natural alphabetical order on A:

$$a\ R\ b \text{ and } b\ R\ c.$$

Then

- Any shorter string is related to any longer string(comes before it in the ordering).
- If two strings have the same length then use the induced partial order from the alphabetical order:

aabc R *abac*

Hasse or Poset Diagrams

- To construct a Hasse diagram:

  1) Construct a digraph representation of the poset *(A, R)* so that all arcs point up (except the loops).
  2) Eliminate all loops
  3) Eliminate all arcs that are redundant because of transitivity
  4) eliminate the arrows at the ends of arcs since everything points up.

Hasse Diagrams

- For instance, consider the directed graph for the partial ordering {(a, b)| a≤ b} on the set {1, 2, 3, 4}. Figure (a).
- we do not have to show these loops because they must be present. Figure (b).
- We do not have to show those edges that must be present because of transitivity. Figure (c)

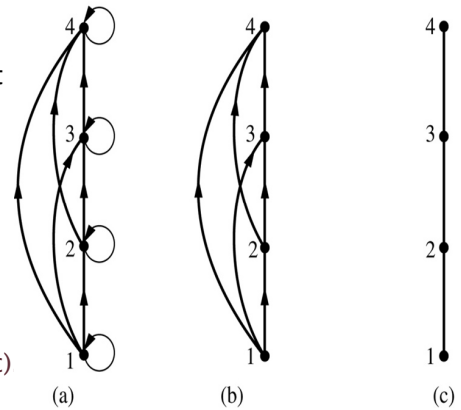
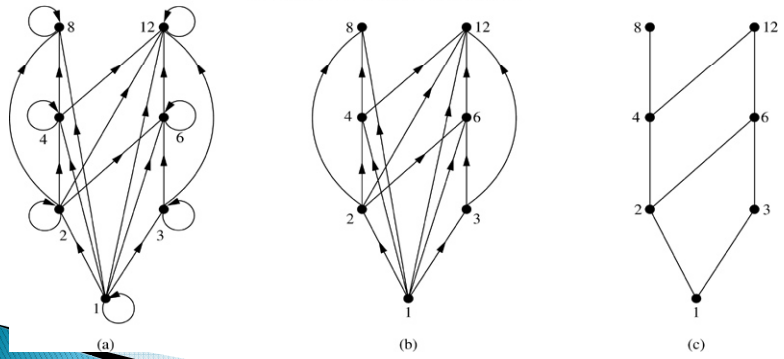


FIGURE Constructing the Hasse Diagram for ({1,2,3,4},≦).

Hasse Diagrams

- Example : Draw the Hasse diagram representing the partial ordering {(a, b)| a divides b} on {1, 2, 3, 4, 6, 8, 12}.



Hasse Diagrams

- Example: Hasse diagram representing the partial ordering {(A, B)| A ⊆ B} on the power set S={a ,b, c}.

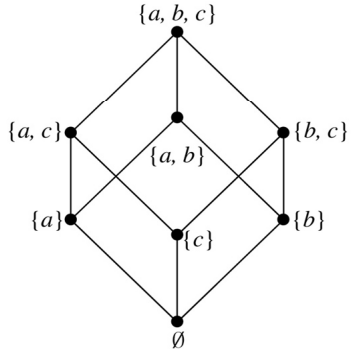


FIGURE The Hasse Diagram of $(P(\{a,b,c\}), \subseteq)$.

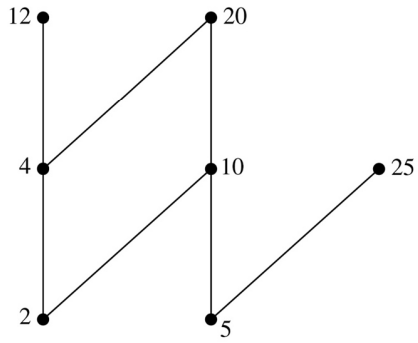
Maximal and Minimal Elements

- **Definition:** Let *(A, R)* be a poset. *Then a in A is a minimal element* if there does not exist an element b in A such that *bRa.*
- Similarly for a *maximal element.*

- Example: In the Hasse diagram (last slide), ∅ is a minimal element and *{a, b, c}* is a maximal element.

Maximal and Minimal Elements

- Example: Which elements of the poset ({2, 4, 5, 10, 12, 20, 25}, |) are maximal, and which are minimal?



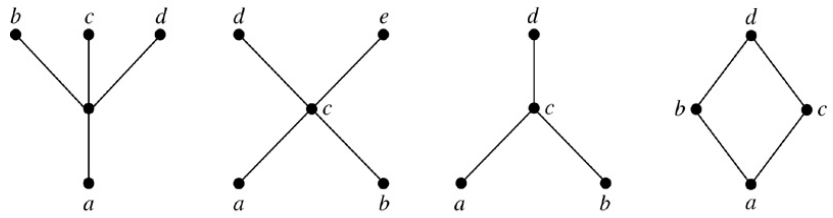
Least and Greatest Elements

- **Definition:** Let *(A, R) be a poset. Then a in A is the least element* if for every element b in A, *aRb* and b is the *greatest element* if for every element *a in A, aRb .*

- Example:
  In the poset on slide 336 *{a, b, c} is the greatest element.*
  ∅ *is* the least element.

Maximal and Minimal Elements

- Example: Determine whether the posets represented by each of the Hasse diagrams in the figure have a greatest element and a least element.

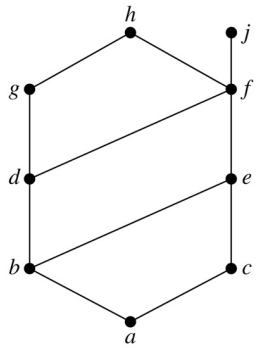


Upper and Lower Bounds

- **Definition:** Let *S* be a subset of *A* in the poset *(A, R).* If there exists an element *a in A* such that *sRa* for all *s in S,* then *a is called an upper bound .*
- Similarly for *lower bounds*.
- Note: to be an upper bound you must be related to every element in the set. Similarly for lower bounds.

Upper and Lower Bounds

- Example: Find the lower and upper bounds of the subsets {a, b, c} , {j, h}, and {a, c, d, f} in the poset with the Hasse diagram shown in the following Figure

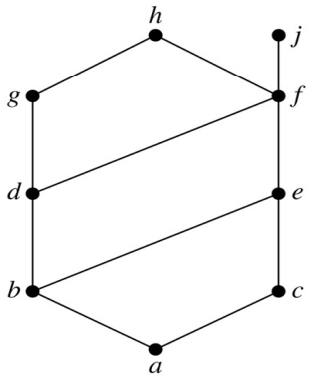


Least Upper and Greatest Lower Bounds

- **Definition:** If *a* is an upper bound for *S* which is related to all other upper bounds then it is the *least upper bound,* denoted lub(*S*) . Similarly for the *greatest lower bound*, glb(*S*) .
- Example: Consider the element {a} in Example 13. Since {a, b, c}, {a, b} {a, c} and {a} are upper bounds and {a} is related to all of them, {a} must be the *lub*. It is also the *glb*.

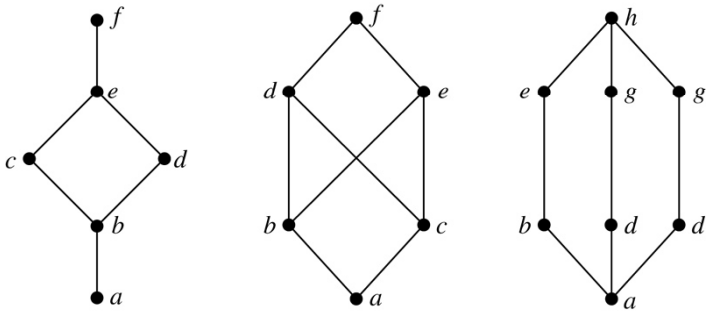
Least Upper and Greatest Lower Bounds

- Example: Find the greatest lower bound and the least upper bound of {b, d, g}, if they exist, in the poset shown in the following Figure .



Lattices

- Example: Determine whether the posets represented by each of the Hasse diagrams in the following Figure are lattices.



Topological Sorting

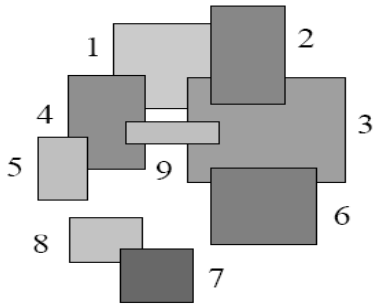
- We impose a total ordering R on a poset *compatible* with the partial order.
- Useful in rendering in graphics to render objects from back to front to obscure hidden surfaces.
- A painter uses a topological sort when applying paint to a canvas – he/she paints parts of the scene furthest from the view first.
- This definition extends naturally to multiple Cartesian products of partially ordered sets:

$$A_1 \times A_2 \times A_3 \times \ldots \times A_n.$$

Topological Sorting

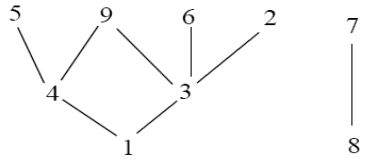
- Example:
- Consider the rectangles *T* and the relation *R* = *"is more* distant than." Then *R* is a partial order on the set of rectangles.
- Two rectangles, T_i *and* T_j, are related, $T_i R T_j$, if T_i is more distant from the viewer than T_j.

Topological Sorting

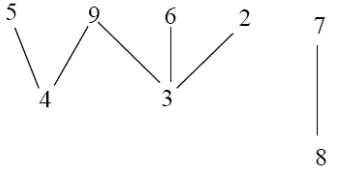


Then 1*R2, 1R4, 1R3, 4R9, 4R5, 3R2, 3R9, 3R6, 8R7.*

The Hasse diagram for *R is*



Draw 1 (or 8) and delete 1 from the diagram to get



Now draw 4 (or 3 or 8) and delete from the diagram. Always choose a minimal element. Any one will do. ...and so forth.

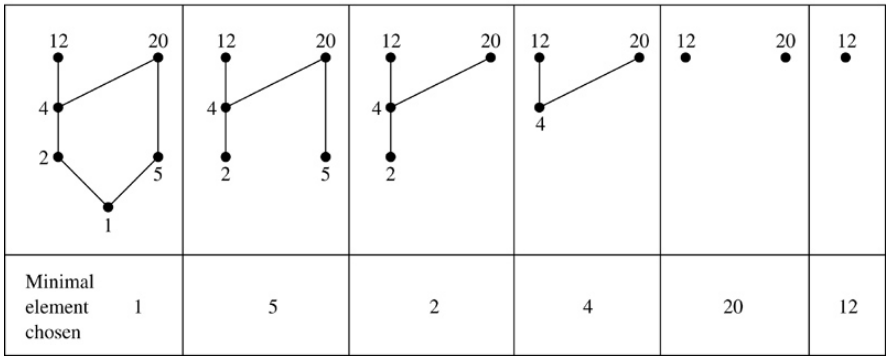
Topological Sorting

- Algorithm 1 Topological Sorting

procedure Topological Sorting ((S, $\preccurlyeq$) : finite poset)
k :=1
while S $\neq \varnothing$
begin
a_k := *a* minimal element of S { such an element exists by Lemma 1}
S := S – {a_k }
k := k + 1
end {a_1, a_2, . . ., a_n is a compatible total ordering of S}

Topological Sorting

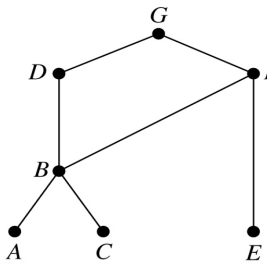
- Example: Find a compatible total ordering for the poset ({1, 2, 4, 5, 12, 20}, |).



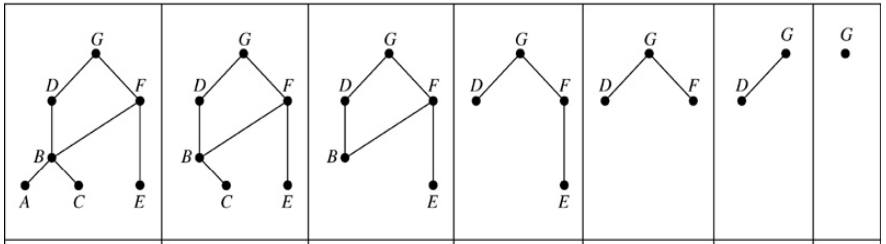
Minimal element chosen	1	5	2	4	20	12

Topological Sorting

- Example : A development project at a computer company requires the completion of seven tasks.
- Some of these tasks can be started only after other tasks are finished.
- A partial ordering on tasks is set up by considering task X ≺ task Y if task Y cannot be started until task X has been completed.
- The Hasse diagram for the seven tasks, with respect to this partial ordering, is shown in the Figure below.
- Find an order in which these tasks can be carried out to complete the project.



Topological Sorting



Minimal element chosen	A	C	B	E	F	D	G