Introduction to Discrete Mathematics

Course Outline

Prof. G. Kesidis, instructor

1

1

Course Outline

- Introduction to logic
- Introduction to methods of proof
- Sequences and induction
- Introduction to set theory
- Counting and probability – discrete random variables (see slidedeck on undergraduate probability)
- Functions and the pigeonhole principle
- Recursions
- Introduction to Complexity
- Relations
- Introduction to modular arithmetic and public-key cryptography
- Introduction to graphs

2

2

Introduction to Discrete Mathematics

Introduction to Logic

© S.S. Epp (2006)
This revision © G. Kesidis (2013)
This document revision is copy-left 2013.
It is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License

3

3

Intro to Logic – Outline

- Logical Form and Equivalence
- Conditional Statements
- Valid and Invalid Arguments
- Intro to Predicates and Quantified Statements
- Statements with Multiple Quantifiers
- Arguments with Quantified Statements

4

4

Concept of Logical Form

How do you know today isn't Easter?

If today is Easter, then it is Sunday.
It is not Sunday
Therefore, today is not Easter.

The form of this argument is called "modus tollens".

If p, then q.
Not q.
Therefore not p.

5

5

Modus tollens example

Example: Argument in the form of modus tollens.

If Sue is guilty, then Sue was in Rio on Aug. 18. (If p, then q.)

Sue was not in Rio on Aug. 18. (Not q.)

Therefore, Sue is not guilty. (Therefore, not p.)

6

6

Modus tollens: premises, conclusion

Common form (modus tollens):
If p, then q. (premise)
Not q. (premise)
Therefore not p. (conclusion)

A premise is a statement **presumed** true for purposes of an argument.

Modus tollens is **valid** in the sense that

- if you have an argument of this form in which the first two statements (the **premises**) are both true,
- then you can be 100% sure that the final statement (the **conclusion**) will be true.

7

7

Mathematical Communication

- Must be unambiguous
- Must express things so that everyone understands exactly what we are saying
- **Consequence:** Careful definitions are necessary

8

8

Statements

Statement: A declarative sentence that is either true or false but not both.

Example: Which of the following are statements?

- $1 + 1 = 2$ is a statement – true sentence
- $1 + 1 = 5$ is a statement – false sentence
- $1 + x = 5$ is not a statement; true for some x and false for others (this kind of sentence is called a "predicate").

9

9

Logical Connectives

Used to put simple statements together to make compound statements

not	~	*negation*
and, but	∧	*conjunction*
or (inclusive)	∨	*disjunction*
if-then	→	*conditional*
if-and-only-if	↔	*biconditional*

10

10

Precedence Rules

1. ~
2. ∨ and ∧ (with left-to-right precedence among these two operations, but better to use parentheses to avoid ambiguity instead of the left-to-right precedence)
3. → and ↔ (ditto)
4. Parentheses may be used to override rules 1-3

Example:

- ~ p ∧ q = (~p) ∧ q : check that this is not the same as ~(p ∧ q)
- p ∧ q ∨ r may be ambiguous. By left-to-right precedence, this is the same as (p ∧ q) ∨ r. Better to just specify whether (p ∧ q) ∨ r or p ∧ (q ∨ r) is intended.

Recall left-to-right precedence from arithmetic: $6/3 \times 9 = 18$ (not 0.5).

11

11

Logical connectives - examples

Let p be "It is winter", q be "It is cold", and r be "It is raining".
Write the following statements symbolically.

- It is winter but it is not cold = p ∧ ~q = p ∧ (~q)
- Neither is it winter nor is it cold = ~p ∧ ~q = (~p) ∧ (~q)
- It is not winter if it is not cold = ~q → ~p
- It is not winter but it is raining or it is cold = (~p ∧ r) ∨ q
- It is not winter but it is raining or cold = ~p ∧ (r ∨ q) ?

Note the use of left-to-right precedence in the second-last example above.

Note in the last example that the lack of separate subject and verb ("it is") with the clause "cold" may imply the different answer given.

12

12

Truth Values for Compound Statement Forms

- **Not Statements (Negations):** The negation of a statement is a statement that exactly expresses what it would mean for the given statement to be false.
- The negation of a statement has opposite truth value from the statement.

p	~p
T	F
F	T

13

13

Truth Table for ∨ ("inclusive or")

- Note how all possible combinations of veracity of the two component statements (independent variables) are considered in the first two columns of the truth table for logical **or**:

p	q	p ∨ q
T	T	T
T	F	T
F	T	T
F	F	F

- The only time an **or** statement is false is when both component statements are false – cf. De Morgan's laws on negating logical **or** statements:
  ~(p∨q) = ~p ∧ ~q

14

14

Truth Table for Λ ("and", "but")

p	**q**	**p Λq**
T	T	T
T	F	F
F	T	F
F	F	F

- The only time an **and** statement is true is when both components are true – again cf. De Morgan's law on negating logical **and** statements: **~(pΛq) = ~p ∨ ~q**

15

15

De Morgan's laws for negating Λ

p	q	p Λq	~(pΛq)	~p	~q	~p ∨ ~q
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

- Note how the ~(pΛq) and ~p ∨ ~q **columns are identical**, i.e., the two compound statements are logically equivalent).
- This proof that ~(pΛq) ≡ ~p ∨ ~q is **directly by taking all cases** (each case is a **row** of the truth table) on the veracity (truth values) of component statements p and q.

16

16

De Morgan's laws for negating ∨

- Exercise: repeat this for negating **or** statements, i.e., show $\sim(p \vee q) \equiv \sim p \wedge \sim q$

17

17

De Morgan's laws - examples

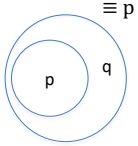
- Question: Write the negation of, "Sue left the door unlocked or she left the window open."
- Answer: "Sue locked the door and she closed the window."
- But is the negation of "Sue left the door unlocked" really "Sue locked the door"?
- Question: Write the negation of, "Hal got an A on the midterm and Hal got an A on the final exam."
- Answer: "Hal did **not** get an A on the midterm **or** Hal did **not** get an A on the final exam."

18

18

Truth Table for → (implies)

- The only time a statement of the form **if p then q** is false is when the hypothesis (**p**) is true and the conclusion (**q**) is false, i.e.,
  ~(p→q) ≡ p ∧ ~q (**Exercise:** check this by truth table)
- When the hypothesis of an if-then statement is false, we say that the if-then statement is "vacuously true" or "true by default." In other words, it is true because it is not false.
- p→q ≡ if p then q
  ≡ q if p
  ≡ p only if q
  ≡ q is a necessary condition for p
  ≡ p is a sufficient condition for q
  ≡ ~p or q



p	q	p → q
T	T	T
T	F	F
F	T	T
F	F	T

19

19

If-then Statements (Conditionals)

- **Imagine** that I promise you:
  "If you get an A on the final exam, then you will get an A in the course."
- Form of conditional: "If hypothesis, then conclusion", equivalently "hypothesis → conclusion".
- Jump forward to one week after the end of the semester. Finding out your final exam grade and your course grade, you exclaim: "He lied."
- What would have to be true to lead you to say that I lied?
- You would have to have earned an A on the final exam **and** not received an A for the course. In all other cases it would not be fair to say that I lied.
- Note: The example statement above is logically equivalent to
  "You get an A on the final exam only if you get an A in the course."

20

20

If-then statements (cont)

- Question: Write the negation of "If Jim got the right answer, then he solved the problem correctly."
- Answer: "Jim got the right answer **and** he did **not** solve the problem correctly."
- Note that one could use "**but**" instead of "**and**" in the answer.
- $\sim(p \rightarrow q) \equiv p \wedge \sim q$

21

21

If-and-Only-If (iff) Statements (Biconditionals)

- A statement of the form **p if and only if q** is true when both p and q have the same truth value (veracity).
- **p if and only if q** is false when p and q have opposite truth values.
- Exercise: Check by truth table that
  $p \leftrightarrow q \equiv (q \rightarrow p) \wedge (p \rightarrow q)$, i.e.,
  p if and only if q ≡ (p if q) and (p only if q)

p	q	p ↔ q
T	T	T
T	F	F
F	T	F
F	F	T

22

22

Some Potentially Ambiguous Terms

Or

- Example: As your prize, you may choose the TV **or** the microwave oven.
- Question: Is it to be understood that you can't choose both the TV and the microwave?
- Answer: YES. In this sentence, the intended meaning of "or" is called "exclusive or", i.e.,

  $p \oplus q$ = false when p=true and q=true.

If-then

- Example : **If** you eat your dinner, **then** you will get dessert.
- Question : Does this imply that if you don't eat your dinner, then you won't get dessert? In other words, does it mean that if you get dessert, you will have eaten your dinner?
- Answer: Mom wants you to think this, but it is not implied by the logical meaning of if-then.

23

23

Moral

- In ordinary speech, words like "or" and "if-then" may have multiple meanings,
- but in technical subjects, we must all understand words in the same way.
- So we choose one meaning for each word.

24

24

Compound Statement Forms

Example :

- p : DePaul University is in Chicago
- q : $1 + 1 = 5$
- r : Chicago is next to Lake Michigan

Question: Knowing that p is T, q is F and r is T, what is the truth value of the following compound statement?

$(p \wedge \sim q) \vee \sim r$

Answer: $(T \wedge \sim F) \vee \sim T = (T \wedge T) \vee F = T \vee F = T$

i.e., the answer is True.

Note how we followed precedence order.

25

25

Truth Table for Exclusive Or

- logical expression for a statement of the form p or q but not both:

  $(p \vee q) \wedge \sim(p \wedge q) \stackrel{\text{def}}{=} p \oplus q$

p	q	p∨q	p∧q	~(p ∧q)	(p ∨ q) ∧ ~(p ∧ q)
T	T	T	T	F	F
T	F	T	F	T	T
F	T	T	F	T	T
F	F	F	F	T	F

26

26

Arguments and Argument Forms

- **Argument**: Sequence of statements. The final statement in the sequence is the (final) **conclusion**; the preceding statements are **premises.** Some statements following the "initial" premises may themselves be conclusions, i.e., forming component arguments.
- **Argument Form**: Obtained by replacing component statements in the argument by variables.
- **Example (modus tollens)**:

If p then q.	(premise)
Not q.	(premise)
Therefore, not p.	(∴ conclusion)

27

27

Valid Arguments

- **Form of argument is valid when**: Every argument of that form that has true premises has a true conclusion. (A more formal version of the definition is in the book)
- **Claim:** Modus tollens is a valid form of argument.
- **Proof**: By last row of the following truth table, wherein both premises (columns 3 and 4) are true and (rightmost) column 5 is the true conclusion.

p	q	p→q	~q	~p
T	T	T	F	F
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

28

28

Invalid Arguments

- **A form of argument is invalid** if there is at least one argument of that form that has true premises and a false conclusion.
- **Example:** Determine whether the following argument form (with three premises) is valid or invalid:

  $\sim p \vee q$
  $p \rightarrow r$
  $q \rightarrow p$
  $\therefore r$

29

29

Valid or Invalid? Example (cont)

p	q	r	~p	~ p ∨q	p →r	q →p	r
T	T	T	F	T	T	T	T
T	T	F	F	T	F	T	F
T	F	T	F	F	T	T	T
T	F	F	F	F	F	T	F
F	T	T	T	T	T	F	T
F	T	F	T	T	T	F	F
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	F

- Only rows 1,7,8 are germane as all premises (cols. 5,6,7) are true just for those cases.
- The 8th (bottom) row shows that it is possible for an argument of this form to have true premises and a false conclusion (col. 8).
- So this form of argument is invalid.

30

30

More Valid and Invalid Forms of Argument

- **Modus ponens (valid)**:
  If Ted is a CS major, then Ted has to take CSC 211.
  Ted is a CS major.
  Therefore, Ted has to take CSC 211.

- **Form**: If p then q
  p
  ∴ q
- It is obviously not possible for the two premises to be true and the conclusion to be false, so this form of argument is valid.
- For a proof, see the first row of the truth table for p→q

31

31

Invalid Argument with a "Converse Error"

- **Example:**

If today is Easter, then it is Sunday.
It is Sunday.
Therefore, today is Easter.

- **Form**: If p then q
  q
  ∴p
- Exercise: Check by truth table that this is **not** a valid form of argument (3rd row of the truth table for p→q).
- The statement q→p is the converse of the statement p→q.
- The converse of a true statement may be true or false, so employing the converse as above results in an invalid argument.

32

32

Invalid Argument with an "Inverse Error"

- **Example:**

If Ted is a math major, then Ted has to take MAT 152.
Ted is not a math major.
Therefore, Ted does not have to take MAT 152.

- **Form**: If p then q
  ~p
  ∴ ~q
- Exercise: Check by truth table that this is **not** a valid form of argument.
- The statement ~p→~q is the inverse of the statement p→q.
- Again, if a statement is true its inverse may be true or false so employing the inverse as above results in an invalid argument.

33

33

"Sound Argument": Valid Argument with True Premises (and thus a true conclusion)

- An invalid argument may have a true conclusion and a valid argument (with a false premise) may have a false conclusion, though these definitions are often used interchangeably in ordinary speech.
- **The validity of the argument does not depend on the truth values of the premises.**
- **Example:** Invalid argument (converse error) with true conclusion.
  If Dick Cheney was vice president, then D.C. worked for Halliburton.
  D.C. worked for Halliburton.
  Therefore, D.C. was vice president.
- **Example:** Valid argument (modus ponens) with false conclusion.
  If all humans are mice then all mice are six feet tall.
  All humans are mice.
  Therefore, all mice are six feet tall.

34

34

Exercise: Spot the logical errors

Paraphrased from Monty Python and The Holy Grail:
Note: She **was** a witch in the end because she did weigh as much as a duck ((i.e., true conclusion though argument is invalid)

SIR BEDEMIR:
There are ways of telling whether she is a witch.
VILLAGER #1:
Are there?
BEDEMIR
Tell me. What do you do with witches?
CROWD:
Burn! Burn them up! Burn!...
BEDEMIR:
And what do you burn apart from witches?
VILLAGER #1:
Wood!
BEDEMIR:
So, why do witches burn?
VILLAGER #3:
B--... 'cause they're made of... wood?
BEDEMIR:
Good! So, how do we tell whether she's made of wood?
VILLAGER #1: Build a bridge out of her.
BEDEMIR:
Ah, but can you not also make bridges out of stone?
VILLAGER #1:
Oh, yeah.
BEDEMIR:
Does wood sink in water?
VILLAGER #2:
No, it floats! It floats!
BEDEMIR:
What also floats in water?
(Villagers don't know)
KING ARTHUR:
A duck!
BEDEMIR:
Exactly. So, logically...
VILLAGER #1:
If... she... weighs... the same as a duck,... she's made of wood.
BEDEMIR:
And therefore?
VILLAGER #2:
A witch!

35

35

Logical Equivalence: e.g., De Morgan

p	q	p ∧q	~(p∧q)	~p	~q	~p ∨ ~q
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

- Recall how the **~(p∧q)** and **~p** ∨ **~q** columns are identical, i.e., these two compound statements are logically equivalent.
- This proof that **~(p∧q)** ≡ **~p** ∨ **~q** is by **taking all cases** (**rows** of the truth table) on the veracity (truth values) of component statements p and q.

36

36

Definition of Logical Equivalence

- **Definition**: Two statement forms are **logically equivalent** if, and only if, it is impossible for one of them to be true and the other false.
- Logical equivalence makes it convenient to express statements in more than one way.
- The symbol for logical equivalence is ≡

37

37

De Morgan's Laws, Negation of "If *p* Then *q*"

- De Morgan's laws:
  $\sim(p \wedge q) \equiv \sim p \vee \sim q$, $\sim(p \vee q) \equiv \sim p \wedge \sim q$
- **Example:** The negation of
  $-4 < x \leq 7$ (read: $-4 < x$ and $x \leq 7$)
  is
  $-4 \geq x$ or $x > 7$.
- Negation of →: $\sim(p \rightarrow q) \equiv p \wedge \sim q$
- **Example:** The negation of
  If Tom is Ann's father, then Leo is her uncle.
  is
  Tom is Ann's father and Leo is not her uncle.
- So, by De Morgan, $p \rightarrow q \equiv \sim(p \wedge \sim q) \equiv \sim p \vee q$ and recall how $p \rightarrow q$ is vacuously true.

38

38

Contrapositive, Converse, Inverse of $p \rightarrow q$

For the conditional statement "if p then q":

- the **converse** is: if q then p
- the **contrapositive** is: if not q then not p
- the **inverse** is: if not p then not q.

39

39

Example – Converse, Inverse and Contrapositive

Conditional Statement: If Sam lives in Chicago then Sam lives in Illinois.

Converse: If Sam lives in Illinois, then Sam lives in Chicago.

Contrapositive: If Sam does not live in Illinois, then Sam does not live in Chicago.

Inverse: If Sam does not live in Chicago, then Sam does not live in Illinois.

40

40

Which are Logically Equivalent?

- $p \rightarrow q \equiv \sim q \rightarrow \sim p$ (conditional statement **is** logically equivalent to its contrapositive, recall modus tollens)
- $p \rightarrow q \not\equiv q \rightarrow p$ (conditional statement is **not** logically equivalent to its converse)
- $p \rightarrow q \not\equiv \sim p \rightarrow \sim q$ (conditional statement is **not** logically equivalent to its inverse)
- inverse is contrapositive of converse, so inverse and converse are logically equivalent: $q \rightarrow p \equiv \sim p \rightarrow \sim q$
- Proof by truth table (directly by exhaustive cases):

p	q	~q	~p	p → q	~q → ~p	q → p	~p → ~ q
T	T	F	F	T	T	T	T
T	F	T	F	F	F	T	T
F	T	F	T	T	T	F	F
F	F	T	T	T	T	T	T

41

41

Converse (of an if-then statement)

- Note from the truth table that "$p \rightarrow q$" true does not imply that its converse "$q \rightarrow p$" is true, i.e., its converse may be true or false.
- That is, the converse of a true conditional (if-then) statement is not necessarily true.
- On the other hand, when "$p \rightarrow q$" is false (i.e., p and ~q are true), the converse "$q \rightarrow p$" is (vacuously) true.

p	q	~q	~p	p → q	~q → ~p	q → p	~p → ~ q
T	T	F	F	T	T	T	T
T	F	T	F	F	F	T	T
F	T	F	T	T	T	F	F
F	F	T	T	T	T	T	T

42

42

Sets

- **Set Notation:** $x \in A$ means that "x is an element of the set A," or "x is in A."
- **Important sets of real numbers:**

  $\mathbb{R}$, the set of all real numbers

  $\mathbb{Q}$, the set of all rational numbers

  $\mathbb{Z}$, the set of all integers

  $\mathbb{R}^{>0}$, the set of all strictly positive real numbers

  $\mathbb{Z}^{\geq 0} = \mathbb{W}$, the set of all nonnegative integers (whole numbers)

  $\mathbb{Z}^{>0} = \mathbb{N}$, the set of all strictly positive integers (natural numbers), sometime also denoted $\mathbb{Z}^{+}$

  etc.

43

43

Quantified Statements

- A **predicate** is a sentence that is not a statement but contains one or more variables and becomes a statement if specific values are substituted for the variables.
- The **domain of a predicate variable** is the set of allowable values for the variable.
- **Example:** Let P(x) be the sentence "$x^2 > 4$" where the domain of x is understood to be the set of all real numbers. Then P(x) is a predicate.
- **Question:** For what numbers x is P(x) true?

  Answer: The set of all real numbers for which $x > 2$ or $x < -2$.

44

44

Truth Set of a Predicate

- The **truth set of a predicate** P(x) is the set of elements in the domain D of x for which P(x) is true.
- We write truth set of P(x) as
  $\{x \in D \mid P(x)\}$
  and we read this as "the set of all x in D such that P of x."
- Note: The vertical line denotes the words "such that" for the set-bracket notation only.
- The words "such that" may also be symbolized by "s.t." or "s. th." or "∋" or ":"

45

45

Truth set of a predicate - example

- Let P(x) be the predicate "$x^2 < x$", with domain the set $\mathbb{R}$ of all real numbers.
- Which of the *statements* P(0), P(1/2), P(2) and P(-3) are true and which are false?
- What is the truth set of P(x)?

P(0):	$0^2 < 0$	FALSE
P(1/2):	$(½)^2 < ½$	TRUE
P(2):	$2^2 < 2$	FALSE
P(-3):	$(-3)^2 < -3$	FALSE

Truth set = $\{x \in \mathbb{R} \mid 0 < x < 1\}$

46

46

Universal Quantification ∀

- The symbol ∀, standing for the words "for all" is called the **universal quantifier.**
- **Question**: Rephrase the following universal statement in less formal language.

  ∀ MAT 140 students *x*, *x* has studied calculus.
- **Answers:**
  - All MAT 140 students have studied calculus.
  - Every MAT 140 student has studied calculus.
  - If a person is a MAT 140 student, then that person has studied calculus.
  - etc.

47

47

Definition of Counterexample

- **Definition**: Given a universal statement of the form "∀x ∈ D, P(x)", a **counterexample** for the statement is a value of x ∈ D for which P(x) is false.
- Note that: ∀x ∈ D, P(x) ≡ ∀x, x ∈ D ⇒ P(x) where the context is that x may belong to some superset containing D (⇒ is "implies" for predicates).
- Also note that "∀x ∈ D, P(x)" is a statement if D is disclosed or understood, otherwise it's a predicate with variable D.
- **Example**: True or false?

  ∀ MAT 140 students x, x has studied calculus.
- **Answer:** The statement is false because you happen to know that Fred is a counterexample to the statement, i.e., because Fred is a MAT 140 student and Fred has **not** studied calculus.

48

48

Existential Quantification ∃

- The symbol ∃, standing for the words "there exists", is called the **existential quantifier**
- **Example**: Rephrase the following existential statement in less formal language, and determine whether it is true or false.

  ∃ a MAT 140 student *x* such that *x* has studied calculus.
- **Answers:**
  - There is a MAT 140 student who has studied calculus.
  - Some MAT 140 student has studied calculus.
  - Some MAT 140 students have studied calculus.
  - At least one MAT 140 student has studied calculus.
  - etc.

49

49

Truth Values of Universal and Existential Statements, and their negations

- **Universal statement:** "**∀x ∈ D, Q(x)**" is **true** if, and only if, Q(x) is true for each individual x ∈ D.
- It is **false** if, and only if, Q(x) is false for at least one x ∈ D.
- A value of x for which Q(x) is false is called a **counterexample** to the statement "∀ x ∈ D, Q(x)".
- So, ∼(**∀x ∈ D, Q(x)**) ≡ **∃x ∈ D such that ∼Q(x)**

- **Existential statement:** "**∃ x ∈ D such that Q(x)**" is **true** if, and only if, Q(x) is true for at least one x ∈ D.
- It is **false** if, and only if, Q(x) is false for each individual x ∈ D.
- So, ∼(**∃x ∈ D such that Q(x)**) ≡ **∀x ∈ D, ∼Q(x)**

50

50

Universal/Existential Statement Examples

- Determine whether the following statements are true and rewrite them formally using a quantifier and a variable:

- All even integers are positive.
  - False: -2 is a counterexample; it is even but not positive.
  - ∀ even integers n, n is positive.
  - ∀ integers n, if n is even then n is positive.
  - ∀ n, if n is an even integer then n is positive.
  - Note in the previous answer, there is an implied superset of the even integers to which n belongs

- Some integers have integer square roots.
  - True: The number 4 has a square root of 2, which is an integer.
  - ∃ an integer x such that x has an integer square root.
  - ∃ x such that x is an integer and x has an integer square root.

51

51

Universal/Existential Statement Examples

- Indicate, if possible, which of the following statements are true and which are false, and rewrite them formally using a quantifier and a variable:

- No prime numbers are even.
  - False: The number 2 is even and prime.
  - ∀ prime numbers p, p is not even.
  - ∀ integers p, if p is prime then p is not even.
  - Note that the integers are a superset of the primes.

- If a person is a student in MAT 140, then that person is at least 18 years old.
  - True?
  - ∀ students P in MAT 140, P is at least 18 years old.
  - ∀ people P, if P is a student in MAT 140 then P is at least 18 years old.
  - Note that people are a superset of students.

52

52

Negating Quantified Statements - Examples

1. ∀ students x in MAT 140, x is at least 30 years old.

Negation: ∃ a student x in MAT 140 such that x is less than 30 years old.

2. ∃ a student x in MAT 140 such that x is at least 70 years old.

Negation: ∀ students x in MAT 140, x is less than 70 years old.

53

53

Negating Quantified Statements - Examples

3. ∀ real numbers x, $x^2 > 0$.
Negation: ∃ a real number x such that $x^2 \leq 0$.

4. ∃ a real number x such that $x^2 = -1$.
Negation: ∀ real numbers x, $x^2 \neq -1$.

Note that the original statement in both examples above happens to be false.

54

54

Negating Quantified Statements and De Morgan's Laws

- In Summary:

$\sim(\forall x \in D, Q(x)) \equiv \exists x \in D$ such that $\sim Q(x)$ … i.e., a counterexample

$\sim(\exists x \in D$ such that $Q(x)) \equiv \forall x \in D, \sim Q(x)$

- But these are just De Morgan's laws on the (potentially uncountably infinite) set D, because we have the following logical equivalents:

  $\forall x \in D, Q(x) \equiv \bigwedge_{x \in D} Q(x)$

  $\exists x \in D$ such that $Q(x) \equiv \bigvee_{x \in D} Q(x)$

- For example, if the set D={a,b,c} (has three elements), then

  $\forall x \in D, Q(x) \equiv Q(a) \wedge Q(b) \wedge Q(c)$

  $\exists x \in D$ such that $Q(x) \equiv Q(a) \vee Q(b) \vee Q(c)$

- So by De Morgan, $\sim(\forall x \in D, Q(x)) \equiv \bigvee_{x \in D} \sim Q(x)$

55

55

Universal Conditional Statements

- Definition: Any statement of the following form is called a universal conditional statement:

  $\forall x \in D$, if $P(x)$ then $Q(x)$

- Equivalent notation for if-then statements involving predicates:

  $\forall x \in D, \ P(x) \Rightarrow Q(x)$

  i.e., $\Rightarrow$ means "implies" for predicates.

56

56

Universal Conditional Statement - Example

- $\forall x \in \mathbb{R}, x > 2 \Rightarrow x^2 > 4$.
- Read: For all x in the set of real numbers, if x is greater than 2 then x-squared is greater than 4.
- Less formal versions:
  - All real numbers that are greater than 2 have squares that are greater than 4.
  - If a real number is greater than 2, then its square is greater than 4.

57

57

Disproving a Universal Statement

Common Method: Find a counterexample!

Example:

- Is the following statement true or false? Explain.
  $\forall x \in \mathbb{R}$, if $x^2 > 25$ then $x > 5$.

- **Solution:**
  - Let $x = -6$. Then $x^2 = (-6)^2 = 36$, and $36 > -6$ but $-6 \leq 5$.
  - So (for this x), $x^2 > 25$ and $x \leq 5$.
  - So, the statement is false by counterexample.

58

58

Negate a universal-conditional statement

- $\sim(\forall x \in D, \text{if } P(x) \text{ then } Q(x)) \equiv \exists x \in D \text{ s.t. } P(x) \wedge \sim Q(x)$
- Example: Write a negation for the following statement
  $\forall x \in \mathbb{R}$, if $x^2 > 4$ then $x > 2$.
- Negation:
  $\exists x \in \mathbb{R}$ s.t. $x^2 > 4$ and $x \leq 2$.
- Note that the fact that the negation is true (and original statement is false) is immaterial to what is being asked.

59

59

Example: Vacuous truth

- Suppose that: **There are no elephants on this desk**.
- Is the following statement True or False?
  All the elephants on this desk have two heads. (*)
- The negation of this statement is:
  There is an elephant on this desk without two heads.
  which is clearly false.
- So, the original statement (*) has to be true!
- This is another example of "vacuous truth" or "truth by default" because it involves an empty-set quantifier:
  $\forall x \in \{\text{elephants on this desk}\}$, x has two heads,
  where the set of elephants on the desk is empty.
- This is related vacuous truth of $p \rightarrow q$ when the premise statement p is false; for predicate statements we write,
  $x \in \{\text{elephants on this desk}\} \Rightarrow$ x has two heads

60

60

Arguments with Quantified Statements

- Universal instantiation: If a property is true for all the elements in a set, then it is true for each individual element of the set.
- Example (multiplication distributes over addition):

  $\forall$ a,b,c $\in \mathbb{R}$, $a(b + c) = ab + ac$.

Thus: $7 \cdot 106 = 7(100+6) = 7 \cdot 100 + 7 \cdot 6 = 742$

And: If $k \in \mathbb{R}$, then $2^k \cdot 3 + 2^k \cdot 5 = 2^k \cdot (3 + 5)$ $\quad (= 2^k \cdot 8 = 2^k \cdot 2^3 = 2^{k+3})$

61

61

Universal Modus Ponens and Modus Tollens

- Example universal fact (true statement)
  All humans are mortal.
- Equivalently,
  $\forall$x, if x is human then x is mortal.
- x is implicitly in the superset of elements for which mortality or immortality are attributes, i.e., a superset of living beings including gods, but not inanimate objects like rocks.
- By universal instantiation the following is true:
  If Socrates is human, then Socrates is mortal.
- So we can argue (modus ponens):
  Socrates is human. $\therefore$ Socrates is mortal.
- By universal instantiation, the following is true:
  If Zeus is human then Zeus is mortal.
- So we can argue (modus tollens):
  Zeus is not mortal. $\therefore$ Zeus is not human.

62

62

Necessary and Sufficient Conditions

Example: What do the following sentences mean?

- Passing all the tests is a sufficient condition for Jon to pass the course.

  Answer: If Jon passes all the tests, then Jon will pass the course.

- Passing all the tests is a necessary condition for Jon to pass the course.

  Answer: If Jon doesn't pass all the tests, then Jon won't pass the course.

  Or: If Jon passes the course, then Jon will have passed all the tests.
- Note that replacing "sufficient" with "necessary" creates a converse statement.

63

63

Necessary and sufficient conditions - Definitions

- **A is a sufficient condition for B**
  - means **if A then B.**
  - i.e., the occurrence of A implies/guarantees the occurrence of B.
- **A is a necessary condition for B**
  - means **if ~A then ~B.**
  - i.e., if A didn't occur, then B didn't occur either.
  - Or, equivalently, it means the contrapositive, **if B then A.**
  - i.e., if B occurred then A also had to occur.

64

64

Necessary and sufficient conditions - Examples

Write each of the following using if-then statements:

1. Being at least 35 years old is a necessary condition for Ann to become president of the U.S.

If Ann is less than 35 years old, then Ann cannot become president of the U.S.

If Ann becomes president of the U.S., then Ann is at least 35 years old.

2. Being appropriately dressed for a job interview is necessary (but not sufficient) for Tom to get the job.

If Tom is not appropriately dressed for a job interview, then Tom won't get the job, but it can happen that Tom is appropriately dressed and still doesn't get the job.

65

65

Necessary and sufficient conditions – Examples (cont)

3. Getting all A's is sufficient (but not necessary) for Sue to graduate with honors.

If Sue gets all A's then she will graduate with honors, but it's possible for Sue to graduate with honors even if she doesn't get all A's.

4. Suppose a teacher says: Getting 100% correct on all the exams is both necessary and sufficient for you to earn an A in the course. What does this mean?

If you earn an A in the course, then you got 100% correct on all the exams, and if you got 100% correct on all the exams, then you got an A in the course.

66

66

Only if and the Biconditional

Example: Cinderella's stepmother makes the following statement. Write it as an if-then statement:

You have permission to go to the ball only if you finish all your work.

Answer:
If you do not finish all your work, then you do not have permission to go to the ball.

Or: If you have permission to go to the ball, then you will have finished all your work.

67

67

Definition: Only If

- **r only if s** means **if ~s then ~r**
- That is, if s didn't occur, then r didn't occur either.
- Or, equivalently, the contrapositive, **if r then s**
- That is, if r is true then s also has to be true.

68

68

Interpretation of If and Only If

- So, **r only if s** means **if r then s**
- and **r if s** means **if s then r** (the converse of: **if r then s**)
- Thus, **r if and only if s**
  - Means **r only if s** and **r if s**
  - Which means **if r then s** and **if s then r**
- Symbolically,
  $r \leftrightarrow s \equiv (r \rightarrow s) \wedge (s \rightarrow r) \equiv s \leftrightarrow r$
  - $\equiv$ r is a necessary and sufficient condition for s
  - $\equiv$ s is a necessary and sufficient condition for r
- Example:

An employee is a non-profit college's football coach if and only if they are the highest paid employee of their non-profit college.

r= "employee is football coach of non-profit college"

s = "employee is highest paid in non-profit college"

69

69

Introduction to Discrete Mathematics

Introduction to Methods of Proof

© S.S. Epp (2006)
This revision © G. Kesidis (2013)
This document revision is copy-left 2013.
It is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License

70

70

Intro to Methods of Proof - Outline

- Direct proof and counterexample
  - Introduction
  - Examples with Rational Numbers
  - Examples on Divisibility
  - Method of Division into Cases
  - Examples with Floor and Ceiling Operators
- Indirect Arguments: contradiction and contraposition
- Examples: $\sqrt{2}$ is irrational, and that there are infinitely many primes

71

71

Elementary Number Theory and Methods of Proof

Assumptions:

- Knowledge of properties of the real numbers (Appendix A), "basic" algebra, and logic
- Properties of equality:

  $A = A$ (= is reflexive)

  If $A = B$, then $B = A$. (= is commutative)

  If $A = B$ and $B = C$, then $A = C$. (= is transitive)
- Integers $\mathbb{Z} = \{0, 1, 2, 3, \ldots, -1, -2, -3, \ldots\}$
  $= \{\ldots -3,-2,-1,0,1,2,3,\ldots\}$
- Any sum, difference, or product of integers is an integer.

72

72

Definition of Even and Odd

- An integer is **even** ↔ it can be expressed as 2 times some integer.
- An integer is **odd** ↔ it can be expressed as 2 times some integer plus 1.

Clarifying the role of ↔ (if and only if) in these definitions:

- If an integer, say n, is even then there is an integer k such that n=2k.

AND the converse,

- If an integer, say n, can be expressed as 2k, for some integer k, then n is even.

Yes!

73

73

Exercise

- **Question:** If k is an integer, is 2k – 1 an odd integer?
- Reference fact/definition: An integer is **odd** ↔ it can be expressed as 2 times some integer plus 1.
- Also can use basic facts, e.g. re. arithmetic with integers.
- Answer: Yes (so the above Question is a Lemma).
- Explanation/Proof:
  - Note that k – 1 is an integer because it is a difference of integers.
  - And $2(k-1)+1 = 2k-2+1 = 2k-1$
  - Q.E.D.

74

74

Exercise

- Some people say that an integer is even if it equals 2k. Are they right?
- Is 1 an even number?
- Does $1 = 2k$?
- Yes: $1 = 2(0.5)$
- So it's pretty important that "some people" require k to be an integer (thereby precluding k=0.5),
- otherwise we have a disproof of what "some people say" by counter-example, i.e., take k=0.5.

75

75

Directly Proving a Universal Statement

- **Method of Generalizing from the Generic Particular:** If a property can be shown to be true for a particular but arbitrarily chosen element of a set, then it is true for every element of the set.
- **Theorem:** Pick a (finite!) number. Add 3. Multiply by 6. Subtract 10. Divide by 2. Subtract 3 times the original number to arrive at your final answer, which is always 4.
- **Proof:** Consider particular but arbitrary finite number x. The final answer is
  $(6(x+3)-10)/2 - 3x = 3(x+3) - 5 - 3x$
  $= 3x + 9 - 5 - 3x$
  $= 4.$ Q.E.D.
- Note that the elementary arithmetic operations in the proof hold for and arbitrary number x!

76

76

Direct Proving a Universal Statement Over a Finite Set

- **Method of Exhaustion**: If a theorem statement concerns elements of a finite set, then this method proves the theorem separately for each element of the set.
- Note that our proofs of logical equivalence by truth table were exhaustive: checking the equivalence for every combination of truth-values of the independent variables.
- **Theorem:** Prove that every even integer from 2 through 10 can be expressed as a sum of at most 3 perfect squares.
- **Proof:**

$2 = 1^2 + 1^2$

$4 = 2^2$

$6 = 2^2 + 1^2 + 1^2$

$8 = 2^2 + 2^2$

$10 = 3^2 + 1^2$ Q.E.D.

77

77

Direct Proof - Example

- **Question**: Is the sum of an even integer plus an odd integer always even? always odd? sometimes even and sometimes odd?
- **Theorem:** $\forall$ x,y $\in \mathbb{Z}$, if x is even and y is odd, then x + y is odd.
- **Proof:** Take particular but arbitrary x,y $\in \mathbb{Z}$. By hypothesis, there are k,i $\in \mathbb{Z}$ such that x=2k and y=2i+1. Thus, x+y = 2k + 2i+1 = 2(k+i)+1 which is odd because k+i $\in \mathbb{Z}$ ($\mathbb{Z}$ is closed under addition). Q.E.D.
- Note that an exhaustive proof would not work because the integers $\mathbb{Z}$ is not a finite set.

78

78

Direct proof generalizing from the generic particular: form

Theorem:

∀ x in D, if <hypothesis> then <conclusion>

Proof:

- suppose x is a particular but arbitrarily chosen element in D such that <hypothesis> is true, and
- show that <conclusion> is true for x (not relying on anything about x the fact that x∈D).
- Q.E.D. (quod erat demonstrandum, i.e., "which was to be shown).

79

79

Directions for Writing Proofs

1. Copy the statement of the theorem to be proved onto your paper (except on exams!).
2. Clearly mark the beginning of your proof with the word "Proof:".
3. Write your proof in complete sentences.
4. Make your proof self-contained. (E.g., introduce all variables, but do not rename variables already defined there!)
5. Give a reason for each assertion in your proof.
6. Include the "little words" that make the logic of your arguments clear. (E.g., then, thus, therefore, so, hence, because, since, Notice that, etc.)
7. Make use of definitions but do not include them verbatim in the body of your proof.

80

80

Common Proof-Writing Mistakes

1. Arguing from non-arbitrary examples.

2. Using the same letter to mean two different things or two different variables to mean the same thing.

3. Jumping to a conclusion.

4. Begging the question.

5. Misuse of the word "if."

81

81

Rational Numbers

- **Definition**: A real number is **rational** if, and only if, it can be written as a ratio of integers with a nonzero denominator.
- That is: $r \in \mathbb{Q} \Leftrightarrow \exists\ a,b \in \mathbb{Z}$ such that $r = a/b$ and $b \neq 0$.
- (*) Numbers with finite or repeating decimal expansions are rational.
- For example,
  $43.205 = 43205/1000$
  $2.3333\ldots = 7/3$
  $-1.2 = (-6)/5 = 6/(-5)$
  $0 = 0/1$
  $21.34343434\ldots =: x$ where $100x - x = 2134 - 21$
  so $x = (2134-21)/99$
- These examples do not form a proof of (*).
- **Exercise:** But the ideas for the proof are there…

82

82

Example: $\mathbb{Q}$ closed under addition

- **Simple Fact (Zero Product Property):** If any two nonzero real numbers are multiplied, the product is nonzero.
- **Theorem:** If m, n $\in \mathbb{Z}^{\neq 0}$ (are nonzero integers), then $(n/m) + (m/n) \in \mathbb{Q}$ (is rational).
- **Proof:**
  - By expressing with a common denominator (nm), we get that $(m/n) + (n/m) = (m^2+n^2)/(nm)$, where:
  - m^2+n^2 and $mn \in \mathbb{Z}$ (since integers are closed under both multiplication and addition) and
  - $mn \neq 0$ by the above simple fact.
  - Q.E.D.
- Exercise: Prove $\mathbb{Q}$ is closed under addition and multiplication.

83

83

Disproof of a universal statement by counter- example

Theorem: The rationals are not closed under division.

Proof:

- Note that we need to prove the following statement is false:
  $\forall x,y \in \mathbb{Q}, x/y \in \mathbb{Q}$
- Equivalently that the following statement is true:
  $\sim(\forall x,y \in \mathbb{Q}, x/y \in \mathbb{Q}) \equiv \exists x,y \in \mathbb{Q}$ s.t. $x/y \notin \mathbb{Q}$
- Consider the rational numbers $x=1=1/1$ and $y=0=0/1$.
- Their quotient $x/y = 1/0$ is not rational (not even real).
- Q.E.D.

84

84

Note regarding the last example

- Read the theorem statement carefully and don't confuse definitions.
- The previous theorem involves a quotient of rational numbers, not (directly) a quotient of integers (as factors in the definition of a rational number).
- Also note that the theorem statement needs its conditions because the quotient of any two real numbers, e.g., $2^{0.5}/3$, is obviously not rational.

85

85

Divisibility

Definition: Given any integers n and $d \neq 0$, the following statements are equivalent.

- n **is divisible by** d
- n **is a multiple of** d
- d **is a factor of** n
- d **is a divisor of** n
- d **divides** n
- $d \mid n$
- n equals d times some integer
- $\exists\, k \in \mathbb{Z}$ such that $n = dk$.

86

86

Examples

1. Is 18 divisible by 6?
Answer: Yes, $18 = 6 \cdot 3$.

2. Does 3 divide 15?
Answer: Yes, $15 = 3 \cdot 5$.

3. Does $5 \mid 30$?
Answer: Yes, $30 = 5 \cdot 6$.

4. Is 32 a multiple of 8?
Answer: Yes, $32 = 8 \cdot 4$.

5. If k is any integer, does k divide 0?
Answer: Yes, $0 = k \cdot 0$, except $0 \nmid 0$.

87

87

Examples (cont)

- **Fact:** If a and b are positive integers and $a \mid b$, then $a \leq b$.

6. Which integers divide 1?

Answer: Only 1 and -1.

7. If m and n are integers, is $10m + 25n$ divisible by 5?

Answer: Yes. $10m + 25n = 5(2m + 5n)$ and $2m + 5n$ is an integer because it is a sum of products of integers (the set of integers is closed under sums and products).

88

88

Divisibility stated formally

n is divisible by d (d≠0) implies d divides n:

$d \mid n \Rightarrow \exists\, k \in \mathbb{Z}$ such that $n = dk$.

The contrapositive of this statement is: ∀ k

$\forall k \in \mathbb{Z}, n \neq dk \Rightarrow d \nmid n$

Example: Does 5 | 12?

Solution: No because 12/5 is not an integer.

Note:

- 12/5 is a **number**: (twelfth fifths) =2 .4
- 5 | 12 is a **statement**: "5 divides 12".

89

89

Divisibility is transitive

Theorem: ∀ a, b, c ∈ ℤ, if a | b and b | c then a | c.

Proof:

- Take arbitrary a, b, c ∈ℤ such that a | b and b | c .
- So, ∃n,m ∈ℤ such that b=na and c=mb.
- By substitution, c=m(na)=(mn)a, where the second equality is the associative property of multiplication of real numbers.
- Since the integers are closed under multiplication, mn ∈ℤ.
- So, a|c.
- Q.E.D.

90

90

Disproof of a universal statement by counter-example

Theorem: The following statement is false:
$\forall a,b \in \mathbb{Z}$, if $a \mid b^2$ then $a \mid b$.

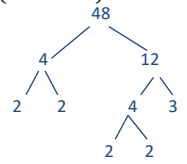
Proof:
- We are required to prove that the following statement is true:
  $\sim(\forall a,b \in \mathbb{Z}$, if $a \mid b^2$ then $a \mid b)$
  $\equiv \exists a,b \in \mathbb{Z}$ s.t. $a \mid b^2$ and $a \nmid b$
- For a=20 and b=10, clearly:
- $20,10 \in \mathbb{Z}$
- $20 \mid 10^2$ where $10^2=100$
- $20 \nmid 10$
- Q.E.D.

91

91

Prime and Composite Numbers

- **Definition**: An integer n is **prime** if, and only if, $n > 1$ and the only positive factors of n are 1 and n.
- **Definition:** An integer n is **composite** if, and only if, $n > 1$ and $n = r\,s$ for some positive integers r and s where neither r nor s is 1.
- **Note:** An integer n is **composite** if, and only if, $n > 1$ and $n = r\,s$ for some positive integers r and s where $1 < r < n$ and $1 < s < n$.
- Also, an integer $n>1$ is either prime or composite.
- **Theorem (Divisibility by a Prime):** Given any integer $n > 1$, there is a prime number p so that $p \mid n$.
- Recalling that divisibility is transitive: Tracing down any branch of a binary **factor tree** leads to a prime factor (at the leaf) of the number (at the root), e.g.,



92

92

Unique Factorization Theorem (*a.k.a. Fundamental Theorem of Arithmetic*)

- **Unique Factorization Theorem for the Integers:** Given any integer $n > 1$, either n is prime or n can be written as a product of prime numbers in a way that is unique, except, possibly, for the order in which the numbers are written
- **Ex. 1**: $500 = 5 \times 100 = 5 \times 25 \times 4 = 5 \times 5 \times 5 \times 2 \times 2 = 2 \times 5 \times 5 \times 2 \times 5 = 2^2 5^3$ **(standard factored form)**
- **Ex. 2**: $500^3 = (2^2 5^3)^3 = (2^2 5^3)(2^2 5^3)(2^2 5^3) = 2^6 5^9$
- **Note**: If 1 were prime, then prime factorizations would not be unique. For instance, $10 = 2 \times 5 = 1 \times 2 \times 5 = 1 \times 1 \times 2 \times 5$.
- **Note:** the previous theorem simply implied by (a corollary of) the UFT.

93

93

Example re. $8! = 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$

Ex. 3: How many 0's are at the end of 8! ?

Solution:

- $8! = 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 2^3 \times 7 \times (2 \times 3) \times 5 \times (2 \times 2) \times 3 \times 2 = 2^7 \times 3^2 \times 5 \times 7$
- Each factor of 10 gives rise to one zero at the end of a number.
- $10 = 2 \times 5$.
- The factorization of 8! contains only one pair 2×5.
- So the answer is that there is only one zero at the end of 8!

94

94

Quotient-Remainder Theorem

- Example: Suppose 14 objects are divided into groups of 3?
- That is: xxx xxx xxx xxx xx
- The result is 4 groups of 3 each with 2 left over.
- We write $14 = 4 \times 3 + 2$ where
  - 4 is the quotient and
  - 2 is the remainder (the remainder is always nonnegative and less than the divisor, 3).
- Equivalently, $14/3 = 4 + 2/3$
- And by long division:

$$\begin{array}{r} 4 \leftarrow \text{quotient} \\ \text{divisor} \rightarrow 3\overline{)\,14} \leftarrow \text{dividend} \\ \underline{-12} \\ 2 \leftarrow \text{remainder} \end{array}$$

95

95

Quotient-Remainder Theorem

- For all integers n and **positive** integers d, there exist unique integers q and r such that

$$n = dq + r \quad \textbf{and} \quad 0 \le r < d.$$

- **Ex**: Find q and r if $n = 23$ and $d = 6$.

Answer: $q = 3$ and $r = 5$

- **Ex**: Find q and r if $n = -23$ and $d = 6$.

Answer: $q = -4$ and $r = 1$

96

96

Consequences: every integer is either even or odd

- Applying the quotient-remainder theorem with d = 2 gives that there exist unique integers q and r such that

$$n = 2q + r \quad \text{and} \quad 0 \le r < 2.$$

- What are possible values for r ?

Answer: $r = 0$ or $r = 1$

- **Consequence**: No matter what integer you start with, it either equals

$2q + 0\ (= 2q)$ or $2q + 1$ for some integer q .

- **So:** Every integer is either even or odd.

97

97

Consequence: dividing by 3

- Similarly: Given any integer n, apply the quotient-remainder theorem with d = 3. The result is that there exist unique integers q and r such that

$$n = 3q + r \quad \text{and} \quad 0 \le r < 3.$$

- What are possible values for r ?

Answer: $r = 0$ or $r = 1$ or $r = 2$

- **Consequence**: Given any integer n, there is an integer q so that n can be written in one of the following three forms:

$n = 3q, n = 3q + 1, \quad n = 3q + 2.$

- Similarly for other values of integer divisors d>0: one can define d different groups of integers based on their remainders after dividing by d, cf. equivalence classes.

98

98

Example Direct Proof by Division into Cases

Theorem: Given any integer n, there is an integer k so that $n^2 = 3k$ or $n^2 = 3k + 1$.

Outline of Proof:

- Suppose n is **any** integer.
- By the quotient-remainder theorem with $d = 3$, there is an integer q so that

  $n = 3q$ OR $n = 3q + 1$ OR $n = 3q + 2$.
- We will show that regardless of which of these happens to be the case, the conclusion of the theorem follows.
- Case 1, $n = 3q$ for some integer q: (exercise: fill in)
- Case 2, $n = 3q + 1$ for some integer q: (exercise: fill in)
- Case 3, $n = 3q + 2$ for some integer q: (exercise: fill in)
- Hence, in every case there exists an integer k so that $n^2 = 3k$ or $n^2 = 3k + 1$.
- Q.E.D.

99

99

Example Direct Proof by Division into Cases (cont)

How would we fill in Case 2, for example?

- If $n = 3q + 1$ for some integer q, then

  $n^2 = (3q + 1)^2$ by substitution

  $= (3q + 1)(3q + 1)$

  $= 9q^2 + 6q + 1$

  $= 3(3q^2 + 2q) + 1$.
- Let $k = 3q^2 + 2q$.
- k is an integer because it is a sum of products of integers.
- Thus there is an integer k such that $n^2 = 3k + 1$.

100

100

Proof by Division into Cases

- How do you prove: If A **or** B is true then C is also true.
- **Technique:** Prove if A is true then C is true **and** if B is true then C is true.
- This is a correct form of argument because

  $(A \vee B) \rightarrow C \equiv (A \rightarrow C) \wedge (B \rightarrow C)$
- **Exercise:** check this by truth table, i.e., that this form of proof is valid. Also, draw the related Venn diagram.
- Some significant thought may be required to divide the statement $A \vee B$ into the cases (here A, B) which result in the simplest proofs for each case ($A \rightarrow C$, $B \rightarrow C$).
- Obviously, more than two cases may be in play and each case may have sub-cases, and each sub-case have sub-sub-cases, etc.
- **Example:** All proofs of logical equivalence by truth table employ division into cases, where each case corresponds to a row in our table format.

101

101

Theorem: $\forall n \in \mathbb{Z}$, if $n > 1$ then $\exists$ prime p s.t. p|n.

Idea of Proof:

- Suppose n is an arbitrary integer such that $n > 1$. Take two cases.
- If n is prime, we are done (since n | n).
- If not (i.e., if n is composite), then by def'n $n = r\,s$ for some integers r and s satisfying

  $1 < r < n$ and $1 < s < n$.
- If either r or s is prime, we are done.
- If not, $r = r_1 s_1$, where r_1 and s_1 are integers with

  $1 < r_1 < r$ and $1 < s_1 < r$.
- If either r_1 or s_1 is prime, we are done (as these are factors of n by transitivity of divisibility).
- If not, repeat with r_1 in place of r. Etc.
- This process must eventually terminate at a prime factor of n because: each successive factor is a positive factor of n (transitivity of divisibility) and $n < \infty$ so that there are only a finite number of successively strictly smaller factors r (all >1 by definition).
- Q.E.D.

102

102

Floor and Ceiling - mapping Reals to integers

- **Definition:** Given any real number x, the floor of x, denoted ⌊x⌋ (or [x]), is the unique integer n such that

  $n \leq x < n + 1$.
- **Definition:** The ceiling of x, denoted ⌈x⌉, is the unique integer n such that

  $n - 1 < x \leq n$.
- Examples: $\lfloor 2.8 \rfloor = 2$; $\lceil 2.8 \rceil = 3$; $\lfloor -2.8 \rfloor = -3$; $\lceil -2.8 \rceil = -2$
- **Lemma:** For all integers k, $\lfloor k + 1/2 \rfloor = k$.
- **Proof:** $k \leq k + 1/2 < k + 1$, so $\lfloor k + 1/2 \rfloor = k$ by definition.

103

103

Example theorem involving floor function with a direct proof not involving cases

Theorem: If n is odd, then $\lfloor n/2 \rfloor = (n - 1)/2$.

Proof:

- Let n be an arbitrary odd integer.
- By definition of odd, there is an integer k so that $n = 2k + 1$.
- Then the LHS of the equation is
- $\lfloor n/2 \rfloor = \lfloor k + 1/2 \rfloor$ by substitution
  $= k$ by lemma of previous slide
  $= (n-1)/2$ by substitution
- Q.E.D.

104

104

Proof by Contradiction: Introduction

- **Definition:** A **contradiction** is a statement that is "always" false.
- If c is a contradiction, then the following is a valid form of argument that p is true:

  ~p (premise, i.e., presumed true)

  ~p → c (by some valid argument)

  ∴ c (modus ponens)

  but a contradiction c is always false so the premise p must be false

  ∴ p (valid conclusion by proof by contradiction)

- Note that if ~p → c ≡ p ∨ c is true (by a valid argument) and c is false then p must be true.

105

105

Method of Proof by Contradiction

- **Suppose** the statement to be proved is not true.
- **Show** that this supposition leads logically to a contradiction.
- **Conclude**: The supposition is false. That is, conclude that the given statement is true.

106

106

Example 1 – Proof by Contradiction

Theorem: There is no largest real number.

Proof:

- Suppose there were a largest real number, N.
- Consider the number N + 1.
- N + 1 is a real number (reals are closed under addition), and N + 1 is larger than N.
- This result contradicts the supposition that N is the largest real number.
- Hence the supposition is false.
- Q.E.D.

107

107

Example 2 – Proof by Contradiction

Definition: An **irrational number** is a real number that is not rational.
Theorem: The negative of any irrational number is irrational ($\in \mathbb{Q}^*$).
Proof:

- Restating the theorem statement formally:
  $\forall x \in \mathbb{Q}^*, -x \in \mathbb{Q}^*$
- For a proof by contradiction, assume the negation of what is to be proved:
  $\exists x \in \mathbb{Q}^*$ s.t $-x \in \mathbb{Q}$
- Take any such x.
- Since $-x \in \mathbb{Q}$, $\exists$ a,b $\in \mathbb{Z}$ such that $b \neq 0$ and $-x = a/b$.
- Thus $x = (-a)/b$.
- Since $a \in \mathbb{Z}$ and $-a \in \mathbb{Z}$.
- So, $x \in \mathbb{Q}$.
- This contradicts the previous assumption, which must therefore be false.
- Q.E.D.

108

108

Review of elementary definitions

- An integer n is even if, and only if n is equal to twice some integer.
- An integer n is odd if, and only if n is equal to twice some integer plus 1.
- A real number r is rational if, and only if it is equal to a quotient of integers (with nonzero denominator otherwise r would not be real).
- Given integers n and d≠0, d divides n (d|n) if, and only if, n equals d times some integer.
- An integer n is prime if, and only if, $n > 1$ and the only positive integer divisors of n are 1 and n.
- Given a real number x, the floor of x is the integer n=⌊x⌋ such that $n \leq x < n + 1$ (n is the largest integer ≤ x)
- Given a real number x, the ceiling of x is the integer n=⌈x⌉ such that $n - 1 < x \leq n$ (n is the smallest integer ≥ x)
- Note: There are other equivalent definitions.

109

109

Recall

- The **quotient-remainder** theorem: For all integers n and positive integers d, there exist unique integers q and r such that $n = dq + r$ and $0 \leq r < d$.
- The **"transitivity of divisibility"** theorem: $\forall$ a, b, c $\in \mathbb{Z}$, if a | b and b | c, then a | c.
- An integer n is **composite** ⇔ n>1 and n is a product of positive integers, neither of which is 1.
- The **unique factorization** theorem: Given any integer $n > 1$, either n is prime or n can be written as a product of prime numbers in a way that is unique, except, possibly, for the order in which the numbers are written.

110

110

Proof by Contraposition: Outline

To prove a universal conditional statement (i.e., of the form "∀ x in D, if P(x) then Q(x)" by contraposition:

1) First formulate the logically equivalent contrapositive of the statement, i.e., "∀ x in D, if ~Q(x) then ~P(x)"

2) Use a direct proof for the contrapositive statement.

111

111

Example proof by contraposition

Lemma: ∀ integers n, if n^2 is even then n is even.
Proof:

- The (logically equivalent) contrapositive of the conditional statement in the lemma is
  ∀ integers n, if n is odd then n^2 is odd.
- To prove this contrapositive, take an arbitrary odd integer n.
- Since n is odd, ∃ an integer k such that $n=2k+1$.
- Thus, $n^2=(2k+1)^2=2(2k^2+2k)+1$.
- Since $2k^2+2k$ is an integer (being the sum of products of integers), n^2 is odd.
- Q.E.D.

Recall: A lemma is a statement used to prove a more important result.
Exercise: Try to prove this theorem directly.

112

112

Proving √2 Is Irrational: Background

- For any nonnegative real number n, the square root of n is the nonnegative number $n^{0.5} = \sqrt{n}$ which, when squared (multiplied by itself), equals n.
- Examples: $\sqrt{4} = 2$, $(25)^{0.5} = 5$, $(16/9)^{0.5} = 4/3$
- Recall: An irrational number is a real number that is not rational.
- Note that $1/0$ is not rational as it is not real.
- Recall: Every rational number can be written in "lowest terms" (with smallest denominator in magnitude) by cancelling out common factors in the numerator and denominator, i.e., so that they're "co-prime."
- Example: $18/24 = 3/4$ (cancelled out 6), $20/(-10) = -2/1$ (cancelled out -10)

113

113

Theorem: √2 Is Irrational

Proof by contradiction:

- Suppose not. That is, assume $\sqrt{2}$ is rational.
- So, there exists integers a and b with $b \neq 0$ such that $\sqrt{2} = a/b$ where a and b are assumed to have no common factors.
- Thus, $a^2 = 2b^2$.
- So, a^2 is even, and hence also that a is even by the previous lemma.
- So, there exists an integer k such that $a = 2k$.
- After substituting for a, we get $4k^2 = 2b^2$, so $2k^2 = b^2$.
- Thus b^2 is even, and hence b is even by the previous lemma.
- Since a and b are both even, they have a common factor of 2.
- This contradicts the assumption that a and b have no common factors.
- Thus the assumption that $\sqrt{2}$ is rational is false.
- Q.E.D.

114

114

Theorem: There are infinitely many prime numbers

Proof by contradiction:

- Suppose not. That is, assume there is a finite set of prime numbers $p_1, p_2 \ldots, p_n$ with $n<\infty$.
- Consider the product of these primes plus 1, i.e., the integer $k = 1 + p_1 \times p_2 \times \ldots \times p_n$
- Note that k is an integer larger than all primes (obviously $k>1$ because we know there exist some primes like 2,3,5,7,11,…).
- Also, no prime number divides k, indeed division by any prime leads to a remainder of 1 (i.e., k mod p =1 for all primes p).
- Thus k is not a composite number as it has no prime factors.
- Thus k is prime, which is a contradiction.
- Q.E.D.

115

115

Euclid's algorithm for greatest common divisor (gcd)

Def'n: gcd(A,B) is the greatest common divisor (>0) of integers A and B.

0. Initial data A,B with $A \geq B \geq 0$. Also, initially note that gcd(A,A)=A and gcd(0,0) is not defined (in latter case return 0 or error statement).
1. If B=0, then return gcd=A and STOP.
2. Else find unique integers q,r such that A=Bq+r, where $0 \leq r < B$ (i.e., quotient-remainder theorem).
3. Set A =B and then B =r (i.e., (A,B) →(B,r)), and go to step 1.

Notes:

- **Exercise** re. step 2: prove that gcd(A,B)=gcd(B,r); i.e., for each iteration of steps 2 and 3, gcd(A,B) does not change.
- As a result of steps 2 and 3, B (≥0) is **strictly** reduced (r<B).
- Also in step 2, r=0 implies B=gcd(A,B) (i.e., B|A).
- So, Euclid's algorithm will converge to find the gcd in a finite number of iterations (cf. well ordering principle).
- 1845 theorem of Lame gives complexity of EA using Fibonacci sequence, see http://wwwdh.cs.fau.de/IMMD8/Lectures/THINF3/Texte/euclid4.pdf

116

116

Euclid's algorithm - example

- Find gcd(284,16) by Euclid's algorithm.
- Euclid's algorithm proceeds by the following iterations since, initially, A=284 > B =16>0.

1. 284 = 16·17 + 12
2. 16 = 12·1 + 4
3. 12 = 4·3 + 0 (remainder is now 0)
4. B=0 so return A=4 – i.e., Euclid's algorithm stops here.

- So, gcd(284,16)=4.

117

117

Introduction to Discrete Mathematics

Sequences and Induction

This revision ©G. Kesidis (2013)

This document revision is copy-left 2013.

It is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License

Note: these slides adapted in part from those of S.J. Lomonaco Jr., available at
http://www.csee.umbc.edu/~lomonaco/f05/203/Slides203.html

118

118

Sequences and Induction- Outline

- Sequences
- Induction
- Strong Induction

119

119

Sequences

- **Sequences** represent **ordered lists** of elements.
- A **sequence** is defined as a function from a subset of $\mathbb{N}$ (i.e., f has countable domain) to a set S.
- We use the notation $a_n = f(n)$ to denote the image of the integer n.
- We call a_n a term (the n^{th} term) of the sequence.
- **Example:** $f(n)=2n$ for $n \in \mathbb{N}$ (here S must contain all even positive integers); since here f is defined for all natural numbers (positive integers), we can write $f: \mathbb{N} \rightarrow S$.

120

120

Sequences

- We use the notation $\{a_n\}_{n\in\mathbb{N}}$ to describe a sequence.
- When possible it is convenient to describe a sequence with a **formula**.
- For example, the sequence {2,4,6,8,…} of the previous slide can be specified more precisely as
  $\{a_n\}_{n=1}^{\infty} = \{a_n\}_{n\in\mathbb{N}}$ where $a_n = 2n$.
- Finding a formula, when one exists and is unique, for a given numerical sequence (or portion thereof) can be very tricky.

121

121

Formulas for simple example sequences

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

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

122

122

Series summations of numeric sequences

- $\sum_{k=m}^{n} a_k$ represents the sum $a_m + a_{m+1} + a_{m+2} + \ldots + a_n$.
- This sum has n-m+1 terms when $n \geq m$ (otherwise the sum is sometimes defined to be zero).
- The variable k is called the **index of summation**, running from its **lower limit** m to its **upper limit** n.
- We could as well have used any other letter to denote this index, i.e., k is a "dummy" variable.

123

123

Summations - examples

- Express in compact summation notation the sum of the first 1000 terms of the sequence $\{a_n\}$ with $a_n = n^2$ for $n \in \mathbb{N}$.
  Answer: $\sum_{k=1}^{1000} k^2$
- What is the value of $\sum_{j=1}^{6} j$?
  Answer: $1 + 2 + 3 + 4 + 5 + 6 = 21$

124

124

Summations

- It is said that as a child, Gauss came up with the following formula:
  $\sum_{k=1}^{n} k = 1+2+\ldots+n = n(n+1)/2$
- For example: $1+2+\ldots+100 = 100(101)/2 = 5050$
- Gauss used the following argument:
- Let $S(n) = \sum_{k=1}^{n} k$.
- Writing the sum forward and backward, we get:
  $S(n) = 1 + 2 + 3 + \ldots + n\text{-}1 + n$
  $S(n) = n + n\text{-}1 + n\text{-}2 + \ldots + 2 + 1$
- Note that we have aligned n numbers in columns, e.g., 1 and n, 2 and n-1, 3 and n-2, etc., each column with sum n+1.
- Thus, by adding the columns we get
  $2S(n) = (n+1) + (n+1) + \ldots + (n+1)$,
  where there are n identical terms $(n+1)$ being added.
- Thus, $2S(n) = (n+1)n$.
- **Exercise:** Write the above as a theorem statement and direct proof.

125

125

Arithmetic sequences of real numbers

- An arithmetic sequence is one where the difference between consecutive terms is constant, when they are arranged in either increasing or decreasing order.
- Let d be this difference and a_1 be the "initial" term of an arithmetic sequence.
- So, the k^{th} term of this series is
  $a_k = a_1 + (k\text{-}1)d$
- For example, the sequence of natural numbers is an arithmetic series with $d=1$ and $a_1=1$.
- Note that if $d>0$ then a_1 is the smallest term of the sequence, but if $d<0$ then a_1 is the largest term of the sequence.
- Also note that the set of all odd integers is an arithmetic sequence without a largest or smallest term (with $d=2$).
- **Exercise:** Use Gauss's direct argument to directly prove the identity
  $\sum_{k=1}^{n} (a_1 + (k\text{-}1)d) = n(2a_1 + (n\text{-}1)d)/2 = n(a_1 + a_n)/2 \quad \forall\, a_1, d \in \mathbb{R}, n \in \mathbb{N}$,
  i.e., n times the average number in the sequence.

126

126

Arithmetic series - Example

- Find the sum of the arithmetic series 7+4.5+…-18.

Solution:

- From the given facts (including that we are dealing with an arithmetic sequence), we immediately deduce $a_1=7$ and $d= -2.5$.
- The final (n^{th}) term is $a_n = a_1 +(n-1)d = -18$; so, $n=11$.
- Finally, apply the prior formula to get that the sum is
  $n(a_1 +a_n)/2 = 11(7 – 18)/2 = -60.5$
- **Exercise:** Show that the same sum is obtained by adding the arithmetic series in reverse order, i.e., with $a_1= -18$ and $d= 2.5$.

127

127

Geometric sequences of real numbers

- A geometric sequence is one where the ratio between consecutive terms is constant.
- Let r be this ratio and a_1 be the "initial" term of a geometric sequence.
- So, the k^{th} term of this sequence is
  $a_k = a_1 r^{k-1}$
- Note that if $|r|>1$ then a_1 is the smallest term of the sequence in magnitude (absolute value), but if $|r|<1$ then a_1 is the largest term of the sequence in magnitude.
- For a formula for the sum of a geometric series, $S:= \sum_{k=1}^{n} a_1 r^{k-1}$, first note that $rS= \sum_{k=2}^{n+1} a_1 r^{k-1}$
- Thus, $(r-1)S=rS – S = a_1 r^n – a_1$ after n-2 common terms cancel out from each series rS and S.
- And so,
  $\sum_{k=1}^{n} a_1 r^{k-1} = a_1 (r^n-1)/(r-1) \quad \forall a_1, r \in \mathbb{R}$ with $r\neq 1$.
- **Exercise:** Write the above as a theorem statement and direct proof.

128

128

Geometric series - Example

- Find the sum of the geometric series 3-3/5+... +3/625.

Solution:

- From the given facts (including that we are dealing with an geometric sequence), we immediately deduce $a_1=3$, r= -1/5.
- The final (n^{th}) term is $a_n = a_1 r^{n-1} = 3/625$; so, n=5.
- Finally, apply the prior formula to get that the sum is $a_1 (1-r^n)/(1-r) = \ldots$
- **Exercise:** Show that the same sum is obtained by adding the geometric series in reverse order, i.e., with $a_1= 3/625$ and r= -5.

129

129

Two Other Useful Series

- $\sum_{k=1}^{n} k = n(n+1)/2$ ...arithmetic
- $\sum_{k=1}^{n} r^k = (1-r^n)/(1-r)$ ...geometric
- $\sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6$
- $\sum_{k=1}^{n} k^3 = n^2(n+1)^2/4$
- We'll return to the proofs of the last two identities later.

130

130

Multiple Summations

- $\sum_{j=a}^{b} \sum_{k=m(j)}^{n(j)} f(j,k) = \sum_{j=a}^{b} g(j)$ where $g(j) := \sum_{k=m(j)}^{n(j)} f(j,k)$
- Obviously, multiple summations are numerically computed by nested loops.
- Example:
  $\sum_{j=1}^{b} \sum_{k=1}^{j} k = \sum_{j=1}^{b} j(j+1)/2 = 0.5\sum_{j=1}^{b} j^2 + 0.5 \sum_{j=1}^{b} j$
  $= 0.5\, b(b+1)(2b+1)/6 + 0.5\, b(b+1)/2$

- Note: Though the summation order and "splitting" the sum up as in the example above is generally OK for sums over finite domains, equivalence after switching the order of summation (Fubini's theorem) over infinite domains requires uniform convergence.
- **Exercise:** Work out the previous example by first switching the order of summations, i.e., $\sum_{k=1}^{b} \sum_{j=k}^{b} k = \sum_{k=1}^{b} (b-k+1)(b+k)/2 = \ldots$

131

131

Induction for proof of predicate over a countably infinite domain

- Suppose we want to prove $\forall n \in D, Q(n)$
  where the set S is of countably infinite size, i.e., S can be enumerated (mapped) by the natural numbers $\mathbb{N}$ or subset thereof.
- Clearly, we cannot prove by dividing into individual cases if the number of cases is infinite.
- We might try to directly prove the statement beginning with an **arbitrary** $n \in S$.
- Alternatively, a proof by induction may be possible.
- For $D=\mathbb{N}$, the inductive proof of "$\forall n \in \mathbb{N}, Q(n)$" is of the form:

1. Prove $Q(1)$, i.e., base case.
2. For arbitrary $n \in \mathbb{N}$, assume $Q(n)$, i.e., inductive assumption.
3. Prove $Q(n+1)$, i.e., inductive step.
4. Q.E.D.

132

132

Induction for proof of predicate over a countably infinite domain (cont)

- The inductive assumption is true for the lowest index n=1 (base case) of the predicate to be proved.
- So, the inductive step iteratively (as counting) proves Q(n) for arbitrarily large n∈ℕ starting from 1.
- More succinctly, the inductive argument on ℕ is

$\forall n \in \mathbb{N}, Q(n) \equiv Q(1) \wedge (\forall n \in \mathbb{N}, \text{if } Q(n) \wedge Q(1) \text{ then } Q(n+1))$

133

133

Induction Example

Theorem: $n < 2^n$ for all positive integers n.

Proof:

- Let Q(n) be the predicate "$n < 2^n$."
- Q(1) is true because $1 < 2^1 = 2$.
- For arbitrary integer $n \geq 1$, assume Q(n).
- Now note that:

  $n+1 < 2^n + 1$ (by the inductive assumption)

  $< 2^n + 2^n$ (since $n \geq 1$, $2^n \geq 2^1 > 1$)

  $= 2^{n+1}$

  i.e., we have established Q(n+1).
- Q.E.D.
- Note that instead we could have argued as $n+1 \leq 2n < 2^{n+1}$ where the second inequality is the inductive assumption times 2.

134

134

Induction Example

Theorem: $\forall n \in \mathbb{N}, \sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6$

Proof:

- Let Q(n) be the predicate "$\sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6$".
- For n=1, we have that $1^2 = 1(1+1)(2\cdot1+1)/6$, i.e., Q(1) is true.
- For arbitrary integer $n \geq 1$, assume Q(n).
- To establish Q(n+1), begin with:

$$\begin{aligned} \sum_{k=1}^{n+1} k^2 &= (n+1)^2 + \sum_{k=1}^{n} k^2 \\ &= (n+1)^2 + n(n+1)(2n+1)/6 \quad \text{(inductive assumption)} \\ &= (n+1)(n+2)(2n+3)/6 \end{aligned}$$

- Q.E.D.

Exercise: Check the last equality

Exercise: Prove the formula for $\sum_{k=1}^{n} k^3$

135

135

Induction Example (cont)

- In the previous example, the inductive step can instead be argued as:

$$\begin{aligned} Q(n+1) \quad &\equiv \quad \sum_{k=1}^{n+1} k^2 = (n+1)(n+2)(2n+3)/6 \\ &\Leftrightarrow \quad (n+1)^2 + \sum_{k=1}^{n} k^2 = (n+1)(n+2)(2n+3)/6 \\ &\Leftrightarrow \quad \sum_{k=1}^{n} k^2 = (n+1)(n+2)(2n+3)/6 - (n+1)^2 \text{ ... algebra...} \\ &\Leftrightarrow \quad \sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6 \quad \equiv \quad Q(n) \end{aligned}$$

- Since Q(n) is true by the inductive assumption and each step above is "if and only if" ($\Leftrightarrow$), Q(n+1) is true.
- **Exercise:** Spot the logical flaw in the following argument that 1=0 leveraging the fact that 1=1:

$$\begin{aligned} 1 &= 0 \\ 0 &= 1 \\ 1+0 &= 0+1 \\ 1 &= 1 \end{aligned}$$

136

136

Strong Induction

- The principle of strong mathematical induction involves a "stronger" inductive assumption.
- In order to prove "$\forall n \in \mathbb{N}$, Q(n)", by strong induction:

1. Prove Q(1) (base case)
2. For arbitrary integer $n \geq 1$, assume Q(k) **for all** $k \in \{1,2,\ldots,n\}$ (**strong** inductive assumption)
3. Prove Q(n+1). (inductive step)

Q.E.D.

137

137

Strong Induction Example 1

Theorem: If s(0)=1, s(1)=2, and s(k+1)=2s(k-1) for all integers k>0, then $s(k) = 2^{\lfloor 0.5k+0.5 \rfloor}$ for all integers $k \geq 0$.

Proof:

- Let Q(k) be the predicate "$s(k) = 2^{\lfloor 0.5k+0.5 \rfloor}$".
- Q(0) is true because $2^{\lfloor 0.5 \cdot 0+0.5 \rfloor} = 2^{\lfloor 0.5 \rfloor} = 2^0 = 1 = s(0)$, where the last equality is the theorem's hypothesis.
- For arbitrary integer $k \geq 0$, assume Q(n) for all $n \in \{0,1,2,3,\ldots,k\}$.
- To prove Q(k+1), we take two cases.
  - If k=0, then $2^{\lfloor 0.5 \cdot 1+0.5 \rfloor} = 2^{\lfloor 1 \rfloor} = 2^1 = 2$, establishing Q(1) by theorem's hypothesis.
  - If k>0, then

$$\begin{aligned} s(k+1) &= 2s(k-1) \quad \text{... by theorem's hypothesis} \\ &= 2 \cdot 2^{\lfloor 0.5(k-1)+0.5 \rfloor} \quad \text{... by strong inductive assump.} \\ &= 2^{\lfloor 0.5(k-1)+0.5 \rfloor + 1} = 2^{\lfloor 0.5(k-1)+0.5+1 \rfloor} = 2^{\lfloor 0.5(k+1)+0.5 \rfloor} \end{aligned}$$

- Q.E.D.

138

138

Strong Induction Example 1 (cont)

- The proof of the previous example can be reworked as:
  1. Prove Q(0) and Q(1) are established in the base case
  2. For arbitrary integer $k \geq 1$, assume Q(k) and Q(k-1) (inductive assumption).
  3. Prove Q(k+1) by using the difference equation (inductive step).
- This is a valid argument because:

  if $Q(0) \wedge Q(1)$ and $\forall k \geq 1$, $Q(k) \wedge Q(k-1) \Rightarrow Q(k+1)$,

  then $\forall k \geq 0$, Q(k).

- The following theorem requires a strong induction proof.

139

139

Strong Induction Example 2

Theorem: Every integer greater than one is either prime or is a product of primes.

Proof:

- Let Q(n) be the predicate "n is prime or can be written as a product of primes."
- Q(2) is true because 2 is prime.
- For arbitrary integer $n \geq 2$, assume Q(k) for all $k \in \{2,3,\ldots,n\}$.
- To prove Q(n+1), we take two cases.
  - If n+1 is prime, Q(n+1) is true by definition.
  - If n+1 is not prime (composite),
    - then there exists integers $n \geq a,b \geq 2$ such that n+1=ab;
    - apply the inductive assumption to both a and b, and
    - substitute their prime factorizations into n+1=ab to show n+1 is a product of primes.
- Q.E.D.

140

140

Induction - Comments

- Note that the initial index in this example was 2, not 1, and that the inductive assumption was adjusted accordingly.
- **Exercise:** Can induction be used to prove a predicate true over a finite domain? If so, how (if at all) does the form of the inductive proof change?

141

141

More general "bootstrapping" examples

- Consider a predicate P.
- Suppose that we have proved P(3).
- Find the complete set of integers k for which P(k) is true if we also proved that:

  $\forall k \geq 1, P(k+1) \Rightarrow P(k) \wedge P(k+3)$. (*)
- **Answer:** The "bootstrap" (*) works for P(k+1) only with $k+1 \geq 2$. So:

  $P(3) \Rightarrow P(2) \wedge P(5)$

  $P(2) \Rightarrow P(1) \wedge P(4)$

  $P(4) \Rightarrow P(3) \wedge P(6)$
- So far, we see how P(3) can be bootstrapped to show P(k) for $k \in \{1,2,3,4,5,6\}$
- Continuing in this way, we see that the P(k) is true for all integers $k \geq 1$.
- **Exercise:** Why is P(0) not necessarily true?

142

142

More general "bootstrapping" examples

- Find the complete set of integers k for which P(k) is true if P(5) is true and we also proved that:

  $\forall k > 0, P(k) \Rightarrow P(2k) \wedge P(k-1)$. (*)
- **Answer:**

  $P(5) \Rightarrow P(10) \wedge P(4)$

  $P(4) \Rightarrow P(8) \wedge P(3)$

  $P(10) \Rightarrow P(9) \wedge P(20)$
- So far, we see how P(5) can be bootstrapped to show

  P(k) for $k \in \{3,4,5, 8,9,10, 20\}$
- Continuing in this way, we see that the P(k) is true for all integers $k \geq 0$ (note that (*) cannot be applied with k=0).
- Note that P(5) and $\forall k > 0, P(k) \Rightarrow P(2k)$ implies that $\forall k \geq 0, P(5 \cdot 2^k)$, and $\forall k > 0, P(k) \Rightarrow P(2k)$ "fills the gaps" between these numbers and gives P(1), P(2), P(3), P(4).

143

143

Remarks: Induction and Countability

- A set is **countable** if each of its element can be placed in one-to-one correspondence with a subset of the positive integers, $\mathbb{N}=\mathbb{Z}^{>0}$
- A set is **countably infinite** if it is **countable** and has an infinite number of elements, e.g.,
  - the set of *all* integers, $\mathbb{Z}$
  - the set of all rational numbers, $\mathbb{Q}$
- To see that $\mathbb{Q}^+$ is countable, construct the matrix whose $(i,j)^{th}$ entry is i/j and count these entries along the anti-diagonals starting from $1=1/1$.
- To see that $\mathbb{Q}$ is countable, count zero then proceed as for $\mathbb{Q}^+$ but count each entry i/j twice (once for the positive and the other for the negative).
- **Uncountable** sets include:
  - the set of real numbers, $\mathbb{R}$
  - the set of irrational numbers, $\mathbb{Q}^* = \mathbb{R} - \mathbb{Q}$
- Induction cannot be used to prove "$\forall x \in D, Q(x)$" for an uncountable set D.

144

144

THE WELL-ORDERING PRINCIPLE - background

- **Definition:** Let B be a set of integers. An integer m is called a least element of B if m is an element of B, and for every j in B, $m \leq j$.
- **Example:** 3 is a least element of the set {4,3,5,11}.
- **Example:** If A be the set of all positive odd integers, then 1 is a least element of A.
- **Example:** Let U be the set of all odd integers. Then U has no least element.
- **Exercise**: Give a proof of the previous statement by contradiction.

145

145

WELL-ORDERING PRINCIPLE - definition

- **The Well-Ordering Principle:** If B is a non-empty set of integers and there exists an integer c such that every element j of B satisfies $c < j$, then there exists a least element of B.
- For example**:** If B is a non empty set of non negative integers then there exists a least element in B (since B has the well-ordering property when c is any negative number).

146

146

WELL-ORDERING - existence of quotient-remainder theorem

Theorem: For every integer a and positive integer d>0 there exist integers q and r such that $0 \le r < d$ and $a = qd + r$.

Proof:

- Let A be the set of all values a – kd for integers k such that $a - kd \ge 0$, i.e., $A=\{a-kd \mid k \in \mathbb{Z}, a-kd \ge 0\}$.
- To apply the well-ordering principle, we need to show that A is not empty:
  - If $a \ge 0$, then $a-kd=a \ge 0$ for k=0, i.e., $a \in A$;
  - else ($a<0$), let k=a so that $a-kd=a-ad=a(1-d) \ge 0$ because $1-d \le 0$ (since $d>0$) and $a<0$, i.e., $a \in A$.
- By the well-ordering principle, A has a least element.
- Let that least element be $r = a - qd$ where $q \in \mathbb{Z}$
- So $a = qd + r$ and $0 \le r$.
- So, the theorem is proved if $r<d$, which can be shown by contradiction…

147

147

WELL ORDERING – existence of quotient remainder theorem (cont)

Proof (continued):

- Suppose that $d \le r$.
- Note that $a = qd + r = qd + d + (r-d) = (q+1)d + r'$ where $r' := (r-d) \ge 0$.
- Also $r' = r-d < r$, because $d > 0$.
- So $a - (q+1)d = r' < r = a - qd$, and $a - (q+1)d = r' \ge 0$.
- So $r' = a - (q+1)d$ is in A, and $r' < r$, thus contradicting the fact that r is the least element of A.
- Q.E.D.

Recall that for each a,d, such q,r in the theorem statement must also be unique, and that this is quickly proved by contradiction.

148

148

Introduction to Discrete Mathematics

Introduction to Set Theory

This revision © G. Kesidis (2013)

This document revision is copy-left 2013.
It is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License

Note: these slides adapted in part from those of
© S.S. Epp and S.J. Lomonaco Jr., the latter available at
http://www.csee.umbc.edu/~lomonaco/f05/203/Slides203.html

149

149

A Glimpse into Set Theory

- Sets contain elements and are completely determined by the elements they contain.
- **So**: two sets are equal if and only if they have exactly the same elements.
- **Notation:** $x \in A$ is read "x is an element of A" (or "x is in A")
- $x \notin A$ is read "x is not an element of A" (or "x is not in A")
- **Ex**: Let $A = \{1, 3, 5\}$
  $B = \{5, 1, 3\}$
  $C = \{1, 1, 3, 3, 5\}$
  $D = \{x \in \mathbb{Z} \mid x \text{ is an odd integer and } 0 < x < 6\}$

  How are A, B, C, and D related?

  Answer: They are all equal.

150

150

Sets – some notation and examples

- {a,b} is the set containing elements "a" and "b"
- {a,{a}} is the set containing elements "a" and {a}, the latter being the set containing the element "a"
- So, sets contain elements and elements themselves may be sets, cf. the power set of a set.
- Cannot list elements as {a,b,…} for an uncountable set.
- For a,b∈ℝ, the following are intervals ("connected" subsets) of ℝ (an "ordered" set):
  - (a,b] = {x ∈ℝ | a<x≤b}
  - [a,b) = {x ∈ℝ | a≤ x<b}
  - [a,b] = {x ∈ℝ | a≤ x ≤ b}, a "closed" interval
  - (a,b) = {x ∈ℝ | a<x<b}, an "open" interval

151

151

Subsets

- **Definition**: Given sets A and B, A ⊆ B (read "A is a subset of B") means every element in A is also in B.
- Equivalently: A ⊆ B ⇔ ∀x, if x ∈ A then x ∈ B

- **Note**: A ⊄ B ⇔ ∃ x such that x ∈ A and x ∉ B.
- **Note**: A = B ⇔ A ⊆ B and B ⊆ A.

- **Ex**: Let A = {2,4,5} and B = {1,2,3,4,6,7}. Is A ⊆ B ?
- Answer: No, because 5 is in A but 5 is not in B.

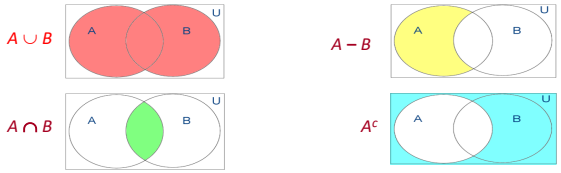
- **Ex**: Let C = {2,4,7} and B = {1,2,3,4,6,7}. Is C ⊆ B ?
- Answer: Yes, because every element in C is in B.

152

152

Definitions of Basic Set Operations

- Given sets A and B that are subsets of a "universal set" Ω.
- Their union is $A \cup B = \{x \in \Omega \mid x \in A$ **or** $x \in B\}$ where "or" is inclusive.
- Their intersection $A \cap B = \{x \in \Omega \mid x \in A$ **and** $x \in B\}$
- The set difference $A - B = \{x \in \Omega \mid x \in A$ and $x \notin B\}$
- The complement of A is $A^c = \{x \in \Omega \mid x \notin A\} = U - A$.
- Note that only complementarity requires specifying the universal set.
- Venn diagrams:



153

153

The Empty Set

- Example: Assume people live in only one place. Let A be the set of all the people in the room who live in Chicago and B be the set of all people in the room who live outside Chicago.
- What is $A \cap B = A \cap B^c$? Note $B = A^c$

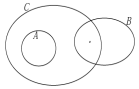
  Answer: This set contains no elements at all.
- **Notation:** The symbol ϕ denotes a set with no elements.
- We call it the empty set or the null set.
- To show a set A is empty, one might first assume there is an element of A and prove a contradiction results.
- Exercise: Show $(5, 3] = \phi$.
- Note that $\phi \subseteq A$ for any set A (vacuously true by the "if … then…" definition of the subset relation, ⊆).

154

154

Example

- Let A = {1, 2, 3} and B = {3, 4, 5} and let the universal set be Ω = {1, 2, 3, 4, 5, 6, 7, 8}.
- A ⋃ B = {1,2,3,4,5}
- A ⋂ B = {3}
- A – B = {1,2} = A – (A ⋂ B) =A ⋂B^c
- A^c = {4,5,6,7,8}

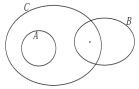


155

155

Venn Diagrams

- The Venn diagram below represents sets A, B, and C so that A ⊆ C, A ⋂ B = ϕ (i.e., A and B are disjoint), and B ⋂ C ≠ϕ.
- A Venn diagram represents infinitely many different discrete instances, e.g., A = {1}, C = {1, 2}, and B = {2, 3}, so that A ⊆ C, A ⋂ B =ϕ, and B ⋂ C = {2}≠ϕ.
- We allow Venn diagrams to contain empty spaces, so we may place a dot inside the region B ⋂ C to explicitly indicate otherwise.
- Note that according to the 3 facts - A ⊆ C, A ⋂ B = ϕ, B ⋂ C ≠ϕ – it's possible that B ⊆ C (a stronger condition) but it's also possible that B⊄C.



156

156

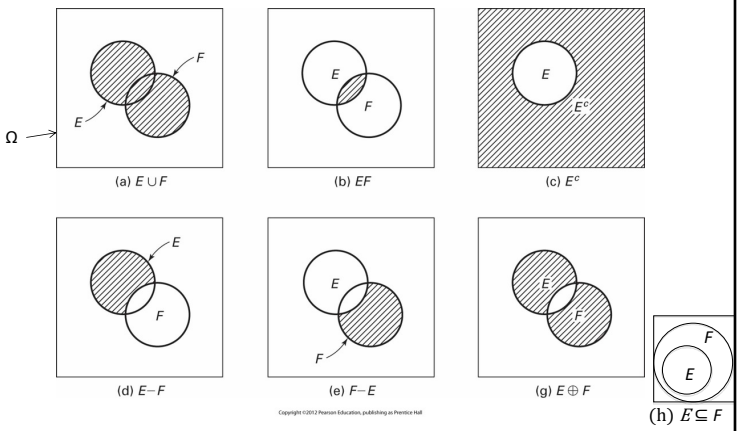
Review of set theory

- Suppose following sets are subsets of some universal set Ω.
- "x is an element of A" is denoted $x \in A$
- A is a subset of B, denoted $A \subseteq B$, when the following statement holds:
  ∀ (for all) $x \in \Omega$, if $x \in A$ then $x \in B$
- The intersection of two sets A and B is the set
  $AB = A \cap B = \{s \in \Omega \mid s \in A \text{ and } s \in B\} = \{s \in \Omega \mid s \in A, s \in B\} = BA$
  where the symbol "|" denotes "such that" (as does ":")
- The union of two sets A and B is the set
  $A \cup B = \{s \in \Omega \mid s \in A \text{ or } s \in B\} = B \cup A$
  where "or" is inclusive allowing $s \in AB$
- The difference of two sets is defined as
  $A - B = A \setminus B = \{s \in \Omega \mid s \in A \text{ and } s \notin B\} = A \cap B^c = A\text{-}AB$
- The exclusive union of two sets is defined as
  $A \oplus B = \{s \in \Omega \mid s \in A \text{ or } s \in B \text{ but } s \notin AB\} = A \cup B - AB$
- The complement of a set $A^c = \{s \in \Omega \mid s \notin A\} = \Omega - A$ (here need to specify Ω)
- Note that $\Omega^c = \phi$, the empty set, and $\phi^c = \Omega$.
- For example, if A={1,2} and B={2,3,4}, then $A \cup B = \{1,2,3,4\}$, AB={2}, A-B = {1}, B-A = {3,4}, $A \oplus B$ {1,3,4}.

157

157

Venn diagrams for set operations/relations, where everything inside the box is Ω



158

158

DeMorgan's theorem- a direct proof

Theorem: ∀ sets A,B, $(A \cap B)^c = A^c \cup B^c$

Proof:

- Plan: show two sets are equal by showing they contain each other.
- Choose arbitrary sets A,B (addressing the universal qualifier ∀).
- First show $A^c \cup B^c \subseteq (A \cap B)^c$:
- If $x \in A^c \cup B^c$ then $x \notin A$ or $x \notin B$ by definition of union, so consider the two cases.
  1. If $x \notin A$ then $x \notin A \cap B$ because $A \cap B \subseteq A$.
  2. If $x \notin B$ then $x \notin A \cap B$ because $A \cap B \subseteq B$.
- Thus, $x \notin A \cap B$ (as this is a consequence of both possible cases).
- Next show $(A \cap B)^c \subseteq A^c \cup B^c$.
- If $x \in A \cap B$ then $x \in B$ and $x \in A$, i.e., x is an element of both.
- So, if $x \in (A \cap B)^c$ then: x cannot be in both A and B, i.e., either $x \notin A$ or $x \notin B$, equivalently $x \in A^c \cup B^c$.
- Q.E.D.

159

159

DeMorgan's theorem for logic – Direct proof by exhaustive cases

- Statements p and q, e.g., for an arbitrary $x \in \Omega$, p = $x \in A$ and q = $x \in B$.
- p, q are either True=1 or False=0.
- The logical negation operator is ~, e.g., ~p = $x \notin A$.
- Note that $x \in AB \equiv p \wedge q$ (i.e., p and q), $x \in A \cup B \equiv p \vee q$ (i.e., p or q).
- Proof of DeMorgan's theorem by truth table (all combinations of p,q):

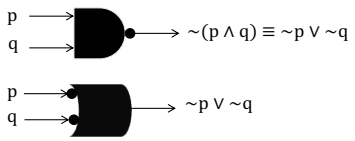
p	q	~p	~q	~p∧~q	p∨q	~(p∨q)
0	0	1	1	1	0	1
0	1	1	0	0	1	0
1	0	0	1	0	1	0
1	1	0	0	0	1	0

- Note the logical equivalence (by column) $\sim(p \wedge q) \equiv \sim p \vee \sim q$. Q.E.D.
- **Exercise:** Show $(A \cup B)^c = A^c \cap B^c$ for all sets A,B, as an immediate consequence (corollary) of the above half of De Morgan's theorem by truth table.
- **Exercise:** Show the more basic "contrapositive": $A \subseteq B$ if and only if $B^c \subseteq A^c$.

160

160

DeMorgan's theorem for equivalent AND (∧) and OR (∨) gate configurations



161

161

DeMorgan's theorem – Proof by contradiction: background

- Suppose want to show $X \stackrel{def}{=} (A \cap B)^c \subseteq Y \stackrel{def}{=} A^c \cup B^c$ for arbitrary $A,B \subseteq \Omega$.
- Define the statements $p = z \in X$ and $q = z \in Y$ for arbitrary $z \in \Omega$.
- So, we want to show $p \rightarrow q$, i.e., "if p then q".
- The negation of this statement, $\sim(p \rightarrow q) \equiv p \wedge \sim q$

p	q	p→q	p ∧ ~q
1	1	1	0
1	0	0	1
0	1	1	0
0	0	1	0

- To prove $p \rightarrow q$ is true, we will show $p \wedge \sim q$ results in a contradiction (and so is false).

162

162

DeMorgan's theorem – Proof by contradiction (cont)

- Assume $p \wedge \sim q$, i.e., $z \in X = (A \cap B)^c$ but $z \notin Y = A^c \cup B^c$.
- If $z \notin Y$ then $z \notin A^c$ and $z \notin B^c$ otherwise z would be in their union (Y).
- So, $z \in A$ and $z \in B$.
- So, $z \in A \cap B$, which contradicts $z \in X$.
- Thus, the first assumption above is false and so $X \subseteq Y$.
- Similarly show $q \wedge \sim p$ is false so that $Y \subseteq X$.
- Thus, X=Y.
- Q.E.D.

In this case, this argument is very similar to the direct proof above.

163

163

DeMorgan's theorem for arbitrary number of sets - Proof by induction

Theorem: $(A_1 \cup A_2 \cup \ldots \cup A_n)^c = A_1^c \cap A_2^c \cap \ldots \cap A_n^c$ for any sets A_k and any $n \in \{2,3,4,\ldots\}$.

Proof:

- **Define predicate Q(n)="**$(A_1 \cup A_2 \cup \ldots \cup A_n)^c = A_1^c \cap A_2^c \cap \ldots \cap A_n^c$**"**
- We have already established Q(2).
- Strong inductive assumption: For arbitrary integer $n \geq 2$, assume Q(k) for all $k \in \{2,3,\ldots,n\}$.
- To complete the inductive proof, we need to show Q(n+1):
- To this end, let $B = A_1 \cup A_2 \cup \ldots \cup A_n$
- By Q(2), $(B \cup A_{n+1})^c = B^c \cap A_{n+1}^c$ and substitute the inductive assumption Q(n) applied to B^c.
- Q.E.D.

Note: Both the base case and inductive assumption were used to prove the inductive step. Also, we could have used weak induction.

164

164

Miscellaneous simple set identities

- Commutative property of ∪
  A∪B = B∪A for all sets A,B
- Associative property of ∪
  (A∪B) ∪C = A∪ (B∪C) for all sets A,B,C
- Similarly, associative and commutative properties of ∩
- Distributive property of ∩ over ∪:
  (A∪B)∩C = (AC) ∪ (BC) for all sets A,B,C.
- Distributive property of ∪ over ∩:
  (AC) ∪B = (A∪B)∩(C∪B) for all sets A,B,C.
- **Exercise**: prove these identities.

165

165

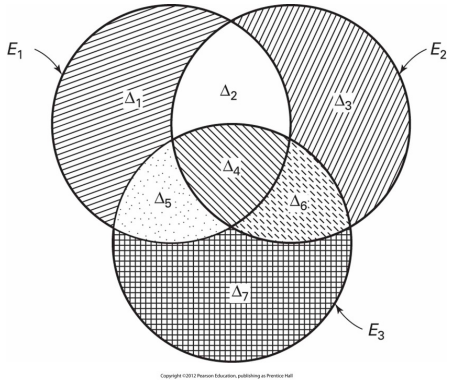
Partitions and Disjoint Coverings

- An n-partition of a set B is a collection of n sets $\Delta_1, \Delta_2, \ldots, \Delta_n$ such that:
  - None are empty, $\Delta_k \neq \phi$ for all k
  - Covering, $B = \Delta_1 \cup \Delta_2 \cup \ldots \cup \Delta_n$
  - Disjoint (non-overlapping), $\Delta_k \cap \Delta_j = \phi$ for all $k \neq j$
- We can write an obvious inclusion-exclusion formula for the union of two arbitrary sets as the union of 3 disjoint sets (a disjoint covering):
  A∪B = [A-B] ∪ [B-A] ∪ [AB]
- Similarly, we can write the union of three arbitrary sets as disjoint-covering of 7 sets :
  A∪B∪C = [A-(B∪C)] ∪ [B-(A∪C)] ∪ [C-(A∪B)] ∪ [AB-C] ∪ [BC-A]
  ∪ [CA-B] ∪ [ABC]
  $= AB^cC^c \cup A^cBC^c \cup A^cB^cC \cup ABC^c \cup A^cBC \cup AB^cC \cup ABC$
- Ignoring the empty sets, these "inclusion-exclusion" decompositions (disjoint-coverings) form partitions of the left-hand-side unions of arbitrary sets.
- Note that $A^cB^cC^c \not\subset A \cup B \cup C$ by De Morgan's law.

166

166

Partitioning $\cup_{i=1}^{3} E_i$ into seven disjoint regions (Δ_1,...,Δ_7) by inclusion/exclusion
Exercise: Write each Δ set in terms of the E sets.



Copyright ©2012 Pearson Education, publishing as Prentice Hall

167

167

Disjoint coverings formula for union of an arbitrary number of sets by induction

- Write $A_1 \cup A_2 \cup \ldots \cup A_k = B \cup A_k$ where $B = A_1 \cup \ldots \cup A_{k-1}$
- Find the 3-disjoint-covering of $B \cup A_k$ by inclusion-exclusion.
- Note that by DeMorgan, the term to $A_k - B = A_k \cap B^c$ simplifies to a single element of the inclusion-exclusion expansion.
- Apply the inductively assumed known inclusion-exclusion expansion for $B=A_1 \cup \ldots \cup A_{k-1}$ to each of the other two terms.
- Each of these other terms will produce n-1 elements after distribution of $-A_k$ ($\cap A_k^c$) or $\cap A_k$
- Note that if g(k-1) is the number of sets involved in the inclusion-exclusion formula for k-1 sets, then $g(k) = 2g(k-1) + 1$.
- **Exercise:** Fill in the details of this inductive argument.
- **Exercise:** Does the argument work if you distribute $\cup A_k$ over the expansion of B first, and then apply the 3-partition in each of the resulting terms?

168

168

An Inclusion-Exclusion Formula with Not-Disjoint Sets

- Consider four sets A,B,C,D not necessarily disjoint.
- An inclusion-exclusion formula for

$$P(A \cup B \cup C \cup D) = P(A)+P(B)+P(C)+P(D) - P(AB)-P(AC)-P(AD)-P(BC)-P(BD)-P(CD) + P(ABC)+P(ABD)+P(ACD)+P(BCD) - P(ABCD)$$

- Note: P(ABCD) is added 4=C(4,1) times in P(A)+…+P(D), 6=C(4,2) times in –P(AB)-…-P(CD), and added 4=C(4,3) times in P(ABC)+…+P(BCD), and thus must subtracted once so that it contributes only once to the union on LHS.
- **Exercise:** State and prove this inclusion-exclusion formula for arbitrary finite number of sets n by induction.

169

169

Cartesian products

- Suppose we want to define the set of "outcomes" after tossing two different 6-sided dice (i.e., the numbers on their upturned faces after they stop moving).
- Each die has outcomes belonging to the set {1,2,3,4,5,6}.
- So, the pair of dice has outcomes belonging to the Cartesian product,
  $\{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\} = \{1,2,3,4,5,6\}^2 = \{(n,m) \mid n,m \in \{1,2,3,4,5,6\}\}$,
  where n is the index of the first die, and m is that of the second.
- The total number of possible outcomes of the pair is $6 \times 6 = 36$.
- Similarly, $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3 = \{(x,y,z) \mid x,y,z \in \mathbb{R}\}$.
- The Cartesian product of intervals of $\mathbb{R}$ is
  $(a,b] \times [c,d] \times (e,f) = \{(x,y,z) \mid a<x\leq b,\ c \leq y \leq d,\ e<z<f\} \subseteq \mathbb{R}^3$

170

170

Power Set

- The power set of a set X, denoted 2^X, is the set of all subsets of X, including the empty set, ϕ, and X itself.
- For example, if X={1,2}, then 2^X={ϕ,{1},{2},X}
- Again, note how the elements of the power set 2^X are themselves sets.
- If the number of elements in X is finite, i.e., $|X|<\infty$, then the size of its power set is $2^{|X|}$, i.e., $|2^X|=2^{|X|}$.
- Exercise: Prove this by induction on |X|.
- Cf. the binomial theorem.

171

171

Introduction to Discrete Mathematics

Introduction to Probability Theory

This revision © G. Kesidis (2013)

This document revision is copy-left 2013.

It is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License

See slidedeck on undergraduate probability

172

172

Introduction to Discrete Mathematics

Functions & Pigeonhole Principle

This revision © G. Kesidis (2013)

This document revision is copy-left 2013.
It is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License

Note: these slides adapted in part from those of S.J. Lomonaco Jr., available at http://www.csee.umbc.edu/~lomonaco/f05/203/Slides203.html

Functions - definition

- A function f from a set A to a set B is an assignment
  - of exactly one element of B
  - to each and every element of A.
- We write

  $f(x) = y$

  if y is the unique element of B assigned by the function f to $x \in A$.
- So, if f is a function then: $\forall x \in A, \exists!\ y \in B$ s.t. $f(x)=y$
- If f is a function is a mapping from set A to B, we write

  $f: A \rightarrow B$

Functions – domain, co-domain and range

- If f:A→B, we say that A is the domain of f and B is the co-domain of f (the co-domain is sometimes called the range).
- If f(x) = y, we say that y is the image of x under f and x is a pre-image of y under f.
- The range of f:A→B is the set of all images of elements of A (this "range" is sometimes called the strict range), which is denoted

  $f(A) := \{f(x) \mid x \in A\} \subseteq B$

175

175

Functions – example where range = co-domain

Let's take a look at the function f:P→C with

- P = {Linda, Max, Kathy, Peter}, and
- C = {Boston, New York, Hong Kong, Moscow}.

Suppose:

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

Here, the range of f is C, i.e., f(P)=C.

176

176

Functions – example where range ⊊ co-domain

Let us re-specify f as follows:

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

- Is f still a function? Answer: Yes.
- The range of f is just {Moscow, Boston, Hong Kong}

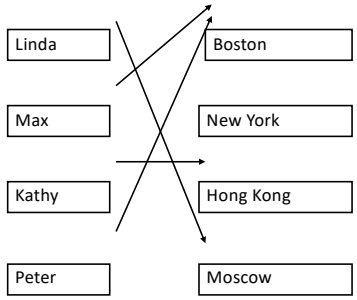
177

177

Functions – table or bipartite-graph representations

- Other ways to represent a function f:

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



178

178

Functions

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

$$f:\mathbb{R}\to\mathbb{R} \text{ with } f(x) = 2x, \forall x\in\mathbb{R}$$

This leads to, e.g.,

- $f(1) = 2$
- $f(3) = 6$
- $f(-2.5) = -5$

179

179

Sums and products of functions

- Let f_1 and f_2 be functions from A to $\mathbb{R}$.
- Then the sum and the product of f_1 and f_2 are also functions from A to $\mathbb{R}$ defined by:
  $(f_1 + f_2)(x) = f_1(x) + f_2(x), \forall x\in\mathbb{R}$
  $(f_1 f_2)(x) = f_1(x)\, f_2(x), \forall x\in\mathbb{R}$

- Examples: $\forall x\in\mathbb{R}$:
  $f_1(x) = 3x,\ f_2(x) = x + 5$
  $(f_1 + f_2)(x) = f_1(x) + f_2(x) = 3x + x + 5 = 4x + 5$
  $(f_1 f_2)(x) = f_1(x)\, f_2(x) = 3x(x + 5) = 3x^2 + 15x$

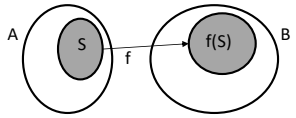
180

180

Functions – image of a domain subset

- Recall the range of a function f:A→B is the set of all images f(x) of elements x∈A, denoted f(A).
- If we only regard a subset S⊆A, the set of all images of elements s∈S is called the image of S.
- We similarly denote the image of S by f(S):

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



181

181

Functions

Consider the following function:

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

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

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

182

182

Properties of Functions – one-to-one/injective

- A function f:A→B is said to be one-to-one (or injective), if
  $\forall x,y \in A, f(x) = f(y) \Rightarrow x = y.$
- Since f is a function, we can state that it's one-to-one if
  $\forall x,y \in A, f(x) = f(y) \Leftrightarrow x = y.$
- In other words: f is one-to-one if and only if it does not map two distinct elements of A onto the same element of B.
- That is, the above (first) definition in (logically equivalent) contrapositive form is: A function f:A→B is said to be one-to-one (or injective), if
  $\forall x,y \in A, x \neq y \Rightarrow f(x) \neq f(y).$

183

183

Properties of Functions – one-to-one: example

Consider the functions f and g:

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

- Is f one-to-one?
- No, Max and Peter are mapped onto the same element of the image.

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

- Is g one-to-one?
- Yes, each element is assigned a unique element of the image.

184

184

Properties of Functions – disproving one-to-one property

- How can we prove that a function f is one-to-one?
- Whenever you want to prove something, first take a look at the relevant definition(s); here,

  $\forall x,y \in A, x \neq y \Rightarrow f(x) \neq f(y)$
- Example:

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

  Note $\sim[\forall x,y \in A, x \neq y \Rightarrow f(x) \neq f(y)] \equiv \exists x,y \in A$ s.t. $x \neq y \wedge f(x)=f(y)$

  Disproof of one-to-one statement by counterexample: x=3, y=-3, i.e., $3 \neq -3$ but $f(3) = f(-3)$, so f is not one-to-one.
- For $\mathbb{R}$-valued functions, there is the horizontal line test: i.e., if you can draw a horizontal line that meets the graph of the function at more than one point, then the function is not one-to-one.
- If bipartite-graph representation of f (with finite-sized domain and co-domain) has two arrows that meet at the same co-domain element, then f is not one-to-one.

185

185

Properties of Functions – one-to-one example

- … and yet another example:
  $f:\mathbb{R}\rightarrow\mathbb{R}$ with $f(x) = 3x$
- Def'n: $f:A\rightarrow B$ is one-to-one, or injective, if: $\forall x,y \in A, f(x) = f(y) \Rightarrow x = y$.
- **Exercise:** Write this definition in contrapositive form.
- To show f is one-to-one consider arbitrary $x,y \in A$ such that

  $f(x) = f(y) \Rightarrow 3x = 3y \Rightarrow x=y$.

186

186

Increasing and decreasing functions are one-to-one

- Consider a function f:A→B with A,B ⊆ ℝ (both ordered sets).
- f is called strictly increasing, if
  $\forall x,y \in A,\ x < y \Leftrightarrow f(x) < f(y)$,
- f is strictly decreasing, if
  $\forall x,y \in A,\ x > y \Leftrightarrow f(x) < f(y)$.

- **Exercise:** Prove that a function that is either strictly increasing or strictly decreasing is one-to-one
  - by using the original definition of one-to-one and contradiction, and
  - by using the contrapositive fprm and a direct proof.

187

187

Properties of Functions – onto/surjective, bijective

- A function f:A→B is called onto, or surjective, if and only if for every element y∈B there is an element x∈A with f(x) = y.
- In other words, f is onto if and only if its range is its entire co-domain, i.e. f(A)=B.
- Recall that a set S is countable if there is a surjective f such that f:ℕ→S.
- A function f: A→B is bijective if and only if it is both one-to-one and onto.
- **Exercise:** Prove by contraction that if f:A→B is a bijection and A and B are finite-sized sets, then |A| = |B|.

188

188

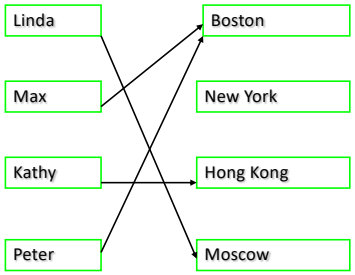
Properties of Functions - examples

- In the following examples, we use the bipartite-graph (arrows) representation to illustrate functions f:A→B.
- In each example, the complete sets A and B are shown.

189

189

Properties of Functions - example

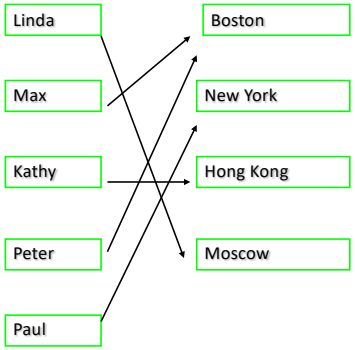


- Is f injective?
- No.
- Is f surjective?
- No.
- Is f bijective?
- No.

190

190

Properties of Functions - example

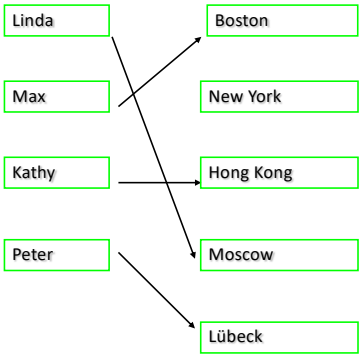


- Is f injective?
- No.
- Is f surjective?
- Yes.
- Is f bijective?
- No.

191

191

Properties of Functions - example

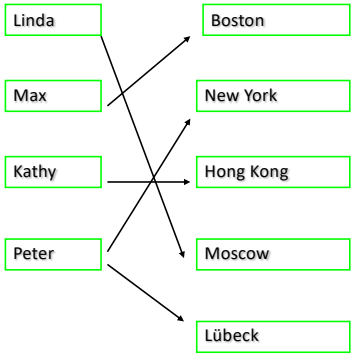


- Is f injective?
- Yes.
- Is f surjective?
- No.
- Is f bijective?
- No.

192

192

Properties of Functions - example

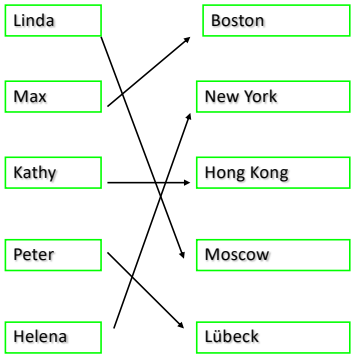


- Is f injective?
- No.
- f is not even a function because x=y does not imply that f(x)=f(y) for the case where x=Peter, i.e., f is two valued at Peter: f(Peter)={New York, Lubeck}.

193

193

Properties of Functions - example



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

194

194

Inversion

- An interesting property of bijections is that they have an **inverse function**.
- The **inverse function** of the bijection f:A→B is also a function denoted f^{-1}:B→A with
  $f^{-1}(y) = x$ whenever $f(x) = y$.
- To see why, note that
  - f is onto implies that $f^{-1}(y)$ is defined $\forall y \in B$
  - f is one-to-one implies that $f^{-1}(y)$ is a unique $\in A$
- Sometimes bijections are called invertible functions.

195

195

Inversion - example

Example:

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

Clearly, f is bijective.

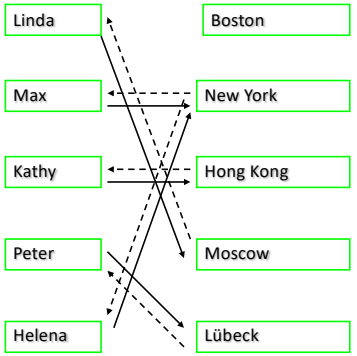
The inverse function f^{-1} is given by:

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

196

196

Inversion - example



f

f^{-1}

f^{-1}:C→P is not a function because

- it is not defined for all elements of C (i.e., for Boston), and
- it assigns two images to its pre-image New York.

197

197

Relations

- A broader family of mappings $f:A \rightarrow 2^B$ are *relations* from A to B, i.e., f *relates* elements $x \in A$ to subsets of B.
- It's possible that for some $x \in A$, $f(x)=\phi$, i.e., no elements of B are related to $x \in A$ under f.
- If $\forall x \in A$, f(x) is a singleton subset of B, then relation f corresponds to a function from A to B.
- So, if a function f is not a bijection, f^{-1} is only a relation.
- For example, if $f:\mathbb{R} \rightarrow \mathbb{R}$ is a function such that $f(x)=x^2$ then $f^{-1}:\mathbb{R} \rightarrow \mathbb{R}$ is relation such that $f^{-1}(x)=\phi$ for $x<0$ and $f^{-1}(x)=\{\pm\sqrt{x}\}$ for $x \geq 0$.

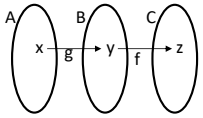
198

198

Composition

- The composition of two functions g:A→B and f:B→C, denoted by f∘g , is defined by

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



- This means that:
  - First, function g is applied to element x∈A mapping it onto an element y=g(x) of B,
  - Then, function f is applied to this element of y∈B, mapping it onto an element z=f(y)=f(g(x)) of C.
  - Therefore, the composite function f∘g:A→C (maps from A to C).
- Note that g∘f is well defined if the range f(B) ⊆ A, i.e., f(B) ⊆ A∩C

199

199

Composition - example

- Example:
- $f(x) = 7x - 4$, $g(x) = 3x$,
- $f:\mathbb{R}\to\mathbb{R}$, $g:\mathbb{R}\to\mathbb{R}$
- $(f \circ g)(5) = f(g(5)) = f(15) = 105 - 4 = 101$
- $(f \circ g)(x) = f(g(x)) = f(3x) = 21x - 4$
- **Exercise:** Show $g \circ f \neq f \circ g$

200

200

Composition with inverse

- Composition of a *bijection* and its inverse:

  $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x, \ \forall x.$

- The composition of a function and its inverse is the **identity function**

  $f^{-1} \circ f = f \circ f^{-1} = I$

  where $I(x) \equiv x$.
- When $f:A \rightarrow B$ is not a bijection (i.e., f^{-1} is a relation), then

  $(f^{-1} \circ f)(x) = \{a$

201

201

Graphs of functions

- The **graph** of a function $f:A \rightarrow B$ is the set of ordered pairs

  $\{(x, y) \mid x \in A \text{ and } y = f(x)\} = \{(x,f(y)) \mid x \in A\} \subseteq A \times B.$

- The graph can be used to visualize f in a two-dimensional coordinate system.
- Plotting the graph with the domain as a horizontal axis:
- All horizontal lines cut the graph of a one-to-one (injective) function less than 2 places.
- All horizontal lines cut the graph of an onto (surjective) function in at least 1 place.

202

202

Recall Floor and Ceiling Functions

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

203

203

The Pigeonhole Principle

- **The pigeonhole principle:** If $(k + 1)$ or more objects are placed into k boxes, then there is at least one box containing two or more of the objects.
- **Example 1:** If there are 11 players in a soccer team that wins 12-0, there must be at least one player in the team who scored at least twice.
- **Example 2:** If you have 6 classes from Monday to Friday, there must be at least one day on which you have at least two classes.
- We now prove the pigeonhole principle by contradiction:
  - Assume $\forall k \in \mathbb{Z}^+$, all k boxes have < 2 objects, i.e., has 1 or 0 objects.
  - Thus the total number of objects $\leq k < k+1$ (a contradiction).
  - Q.E.D.

204

204

The Generalized Pigeonhole Principle

- **The generalized pigeonhole principle:** If N objects are placed into k boxes, then there is at least one box containing at least $\lceil N/k \rceil$ of the objects.
- **Example 1:** In a 62-student class, at least $13=\lceil 62/5 \rceil$ students will get the same letter grade, of which there are 5 different ones (A, B, C, D, or F).
- **Exercise:** Prove the generalized pigeonhole principle by contradiction.
  Hint: $\forall x \in \mathbb{R}, \lceil x \rceil - 1 < x$

205

205

The Pigeonhole Principle - Examples

- **Example 2:** Assume you have a drawer containing a random distribution of a dozen identical brown socks and a dozen identical black socks, all loose in the drawer. It is dark, so how many socks do you have to pick to be sure that among them there is a matching pair?
- There are two types of socks, so if you pick at least 3 socks, there must be either at least two brown socks or at least two black socks
- That is, by the generalized pigeonhole principle, we want to find the integer n such that $\lceil n/2 \rceil = 2$. The solution is n=3.
- **Exercise:** Show using the generalized pigeonhole principle that if 67 different numbers are chosen from the set of the first 99 natural numbers {1,2,…,98,99}, then at least three chosen numbers will be consecutive. Hint: consider 33 "bins" corresponding to the three-tuples (1,2,3), (4,5,6), …, (94,95,96), (97,98,99).

206

206

Pigeonhole principle example: Dirichlet's Approximation Theorem

- **Theorem:** $\forall a \in \mathbb{R}$ and $\forall$ positive $N \in \mathbb{Z}$, $\exists\ p,q \in \mathbb{Z}$ such that $1 \le q \le N$ and $|qa-p| < 1/N$.
- Note: This implies that for any irrational a, there is a rational p/q such that $|a-p/q| < 1/(qN) \le 1/N$, i.e., an arbitrarily close approximation by a rational.
- Thus, $\mathbb{Q}$ is a dense subset of $\mathbb{R}$, and since $\mathbb{Q}$ is countable, we say that (uncountable!) $\mathbb{R}$ is separable.
- Dirichlet, who employed the pigeonhole principle to prove this theorem, also coined the name for this method of argument.
- Note that you can intuitively do such approximations (given a decimal expansion of an irrational) by truncating its decimal expansion, the truncation being rational: if one truncates at the kth decimal digit, then the resulting approximation error is $<10^{-k}$

207

207

Proof of Dirichlet's Approximation Theorem

- If a is rational, we are done by definition. So suppose a is irrational.
- Define $f(a) = a - \lfloor a \rfloor$ as the fractional part of $a \in \mathbb{R}$, so that $f: \mathbb{R} \to (0,1)$.
- Divide the interval [0,1) into N subintervals of equal length, 1/N.
- Consider the set of numbers $\{f(an) \mid n \in \{1,2,\ldots,N+1\}\}$.
- **Exercise:** One can easily show that there are N+1 different numbers in this set (otherwise there is a contradiction of the irrationality of a).
- So, by the pigeonhole principle, there must be two different numbers from this set that are in the same subdivision, say
  $k/N \le f(an), f(am) < (k+1)/N$ for some $k \in \{0,1,2,\ldots,N-1\}$ with $n > m$.
- So, $1/N > |f(an)-f(am)| = |an - \lfloor an \rfloor - (am - \lfloor am \rfloor)|$
- We can take $q = n-m$ and $p = \lfloor an \rfloor - \lfloor am \rfloor$.
- Q.E.D.

208

208

Introduction to Discrete Mathematics

Recursions

This revision © G. Kesidis (2013)
This document revision is copy-left 2013.
It is licensed under a Creative Commons
Attribution-Noncommercial-Share Alike 3.0 United States License

209

Outline

- Definition of a recurrence relation and initial conditions defining a numerical sequence.
- Numerically generating the sequence by iterative substitution from initial conditions.
- Verifying an explicit formula (solution) to the recurrence relation by strong induction.
- Heuristic techniques for solving recursions.
- Systematic solution of a linear and time-invariant recurrence relation.
- Examples.

210

210

Recursively defined sequences

- Consider a sequences of numbers $x_0, x_1, x_2, x_3, \ldots$
- Sequences can be explicitly specified with a function $f:\mathbb{Z}^{\geq 0} \rightarrow \mathbb{R}$, i.e.,
  $x_n = f(n)$, for all $n \in \{0,1,2,3, \ldots\}$.
- For example, the harmonic sequence $x_n = 1/(n+1)$, for all $n \geq 0$.
- Alternatively, we can define the sequence "recursively" by expressing
  x_n as a function of $x_{n-1}, x_{n-2}, x_{n-3}, \ldots, x_0$, for all $n \in \{1,2,3, \ldots\}$.
- That is, in a recursive specification, a sequence element is defined in terms of past elements.
- For many problems of interest, there is a finite "order" or "degree", say k, of the recursion in that each sequence element can be specified (recursively) only in terms of the past k values of the sequence, i.e.,
  x_n as a function of $x_{n-1}, x_{n-2}, x_{n-3}, \ldots, x_{n-k}$, for all $n \in \{k,k+1,k+2, \ldots\}$
  where
  $x_0, x_1, x_2, \ldots x_{k-1}$
  are the k "initial conditions" of the sequence for the recursion.

211

211

Recursively defined sequences – computing terms

- Given a recursion of finite order k,
  $x_n = g_n(x_{n-1}, x_{n-2}, x_{n-3}, \ldots, x_{n-k})$ for $n \geq k$,
  (i.e., given g_n) and given the k initial conditions
  $x_0, x_1, x_2, \ldots x_{k-1}$,
  we can iteratively substitute to compute
  $x_k, x_{k+1}, x_{k+2}, \ldots$
- For example, suppose k=2, $x_n = g_n(x_{n-1}, x_{n-2}) = x_{n-1}+3nx_{n-2}+7$ for $n \geq 2$, $x_0=1$, $x_1=0$.
- By substitution:
  $x_2 = g_2(x_1, x_0) = x_1+3\cdot 2\cdot x_0+7 = 0 +3\cdot 2\cdot 1+7 = 13$
  $x_3 = g_3(x_2, x_1) = x_2+3\cdot 3\cdot x_1+7 = 13 +3\cdot 3\cdot 0+7 = 20$
  $x_4 = g_4(x_3, x_2) = x_3+3\cdot 4\cdot x_2+7 = 20 +3\cdot 4\cdot 13+7 = 183$
  etc.
- Note how both the recursion g_n and the initial conditions affect the outcome
- Note: This example is time-varying because the coefficient of x_{n-2}, 3n, depends on index n (time).

212

212

Recursively defined sequences – checking a solution

- Suppose a putative explicit formula ("solution") $x_n = f(n)$ for a given recursion $x_n = g_n(x_{n-1}, x_{n-2}, x_{n-3}, \ldots, , x_{n-k})$, for $n \geq k$, and i.c.'s $x_0, x_1, x_2, \ldots x_{k-1}$.
- To verify the solution, we need to check
  $f(n) = x_n$ for all $0 \leq n \leq k-1$ (i.e., the initial conditions) and
  $f(n) = g_n(f(n-1), f(n-2))$ for arbitrary $n \geq k$ … by strong induction!
- **Example:** Theorem: $x_n = f(n) = 2(-2)^n - 2.5n(-2)^n$ is the solution to
  $x_n = -4x_{n-1} - 4x_{n-2}$ for $n \geq 2$, $x_0 = 2$, $x_1 = 1$.
- **Proof:** To verify this solution, first check the k=2 initial conditions:
  $f(0) = 2(-2)^0 - 2.5 \cdot 0 \cdot (-2)^0 = 2 = x_0$
  $f(1) = 2(-2)^1 - 2.5 \cdot 1 \cdot (-2)^1 = -4 + 5 = 1 = x_1$
- For an arbitrary $n \geq 1$, assume $x_m = f(m)$ up to $m = n$.
- To prove the claim for n+1:

$$\begin{aligned} x_{n+1} &= -4x_n - 4x_{n-1} && \text{(by the given recursion)} \\ &= -4f(n) - 4f(n-1) && \text{(by the inductive assumption)} \\ &= -4[2(-2)^n - 2.5n(-2)^n] - 4[2(-2)^{n-1} - 2.5(n-1)(-2)^{n-1}] \\ &= f(n+1). \text{ Q.E.D.} \end{aligned}$$

- **Exercise:** verify the last equality.
- **Exercise:** Explain why $n \geq 1$ in the inductive assumption and not $n \geq 0$ or $n \geq 2$.

213

213

Solving simple first-order recursions: Arithmetic and geometric progressions

- Recall the (first order) arithmetic progression,
  $x_n = x_{n-1} + d$ for $n \geq 1$, with initial condition x_0
- Thus, for $n \geq 0$,

$$\begin{aligned} x_n &= (x_{n-2} + d) + d \text{ (substituting for } x_{n-1}) \\ &= x_{n-2} + 2d \\ &= x_{n-n} + nd \text{ (after n such substitutions)} \\ &= x_0 + nd \quad (=f(n)) \quad \text{for } n \geq 0 \end{aligned}$$

- Similarly, for a geometric progression,
  $x_n = rx_{n-1}$ for $n \geq 1$, with initial condition x_0 ,
  the solution is
  $x_n = r^n x_0 \quad (=f(n)) \quad \text{for } n \geq 0$

214

214

Solving simple first-order recursions: Arithmetic and geometric progressions

- We can, e.g., sum a sequence to create another
  $s_n = \sum_{i=0}^{n} x_i$ i.e., $s_n = s_{n-1} + x_n = s_{n-1} + x_0 + nd$
- s is a first order recursion.
- Recall that if x is arithmetic then the solution for s is:
  $s_n = (n+1)(x_n + x_0)/2 = (n+1)(2x_0 + nd)/2$
- If x is geometric, then the series recursion is
  $s_n = s_{n-1} + x_n = s_{n-1} + x_0 r^n$
  and recall that the solution for s is:
  $s_n = x_0 (r^{n+1} - 1)/(r-1)$.

215

215

Solving linear and time-invariant recurrence relations of finite degree

- Suppose that the recurrence relation is of finite degree/order k and is linear and time-invariant:
  $x_n = \sum_{i=1}^{k} a_i x_{n-i} = g(x_{n-1}, x_{n-2}, x_{n-3}, \ldots, , x_{n-k})$, (*)
  where g is linear (the a_i are all scalars) and does not depend on index/time (n).
- Given the k initial conditions, one employ the theory of Z-transforms to derive an explicit formula for x_n for all $n \geq k$.
- Equivalently, find the roots of the (characteristic) polynomial
  $Q(z) = z^k - \sum_{i=1}^{k} a_i z^{k-i}$.
- By the fundamental theorem of algebra, there are k such roots (or characteristic modes), $r_1, r_2, \ldots r_k$
- Exercise: Verify $x_n = r^n$ satisfies the recursion (*) above $\forall$ roots r of Q.
- In general, the roots r may be repeated and may be complex, but if complex they come in complex-conjugate pairs because all coefficients a_i of Q are assumed real.

216

216

Linear and time-invariant recurrence relations of finite degree

- Assuming none of the roots r of Q are not repeated (i.e., each is just a single root of Q), we can write an explicit formula for x_n (i.e., "solve" x_n):

  $x_n = \sum_{i=1}^{k} c_i r_i^n$ for all $n \geq 0$

  where the k scalars c_i are found by using the k given initial conditions, i.e., solve the k equations,

  $x_n = \sum_{i=1}^{k} c_i r_i^n$ $k-1 \geq n \geq 0$,

  for the k unknowns $c_1, c_2, \ldots c_k$
- If the root r of Q is of multiplicity $m \leq k$, then use the following m "linearly independent" characteristic modes in the solution above (instead of m instances of r_i^n):

  r_i^n , nr_i^n , $n^2 r_i^n$, ... $n^{m-1} r_i^n$,

  see the previous example for root r=-2 of order m=2.

217

217

Linear and time-invariant recurrence relations of finite degree

- For example, suppose and $x_n = g_n(x_{n-1}, x_{n-2}) = 3x_{n-1} - 2x_{n-2}$ for $n \geq 2$, and $x_0 = 1$, $x_1 = -1$.
- Here, k=2 and $Q(z) = z^2 - 3z + 2 = (z-2)(z-1)$
- So, the roots of Q are 2 and 1.
- Thus, the solution $x_n = f(n) = c_2 2^n + c_1 1^n = c_2 2^n + c_1$ for $n \geq 0$.
- To solve for the scalars c_2 , c_1 , use the given initial conditions:

  $f(0) = c_2 + c_1 = 1 = x_0$

  $f(1) = 2c_2 + c_1 = -1 = x_1$

  leading to

  $c_2 = -2$ and $c_1 = 3$.
- Thus, $x_n = -2^{n+1} + 3$ for $n \geq 0$.

218

218

Solving more general forms of recurrence relations

- Systematic approaches to the LTI recursion can be extended to consider given "input" (or forcing) function, so that the solution can be written as a sum of
  - a solution depending only on the initial conditions (zero input response) and
  - another solution depending only on the given input function (zero initial state response);
  - e.g., the constant input (7) of the previous affine example.
- Systematic approaches to the solution of more general (e.g., nonlinear) forms of recurrence relations may not exist.
- Sometimes, iterative substitution or numerically evaluating the sequence for several instances will give some insight and be the basis of a guess about the solution.
- Any guess should be checked by strong inductive proof, of course.

219

219

The Tower of Hanoi

- In the 3-peg Tower of Hanoi problem, a stack of disks initially reside on a single peg, while the other two pegs are empty.
- The disks are all of different widths.
- Initially, they are stacked in width-order such that the largest disk is at the bottom, i.e., they form a cone shape on the peg.
- The problem is to move all the disks from peg to peg so that
  - they form the same cone on a different peg, and
  - a large disk is never set down upon a smaller disk on a peg.

220

220

The Tower of Hanoi - 3 pegs

- Let x_n = be the minimum number of moves/steps required to move n disks.
- Thinking "inductively", suppose we have n+1 disks on peg 1.
- Leave the largest disk at bottom alone, and move the remaining n disks to peg 2 in x_n steps.
- Move the largest $(n+1)^{st}$ to peg 3, requiring 1 step.
- Finally, move the n disks from peg 2 to peg 3 (atop the largest disk), again requiring x_n steps.
- So, $x_{n+1} = x_n + 1 + x_n = 2x_n + 1$ steps.

221

221

The Tower of Hanoi (cont)

- To see why this recursion gives the minimal number of moves, note that one simply cannot move the largest disk until on of the other two pegs is empty.
- When this occurs, only the largest disk is on one peg, one peg is empty, and the third peg must have all n other disks stacked by width order.
- That is, to get to the point where one can allowably move the large disk requires a minimum of x_n steps/moves of the n smaller disks.
- Now how this argument does not hold if there are four or more pegs because need not stack all n smaller disks on a single post before we can move the larger one.
- So, in the case of 4 or more posts, we can use the above argument only to conclude is that

  $x_{n+1} \leq 2x_n + 1$.

222

222

The Tower of Hanoi (cont)

- For the 3-peg problem, note that
  $x_{n+1} = 2x_n + 1$ for $n > 1$ with $x_1 = 1$
  is a first order recursion with constant input 1.
- Numerically evaluating the sequence, we get
  1, 3, 7, 15, 31, …
  from which we can guess $x_n = 2^n - 1$ for $n \geq 1$.
- The zero input response (to just the initial conditions) is
  $x_n = 2^{n-1} x_1 = 2^{n-1}$ for $n \geq 1$
- The zero (initial) state response (to just the input 1) is
  $x_n = 2^{n-1} - 1$ for $n \geq 0$;
  (this can be systematically found by convolution or Z-transform).
- So, the total response is
  $x_n = 2^{n-1} + 2^{n-1} - 1 = 2^n - 1$ for $n \geq 1$.

223

223

Example: Choosing your noodles

- Consider a bowl with n noodle strands, each with 2 ends.
- Two noodle-ends are independently chosen uniformly at random from the bowl; if both ends belong to the same noodle, the noodle is removed from the bowl, otherwise the ends are joined to form a longer noodle which is returned to the bowl.
- This process is repeated until the bowl is empty (in n steps).
- Find the expected number X_n of noodles EX_n drawn from the bowl.
- Clearly $1 \leq X_n \leq n$.

224

224

Example: Choosing your noodles (cont)

- To obtain the answer, consider what happens in the first choice:
  - with probability $n/C(2n,2)=1/(2n-1)$ the ends of the same noodle are chosen, i.e., $X_n = 1+ X_{n-1}$
  - with probability $1- 1/(2n-1)$ the ends of the different noodles are chosen, i.e., $X_n = X_{n-1}$
- So, by *conditioning on the first choice,*

  $EX_n = (1+ EX_{n-1}) \cdot 1/(2n-1) + (EX_{n-1})\cdot(1-1/(2n-1))$

  $= 1/(2n-1) + EX_{n-1}$

  where we have obviously used the linearity property of expectation.
- By recursive substitution,

  $EX_n = 1/(2n-1) + 1/(2n-3) + \ldots + 1/3 + 1,$

  where

  $EX_1 = X_1 = 1$, i.e., X_1 is constant.
- This question was asked during Qualcomm job interviews in 2011.

225

225

Finding the maximum of a unimodal function by sectional search

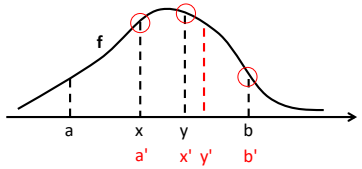
- A function $f:[a,b] \to \mathbb{R}$ is strictly unimodal over an interval $[a,b] \subseteq \mathbb{R}$ if
  - it has a unique maximizing point $z \in [a,b]$,
  - f is strictly increasing on [a,z], and
  - f is strictly decreasing on [z,b].
- The objective is to find z by sampling f in [a,b].
- But assume f (x) is very costly to evaluate for all points $x \in [a,b]$.
- Initially, for "sectional" search, we have
  - interval $I(0)=[a,b]$,with endpoints $a(0)=a$ and $b(0)=b$
  - Two initial intermediate points $x(0),y(0) \in I(0)$ such that $a(0)<x(0)<y(0)<b(0)$.
  - The function f evaluated at all of these four points.

226

226

Finding the maximum of a unimodal function by sectional search

- Since f is unimodal:
  If $f(x(0)) \geq f(y(0))$ then $z \in [a(0),y(0)]$,
  else if $f(x(0)) \leq f(y(0))$ then $z \in [x(0),b(0)]$
- That is, we can determine the sub-interval containing the f-maximizing point z if we have two intermediate points.
- Note that one cannot make this determination if only one intermediate point is used.
- The plan is to shrink the interval down to the sub-interval containing z in the next iteration, and to do so by a constant factor for every iteration.



227

227

Finding the maximum of a unimodal function by sectional search

So, for the nth interval $I(n)=[a(n),b(n)]$, $n \geq 0$:

- if $f(x(n)) \geq f(y(n))$ then:
  - $a(n+1)=a(n)$ and $b(n+1)=y(n)$, (since $z \in [a(n),y(n)]$)
  - select a point $v \in [a(n+1),b(n+1)]$,
  - evaluate f(v), and
  - take $\{x(n+1),y(n+1)\}=\{x(n),v\}$ s.t. $x(n+1)<y(n+1)$
- else:
  - $a(n+1)=x(n)$ and $b(n+1)=b(n)$, (since $z \in [x(n),b(n)]$)
  - select a point $v \in [a(n+1),b(n+1)]$,
  - evaluate f(v), and
  - take $\{x(n+1),y(n+1)\}=\{y(n),v\}$ s.t. $x(n+1)<y(n+1)$
- If f is also continuous near its maximum, a natural stopping rule for search is when the interval becomes smaller than a predefined threshold, otherwise n++ and repeat the above.

228

228

Finding the maximum of a unimodal function by golden-section search

- Note that , beyond preserving
  $a(n) < x(n) < y(n) < b(n)$,
  we haven't yet precisely specified how sectional search works.
- Suppose our objective is: for each iteration n:
  - evaluate f at just one new point v (except at two points initially (n=0)), and
  - reduce the width of the interval by the same factor, g.
- That is, let $d(n)=b(n)-a(n)$ be the interval width, and suppose that, for all n, we wish to fix the proportions
  $g:=[y(n)-a(n)]/d(n) = [b(n)-x(n)]/d(n)$
  $\Rightarrow [b(n)-y(n)]/d(n) = 1-[y(n)-a(n)]/d(n) = 1-g.$
- So, if $a(n+1)=x(n)$ and $b(n+1) = b(n)$, so that $d(n+1)=gd(n)$, we then assign $x(n+1)=y(n)$ and take $v=y(n+1)>x(n+1)$ such that $g=[v-a(n+1)]/d(n+1)$.
- Thus also $g=[b(n+1)-x(n+1)]/d(n+1)$ which implies
  $g = [b(n)-y(n)]/[g\, d(n)] = (1-g)/g$

229

229

Finding the maximum of a unimodal function by golden-section search

- So,
  $g = (1-g)/g$, i.e.,
  $g^2 + g - 1 = 0.$
- Therefore,
  $g = (-1 + 5^{0.5})/2 \approx 0.618$
- 1+g is the "golden ratio" of ancient Greece.
- If the stopping threshold is positive $\theta \ll 1$ then because the length of the intervals satisfies the recursion $d(n+1)=gd(n)$, the number of iterations N required by golden-section search is the smallest integer N s.t.
  $d(N)=d(0)g^N < \theta$, i.e.,
  $N=\lceil \log(\theta/d(0))/\log(g) \rceil$.
- So, the computational complexity of golden-section search is $\Theta(N)$.

230

230

Introduction to Discrete Mathematics

Introduction to Complexity

This revision © G. Kesidis (2013)

This document revision is copy-left 2013.

It is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License

Note: these slides adapted in part from those of S.J. Lomonaco Jr., available at
http://www.csee.umbc.edu/~lomonaco/f05/203/Slides203.html

Algorithms

- What is an algorithm?
- An algorithm is a finite set of precise instructions for performing a computation or for solving a problem.
- This is a rather vague definition. You will get to know a more precise and mathematically useful definition.
- But this one is good enough for now…

Algorithms

- An algorithm has an
  input from a specified set,
  and produces an
  output from a specified set (solution).

- Properties of algorithms:
- **Definiteness** of every step in the computation,
- **Correctness** of output for every possible input,
- **Finiteness** of the number of calculation steps,
- **Effectiveness** of each calculation step and
- **Generality** for a class of problems.

233

233

Algorithm Example: Find the Maximum

- We will use a pseudocode to specify algorithms, which slightly reminds us of Basic and Pascal.

- Example:

procedure max(a_1, a_2, …, a_n: integers)
  max := a_1
  for i := 2 **to** n
    if max < a_i **then** max := a_i

- Note that the procedure finds "max" = largest element of {a_1, a_2, …, a_n}

234

234

Algorithm Example: Linear Search of Unordered List

- Another example: a linear search algorithm, that is, an algorithm that linearly searches a sequence for a particular element.

procedure linear_search(x: integer; a_1, a_2, …, a_n: integers)
i := 1
while (i ≤ n and x ≠ a_i)
i := i + 1
if i ≤ n **then** location := i
else location := 0

- Note that location is the subscript of the term that equals x, or is zero if x is not found
- Also, the worst-case number of iterations is n-1.

235

235

Algorithm Example: Binary Search of Ordered List

- If the terms in a sequence are ordered, a binary search algorithm is more efficient than linear search.
- The binary search algorithm iteratively restricts the relevant search interval until it closes in on the position of the element to be located.

236

236

Algorithm Example: Binary Search of Ordered List (cont)

```
procedure binary_search(x: integer; a1, a2, ..., an: integers)
i := 1   {i is left endpoint of search interval}
j := n   {j is right endpoint of search interval}
while (i < j)
begin
        m := ⌊ (i + j)/2 ⌋
        if x > am then i := m + 1
        else j := m
end
if x = ai then location := i
else location := 0
```

- **Note:** location is the subscript of the term that equals x, or is zero if x is not found
- **Exercise:** Show that in the worst case, the number of iterations i required satisfies $1 = n/2^i$, i.e., $i = \log_2(n)$
- Compare the problem addressed by this algorithm to that of golden-section search (assuming unimodal function).

237

237

Complexity

- We are typically not so much interested in the time and space (memory size) complexity for very small inputs sizes.
- For example, while the difference in time complexity between linear and binary search is meaningless for a sequence with $n = 10$ elements, it is gigantic for $n = 2^{30}$.

238

238

Complexity - example

- For example, let us assume two algorithms A and B that solve the same class of problems of "size" n, where n reflects the amount of input data.
- The time complexity of A is 5,000n, the one for B is $\lceil 1.1^n \rceil$ for an input with n elements.
- For n = 10, A requires 50,000 steps, but B only 3, so B seems to be superior to A.
- For n = 1000, however, A requires 5,000,000 steps, while B requires 2.5×10^{41} steps.

239

239

Complexity - example (cont)

- This means that algorithm B cannot be used for large inputs, while algorithm A is still feasible.
- So what is important is the **growth** of the complexity functions.
- The growth of time and space complexity with increasing input size n is a suitable measure for the comparison of algorithms.

240

240

Complexity - example (cont)

- Comparison: time complexity of algorithms A and B

Input Size	Algorithm A	Algorithm B
n	5,000n	$\lceil 1.1^n \rceil$
10	50,000	3
100	500,000	13,781
1,000	5,000,000	2.5×10^{41}
1,000,000	5×10^9	4.8×10^{41392}

241

241

The Growth of Functions

- The growth of functions is usually described using the **big-O notation**.
- **Definition:** Let f and g be functions from the integers or the real numbers to the real numbers.
- We say that f is of order at most g (or just of order g), i.e., f(x) is O(g(x)) (or just f=O(g)) if there are positive constants C, k <∞ such that

  $|f(x)| \leq C|g(x)|$ whenever $x > k$,

  i.e., the inequality holds for all sufficiently large x.

242

242

The Growth of Functions

- When we analyze the growth of **complexity functions**, f(x) and g(x) are always positive.
- Therefore, we can simplify the big-O requirement to

  $f(x) \leq C \cdot g(x)$ whenever $x > k$,

  i.e., absolute values are not necessary.
- If we want to show that f=O(g), we only need to find **one** pair (C, k), never unique, that make the inequality work.

243

243

The Growth of Functions

- The idea behind the big-O notation is to establish an **upper bound** for the growth of a function f(x) for large x.
- This bound is specified by a function g(x) that is usually much **simpler** than f(x).
- We accept the constant C in the requirement

  $f(x) \leq C \cdot g(x)$ whenever $x > k$,

  because **C does not grow with x.**
- We are only interested in large x, so it is OK if $f(x) > C \cdot g(x)$ for $x \leq k$.

244

244

The Growth of Functions – Polynomial Example

- Example: Show that $f(x) = x^2 + 5x + 1$ is $O(x^2)$.
- For $x > 1$ we have:

  $x^2 + 5x + 1 \leq x^2 + 5x^2 + x^2$
  $\Rightarrow x^2 + 5x + 1 \leq 7x^2$
- Therefore, for $C = 7$ and $k = 1$,

  $f(x) \leq Cx^2$ whenever $x > k$

  $\Rightarrow f(x)=O(x^2)$.

245

245

Complexity Example

- What does the following algorithm compute?

```
procedure who_knows(a1, a2, …, an: integers)
    m := 0
    for i := 1 to n-1
        for j := i + 1 to n
            if |ai – aj| > m then m := |ai – aj|
```

- Answer: (the returned value of) m is the maximum difference between any two numbers in the input sequence, $\max_{i<j} |a_i - a_j|$
- Number of comparisons made in the procedure are
  $n-1 + n-2 + n-3 + \ldots + 1 = (n-1)n/2 = 0.5n^2 - 0.5n = C(n,2)$
- So, time complexity of the procedure is $O(n^2)$.

246

246

Complexity Example

- Another algorithm solving the same problem:

procedure max_diff(a_1, a_2, …, a_n: integers)
  min := a_1
  max := a_1
  for i := 2 to n
    if a_i < min **then** min := a_i
    else if a_i > max **then** max := a_i
  m := max - min

- That is, $\max_{i<j} |a_i - a_j| = \max_i a_i - \min_i a_i$
- The number of comparisons in this procedure is 2n - 2

- So, the time complexity is O(n).

247

247

The Growth of Functions – common simple functions

- Common "simple" functions g(n) are
  1, 2^n, n^2, n!, n, n^3, log(n), n log(n), etc.
- **Exercise:** Do we need to specify the base of the log in O(log n)?
- Listed from slowest to fastest growth:
  1
  log(n) … binary search of ordered list
  n … linear search of unordered list is O(n)
  n log(n) … some sorting algorithms are O(n logn)
  n^2
  n^3
  2^n
  n!
  n^n

- Note: cost of sorting n-list may be amortized over m searches:
  nlogn + mlogn = m ((nlogn)/m + logn) < mn for sufficiently large m

248

248

Simple Properties for Big-O

- For any **polynomial** $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, where $a_0, a_1, \ldots, a_n$ are real numbers,
  $f(x)$ is $O(x^n)$, i.e., $\exists\ C,k>0$ s.t. $|f(x)| \leq C\ \ \forall x \geq k$
- To see why note that by the triangle inequality
  $|f(x)| \leq \sum_{k=0}^{n} |a_k x^k| = \sum_{k=0}^{n} |a_k| x^k \leq (\sum_{k=0}^{n} |a_k|) x^n$ for $x \geq \max\{1,k\}$
- Similarly, one can use the triangle inequality to show the next two statements.
- If $f_1 = O(g)$ and $f_2 = O(g)$, then
  $f_1 + f_2 = (g)$; for example, see polynomial f above.
- More generally, if $f_1 = O(g_1)$ and $f_2 = O(g_2)$, then
  $f_1 + f_2 = O(\max\{g_1, g_2\})$; order of tandem algorithms is most complex one.
- If $f_1 = O(g_1)$ and $f_2 = O(g_2)$, then
  $f_1 f_2 = O(g_1 g_2)$; each iteration of one algorithm calls another.

249

249

The Growth of Functions – Imprecision of big-O

- If C is very large in order for the upper bound to hold, then the big-O bound may be crude.
- Also, if k is much larger than the job sizes x seen in practice, then the big-O bound may not be relevant.
- For algorithms of complexity f on large inputs x, we can ask the following type of question:
  If $f(x)$ is $O(x^2)$, is it also $O(x^3)$?
- The answer is **Yes:** x^3 grows faster than x^2, so x^3 also grows faster than $f(x)$.
- Therefore, we always want to find the **smallest** simple-function g for which $f = O(g)$.

250

250

Ω and Θ notation

- We say f is of order at least g, i.e., $f = \Omega(g)$, if $\exists$ positive $c,k<\infty$ such that
  $|f(x)| \geq c|g(x)| \ \ \forall x>k$.
- We say f is of order exactly g (or just of order g), i.e.,
  $f=\Theta(g)$ if $\exists$ positive $C,c,k<\infty$ such that
  $C|g(x)| \geq |f(x)| \geq c|g(x)| \ \ \forall x>k$.
- Clearly, $f= \Theta(g) \Leftrightarrow f =O(g)$ and $f=\Omega(g)$.
- The simple properties for Big-O mentioned above have analogs for Ω and Θ.
- Note that when authors say just "of order g" they often mean $=O(g)$.

251

251

The Growth of Functions – Rational Polynomial Example

Example: Show that $f(x) = (x^5 + 2x + 1)/(5x^2+6x)$ is $\Theta(x^3)$.

- As above, we have $x^5 + 2x + 1 = O(x^5)$ with k=1 and C=4, and $5x^2+6x = O(x^2)$ with k=5 and C=11.
- But also, $x^5 + 2x + 1 \geq x^5$ for all x>1, so $x^5 + 2x + 1 = \Omega(x^5)$ with k=1 (also with k=0) and C=1.
- Similarly, $5x^2+6x =\Omega(x^2)$ with k=1 and C=5.
- Thus, by using the upper bound on the numerator and lower bound on the denominator, we get $f(x)= O(x^3)$ because $f(x) \leq Cx^3$ whenever $x > k$ with k=1 and C=4/5.
- Or just $f(x)= O(x^5)/\Omega(x^2) =O(x^3)$.
- Similarly, by using the lower bound on the numerator and the lower bound on the denominator, we get $f(x)= \Omega(x^3)$ because $f(x) \geq Cx^3$ whenever $x > k$ with k=1 and C=1/11.
- Or just, $f(x)= \Omega(x^5)/O(x^2) = \Omega(x^3)$.
- Thus, $f(x)=\Theta(x^3)$.
- Note how we established the simpler result that $x^5 + 2x + 1 = \Theta(x^5)$.
- **Exercise:** Prove this result by first using polynomial long division on f.
- **Exercise:** Prove $5x^2-6x = \Omega(x^2)$. Hint: consider $5x^2(1-6/(5x))$ for large x.

252

252

Problem tractability and solvability

- A problem that can be solved with polynomial worst-case complexity is called **tractable**.
- Problems of higher complexity are called **intractable.**
- There are some well-known problems for which the question of tractability is not known, e.g., the travelling salesman problem.
- Problems that no algorithm can solve are called **unsolvable**.
- More on this subject in later courses…

253

253

Introduction to Discrete Mathematics

Relations

This revision © G. Kesidis (2013)

This document revision is copy-left 2013.
It is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License

Note: these slides adapted in part from those of S.J. Lomonaco Jr., available at
http://www.csee.umbc.edu/~lomonaco/f05/203/Slides203.html

254

254

Relations

- If we want to describe a relationship between elements of two sets A and B, we can use **ordered pairs** with their first element taken from A and their second element taken from B.
- Since this is a relation between **two sets**, it is called a **binary relation**.
- **Definition:** Let A and B be sets. A binary relation from A to B is a subset of $A \times B$.
- In other words, for a binary relation R we have $R \subseteq A \times B = \{(a,b) \mid a \in A, b \in B\}$.
- We may also use the notation aRb to denote that $(a, b) \in R$.

255

255

Relations

- When (a, b) belongs to R, a is said to be **related** to b by R.
- **Example:** Let P be a set of people, C be a set of vehicles, and D be the relation describing which person drives which vehicle(s).
- P = {Carl, Suzanne, Peter, Carla},
- C = {Mercedes, BMW, tricycle},
- D = {(Carl, Mercedes), (Suzanne, Mercedes),(Suzanne, BMW), (Peter, tricycle)}
- This means that Carl drives a Mercedes, Suzanne drives a Mercedes and a BMW, Peter drives a tricycle, and Carla does not drive any of these vehicles.
- That is, Carl D Mercedes.
- Note how Carla does not drive anything and how Suzanne drives more than one vehicle - for either of these reasons, R is not a function.

256

256

Functions as Relations

- You might remember that a **function** f from a set A to a set B (f:A→B) assigns a single element b ∈ B to each element a ∈ A, i.e., f is a function from domain A to co-domain B if

  ∀a ∈ A, ∃ unique b ∈ B s.t. b=f(a).
- Recall that we do not mean that there is a single element of B to which f maps all elements of A, i.e., notice the difference between the above definition of a function and

  ∃ unique b ∈ B s.t. ∀a ∈ A, b=f(a).
- So, we can define the relation corresponding to function f as

  {(a,f(a)) | a ∈A}.
- Conversely, if R is a relation from A to B such that every element in A is the first element of exactly one ordered pair of R, then a function can be defined using R.
- This is done by assigning to each element a∈A the unique element b∈B such that (a, b)∈R.

257

257

Relations on a (single) set

- **Definition:** A relation *on the set* A is a relation from A to A.
- In other words, a relation on the set A is a subset of A×A=A^2.
- **Example:** Let A = {1, 2, 3, 4}. Which ordered pairs are in the relation

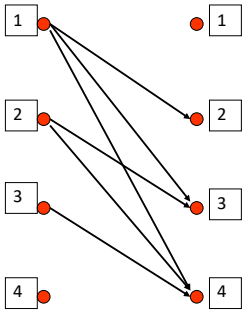
  R = {(a, b) | a < b} ?
- **Solution:** R = {(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)}

258

258

Relations – Bipartite Graph Depiction (both domain and co-domain depicted)

- **Example :** $R = \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$

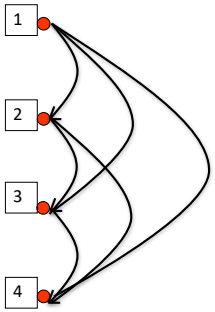


259

259

Relations on a single set – directed graph (digraph) depiction

- **Example :** $R = \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$



260

260

Relations – adjacency matrix

- **Example Solution:** R = {(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)}
- Note: row is domain element and columns are co-domain elements

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

R	1	2	3	4
1		x	x	x
2			x	x
3				x
4				

261

261

Number of Relations on a Set

How many different relations can we define on a set A with n elements?

- A relation on a set A is a subset of A×A.
- How many elements are in A×A ?
- There are n^2 elements in A×A, so how many subsets (= relations on A) does A×A have?
- The number of subsets that we can form out of a set with m elements is 2^m.
- Therefore, $2^{n^2} = 2^{n \cdot n}$ subsets can be formed out of A×A.

262

262

Properties of Relations on a Set - Reflexivity

- We will now look at some useful ways to classify relations.
- **Definition:** A relation R on a set A is called **reflexive** if $(a, a) \in R$ for every element $a \in A$, i.e.: $\forall a \in A$, aRa.
- Are the following relations on {1, 2, 3, 4} reflexive?
- $R = \{(1, 1), (1, 2), (2, 3), (3, 3), (4, 4)\}$ …No, missing (2,2)
- $R = \{(1, 1), (2, 2), (2, 3), (3, 3), (4, 4)\}$ … Yes.
- $R = \{(1, 1), (2, 2), (3, 3)\}$ … No, missing (4,4)
- **Definition:** A relation on a set A is called **irreflexive** if $(a, a) \notin R$ for every element $a \in A$, i.e.: $\forall a \in A$, $(a,a) \notin R$.
- Note that a reflexive relation will have an adjacency matrix with diagonal all 1s (diag(R)=$\underline{1}$), while an irreflexive relation's adjacency matrix will have diagonal all 0s (diag(R)=$\underline{0}$).
- Also, all elements will have self loops in the directed-graph depiction of a reflexive relation , while an irreflexive relation will have no self-loops.
- None of the three examples above are irreflexive.
- Previous "<" relation was irreflexive, while "≤" is reflexive.

263

263

Properties of Relations on a Set - Symmetry

- A relation R on a set A is called **symmetric** if :
  $(b, a) \in R$ whenever $(a, b) \in R$; equivalently,
  $\forall a,b \in A$, if $(a, b) \in R$ then $(b, a) \in R$.
- Note that if R is symmetric, its adjacency matrix $R=R^T$ (its transpose).
- A relation R on a set A is called **antisymmetric** if :
  $\forall a,b \in A$, if $(a, b) \in R$ and $(b, a) \in R$ then $a=b$
  $\equiv$ $\forall a,b \in A$, if $a \neq b$ then $(a, b) \notin R$ or $(b, a) \notin R$
- A relation R on a set A is called **asymmetric** if:
  $\forall a,b \in A$, if $(a, b) \in R$ then $(b, a) \notin R$.
- Note that if $(a,a) \in R$ for some $a \in A$, then R may be antisymmetric but not asymmetric.
- **Exercise:** Argue that R is asymmetric if and only if it is irreflexive and antisymmetric.

264

264

Properties of Relations – Symmetry Examples

- Are the following relations on {1, 2, 3, 4} symmetric, antisymmetric, asymmetric, reflexive, or irreflexive?

- R = {(1, 1), (1, 2), (2, 1), (3, 3), (4, 4)} is symmetric
- R = {(1,1)} is symmetric and antisymmetric
- R = {(1, 3), (3, 2), (2, 1)} is antisymmetric, irreflexive and asymmetric
- R = {(4, 4), (3, 3), (1, 4)} is antisymmetric

265

265

Counting Relations with Properties

- How many different reflexive relations can be defined on a set A containing n elements?
  - A reflexive relation **must** contain the n elements (a, a) for every $a \in A$.
  - Consequently, we can only choose among the remaining $n^2 - n = n(n-1)$ elements to generate different reflexive relations.
  - So, there are $2^{n(n-1)}$ of them.
- How many different symmetric relations can be defined on a set A containing n elements?
  - A symmetric relation **may** contain the $n=C(n,1)$ elements (a, a) for every $a \in A$.
  - A symmetric relation **may** contain $C(n,2)= n(n-1)/2$ element pairs (a,b) and (b,a) for $a \neq b$.
  - So, there are $2^n 2^{n(n-1)/2} = 2^{n(n+1)/2}$ of them, including the null relation.
- **Exercise:** Show that the number of antisymmetric relations on a set A containing n elements is $2^n 3^{n(n-1)/2}$, and find the number of asymmetric relations. Hint: $\sum_{k=1}^{N} C(N,k)2^k = 3^N$ where $N = C(n,2)=n(n-1)/2$

266

266

Properties of Relations - Transitivity

- A relation R on a set A is called **transitive** if
  ∀ a,b,c∈A, if (a, b)∈R and (b, c)∈R, then (a, c)∈R.
- The directed-graph depiction of transitive relations have the property that all two-hop paths connecting elements also have single-hop paths connecting (relating) those elements.
- For example, "<" and "≤" are both transitive.
- Are the following relations on {1, 2, 3, 4} transitive?
- R = {(1, 1), (1, 2), (2, 2), (2, 1), (3, 3)} …Yes
- R = {(1, 3), (3, 2), (2, 1)} …No
- R = {(2, 4), (4, 3), (2, 3), (4, 1)} …No

267

267

Combining Relations

- Relations are sets, and therefore, we can apply the usual **set operations** to them.
- If we have two relations R_1 and R_2, and both of them are from a set A to a set B, then we can combine them to $R_1 \cap R_2$, $R_1 \cup R_2$, or $R_1 - R_2$.
- In each case, the result will be **another relation from A to B**.

268

268

Closure of Relations to Achieve Properties

- Suppose a relation R on a set A does not possess a property P.
- The relation S on A is called the P-closure of R if
  - R⊆S,
  - S has property P, and
  - S-R (the relations added to R to obtain S) is minimal in size.

269

269

Transitive Closure - Example

- For example, recall that R = {(1, 3), (3, 2), (2, 1)} on A={1,2,3,4} was not transitive.
- Let S=R.
- For transitive closure, we need (1,2) because (1, 3), (3, 2)∈S, so set
  S = S∪{(1,2)}.
- Similarly, we need (3,1) because (3, 2), (2, 1)∈S, so set
  S = S∪{(3,1)}.
- But adding (1,2) means we also need to add (1,1) and (2,2) since (2, 1)∈S, so set S= S∪{(1,1),(2,2)}.
- Now, (2,1) and (1,3) ∈S, so we need to add (2,3) to S and, because (3,2)∈S, we also need to add (3,3).
- Verify that S={(a,b)|a,b ∈{1,2,3}}, i.e., the "completely connected" relation on {1,2,3} ⊆A, is the transitive closure of R on A.

270

270

Combining Relations by Composition

- **Definition:** Let R be a relation from a set A to a set B and S a relation from B to a set C. The **composite** of R and S is the relation consisting of ordered pairs (a, c), where $a \in A$, $c \in C$, and for which there exists an element $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$:
- We denote this composite of R and S by $S \circ R$.
- Again,
  If $(a, c) \in S \circ R$ then $\exists\, b \in B$ s.t. $(a, b) \in R$ and $(b, c) \in S$
- Also:
  If $(a, b) \in R$ and $(b, c) \in S$, then $(a, c) \in S \circ R$

271

271

Combining Relations - Example

- **Example:** Let D and S be relations on $A = \{1, 2, 3, 4\}$.
- $D = \{(a, b) \mid b = 5 - a\}$ "b equals (5 – a)"
- $S = \{(a, b) \mid a < b\}$ "a is smaller than b"
- Equivalently,
  $D = \{(1, 4), (2, 3), (3, 2), (4, 1)\}$
  $S = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$
- $S \circ D = \{(2,4),(3,3),(3,4),(4,2),(4,3),(4,4)\}$
- D maps an element a to the element (5 – a), and afterwards S maps (5 – a) to all elements larger than (5 – a), resulting in
  $S \circ D = \{(a,b) \mid b > 5 - a\}$, equivalently $S \circ D = \{(a,b) \mid a + b > 5\}$.
- **Exercise:** Find $D \circ S$ and compare with $S \circ D$.

272

272

Combining a Relation with Itself

- **Definition:** Let R be a relation on the set A. The powers R^n, n = 1, 2, 3, …, are defined inductively by

  $R^1 = R$, and

  $R^{n+1} = R^n \circ R$ for $n \geq 1$.

- In other words:

  $R^n = R \circ R \circ \ldots \circ R$ (n relations R composed)

273

273

Self-Combining Transitive Relations

Theorem: The relation R on a set A is transitive if and only if $R^n \subseteq R$ for all positive integers n.

Proof:

- Recall that A relation R on a set A is called transitive if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$ for all $a, b, c \in A$.
- So by definition, transitivity of $R \Leftrightarrow R \circ R \subseteq R$.
- What remains to prove is that if R is transitive, then $R^n \subseteq R$ for all integers $n > 2$.
- This can be easily shown by induction, i.e., composition of R^{n-1} by (transitive) R does not add relations not already $\in R$.
- Q.E.D.

274

274

Partial-order relations (PORs)

- A relation R on A is a **partial-order relation (POR)** if it is **reflexive, antisymmetric, and transitive**.
- For example, if A is a set of sets and R is the subset relation $\subseteq$, then R is a POR because $\subseteq$ is clearly reflexive and transitive, and for any two *different* subsets $a,b \in A$, if $a \subseteq b$ then $b \not\subset a$ (i.e., $\subseteq$ is antisymmetric).
- **Exercise:** Check that the divides "|" relation on $\mathbb{Z}$ is a POR.
- Note that the relations $>$ and $<$ on $\mathbb{R}$ are not PORs because they are not reflexive.
- Order relations are sometimes called strong or weak depending on whether they are reflexive-and-antisymmetric (as $\geq$ and $\leq$) or asymmetric (as $<$ and $>$) – we will not consider such qualifications here.

275

275

Total-order relations (TORs)

- A relation R on A is **total** if
  $\forall a,b \in A$, if $a \neq b$ then $(a,b) \in R$ or $(b,a) \in R$ but not both.
- That is, R on A is total if every pair of elements in A is comparable/relatable.
- A relation R on A is a **total-order relation (TOR)** if it is a **total POR**.
- For example, if A is a set of real numbers then any $R \in \{\leq, \geq\}$ is a TOR.
- With a total order relation R, all elements of a countable set A can be enumerated as $\{a_n\}=A$ so that $(a_n, a_{n+1}) \in R$ for all n.
- Note that $\subseteq$ may not be total, and hence not a TOR, because it's possible to have two different sets $a,b \in A$ such that $b \not\subset a$ and $a \not\subset b$, e.g.,
  $a=\{1,2,3\}$ and $b=\{2,3,4\}$.

276

276

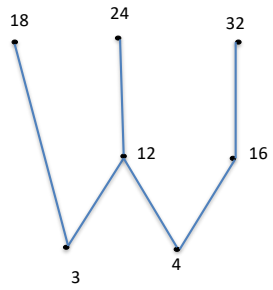
Chains and extrema in PORs

- A **chain** of a POR R on A is a subset B ⊆ A such that P is a TOR on B.
- For example, for the divides "|" relation on A={3^k4^i : k,i ∈ {0,1,2,3,4}}, the sets {3,9,27} and {1,4,12,36} are chains.
- If we interpret aRb as b is "greater than or equal to" for a POR R, then we have the following notions:
- A maximal element is the largest element of a chain, if it exists.
- A greatest element is the unique maximal element, if it exists.
- A minimal element is the smallest element of a chain, if it exists.
- A least element is the unique maximal element, if it exists.
- For the above example, the least element is 1 and the greatest 3^44^4.
- But for the same divides relation on {3,4,12,16,18,24,32}, the minimal elements are 3,4, the maximal ones are 18,24,32, and there is neither a greatest nor least element.

277

277

Hasse Diagrams for PORs – Example: divides on {3,4,12,16,18,24,32}



278

278

Equivalence Relations - Definition

- **Equivalence relations** are used to relate objects that are similar in some way.
- **Definition:** A relation on a set A is called an **equivalence relation** if it is **reflexive, symmetric, and transitive.**
- Two elements that are related by an equivalence relation R are called **equivalent**.

279

279

Equivalence Relations –Definition (cont)

- Since R is **symmetric**, a is equivalent to b whenever b is equivalent to a.
- Since R is **reflexive**, every element is equivalent to itself.
- Since R is **transitive**, if a and b are equivalent and b and c are equivalent, then a and c are equivalent.
- Obviously, these three properties are necessary for a reasonable definition of equivalence.

280

280

Equivalence Relations - Example

Example:

Suppose that R is the relation on the set of strings that consist of English letters such that aRb if and only if l(a) = l(b), where l(x) is the length of the string x.

Is R an equivalence relation?

Solution:

- R is reflexive, because l(a) = l(a) and therefore aRa for any string a.
- R is symmetric, because if l(a) = l(b) then l(b) = l(a), so if aRb then bRa.
- R is transitive, because if l(a) = l(b) and l(b) = l(c), then l(a) = l(c), so aRb and bRc implies aRc.
- R is an equivalence relation.

281

281

Equivalence Classes

- **Definition:** Let R be an equivalence relation on a set A. The set of all elements that are related to an element a ∈ A is called the **equivalence class** of a.
- The equivalence class of a with respect to R is denoted by $\mathbf{[a]_R}$.
- When only one relation is under consideration, we will delete the subscript R and write **[a]** for this equivalence class.
- If $b \in [a]_R$, b is called a **representative** of this equivalence class and we can write $[a]_R = [b]_R$.

282

282

Equivalence Classes - Example

- **Example:** In the previous example (strings of identical length), what is the equivalence class of the word mouse, denoted by [mouse] ?
- **Solution:** [mouse] is the set of all words containing five English letters.
- For example, "horse" would be a representative of this equivalence class.

283

283

Equivalence Classes and Set Partitions

- **Theorem:** If R is an equivalence relation on a set A, then the following statements are equivalent:
  - aRb
  - $[a] = [b]$
  - $[a] \cap [b] \neq \varnothing$
- **Definition:** A **partition** of a set A is a collection of disjoint nonempty subsets of A that have A as their union (i.e., that "cover" A).
- In other words, the collection of subsets S_i, $i \in I$, forms a partition of A if and only if
  - $S_i \neq \varnothing$ for $i \in I$
  - $S_i \cap S_j = \varnothing$ if $i \neq j$
  - $\cup_{i \in I} S_i = A$

284

284

Equivalence Classes - Examples

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

- {{m, o, c, k}, {r, u, b, s}} yes.
- {{c, o, m, b}, {u, s}, {r}} no (k is missing).
- {{c, o, m, t}, {b,u, s}, {r}} no (t ∉ A).
- {{u, m, b, r, o, c, k, s}} yes (A is the trivial 1-partition of itself).
- {{b, o, o, k}, {r, u, m}, {c, s}} yes ({b,o,o,k} = {b,o,k}).
- {{u, m, b}, {r, o, c, k, s}, ∅} no (∅ is not allowed as a partition element).

285

285

Equivalence Classes and Set Partitions (cont)

Theorem:

- If R is an equivalence relation on a set A, then the **equivalence classes** of R form a **partition** of A.
- Conversely, given a partition $\{S_i \mid i \in I\}$ of the set A, there is an equivalence relation R that has the sets S_i, $i \in I$, as its equivalence classes.

Proof:

- The proof of the first statement follows directly by definition (the previous Theorem).
- Given a partition of A, one can construct the corresponding equivalence relation by simply "relating" (in every way) elements of A that are part of the same partition element, and by not relating (in any way) elements of A from different partitions.

286

286

Equivalence Classes - Example

- **Example:** Let us assume that Frank, Suzanne and George live in Boston, Stephanie and Max live in Lübeck, and Jennifer lives in Sydney.
- Let R be the **equivalence relation** {(a, b) | a and b live in the same city} on the set P = {Frank, Suzanne, George, Stephanie, Max, Jennifer}.
- Then R = {(Frank, Frank), (Frank, Suzanne), (Frank, George), (Suzanne, Frank), (Suzanne, Suzanne), (Suzanne, George), (George, Frank), (George, Suzanne), (George, George), (Stephanie, Stephanie), (Stephanie, Max), (Max, Stephanie), (Max, Max), (Jennifer, Jennifer)}.
- **Exercise:** Can one construct an equivalence relation on P if Suzanne also lived in Sydney?

287

287

Equivalence Classes – Example (cont)

- Then the **equivalence classes** of R are:

  {{Frank, Suzanne, George}, {Stephanie, Max}, {Jennifer}}.
- This is a **partition** of P.
- The equivalence classes of any equivalence relation R defined on a set S constitute a partition of S, because every element in S is assigned to **exactly one** of the equivalence classes.
- If the elements of a set P are listed by equivalence class, then the adjacency matrix of the equivalence relation is block diagonal.
- For the previous example with P={F,Su,G,St,M,J},

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

288

288

Equivalence Classes – Modulo Relation

- **Another example:** Let R be the relation $\{(a, b) \mid a \equiv b \pmod 3\}$ on the set of integers.
- Is R an equivalence relation?
- Yes, R is reflexive, symmetric, and transitive.

- What are the equivalence classes of R ?
- [0]={{…, -6, -3, 0, 3, 6, …},
  [1]={…, -5, -2, 1, 4, 7, …},
  [2]={…, -4, -1, 2, 5, 8, …}}

289

289

Introduction to Discrete Mathematics

Introduction to Modular Arithmetic and Public Key Cryptography

This revision © G. Kesidis (2013)

This document revision is copy-left 2013.
It is licensed under a Creative Commons
Attribution-Noncommercial-Share Alike 3.0 United States License

This slidedeck was revised from those available at
http://www.cs.kent.edu/~rothstei/modular_arith.ppt
http://homepages.gold.ac.uk/rachel/CIS326week5lession1.ppt

290

Definition of modulo operator

- The remainder after dividing integer k by $n \neq 0$ denoted
  k mod n or k%n
- That is r=k mod n means n|(k-r) or $\exists\ q \in \mathbb{Z}$ s.t. $k = nq + r$.
- This **representative** remainder is in range
  {0,1,2,…,n-1}
- So, the set of integers $\mathbb{Z}$ is divided into n equivalence classes by the mod n operator, i.e., two integers k and m are in the same equivalence class if they are congruent mod n, i.e., if
  $k \equiv m \bmod n$,
  equivalently:
  $k \bmod n \equiv m \bmod n$,
  $0 \equiv (k-m) \bmod n$,
  $k-m \equiv 0 \bmod n$.
- Congruence (equivalence) mod n (i.e., equal remainders after division by n) is often signified by ≡, though we will use just = in the following.
- For example, $5 = 40 \bmod 7 = -9 \bmod 7$, so 5, 40 and -9 are in the same equivalence class (congruent) mod 7 – this equivalence class is denoted "5" because $0 \leq 5 < 7$, i.e., here "5" = [5] = {…, -9,-2,5,12,17,…}

291

291

What is modular arithmetic?

- Modular arithmetic is arithmetic with the remainders upon division by a fixed number n.
- It is based upon the idea that the remainder of the sum/difference/product of two numbers is the remainder of the sum/difference/product of the remainders.
- For an example of how mod distributes over +: if n=5,
  - $(34+7)\%5 = 41\%5 = 1$, and
  - $(34\%5+7\%5)\%5 = (4+2)\%5=1$ too

292

292

Properties of Modular Arithmetic

Theorem: $\forall n \neq 0, a, b \in \mathbb{Z}$,

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Proof of 3.: For arbitrary $n \neq 0, a, b \in \mathbb{Z}$:

- Let $R_a = a \bmod n$ and $R_b = b \bmod n$.
- So $\exists\ j,k \in \mathbb{Z}$ s.t. $a = R_a + jn$ and $b = R_b + kn$.
- Thus, the right-hand side of statement 3. is

$$\begin{aligned}(a\ b) \bmod n &= (R_a R_b + n(jR_b + kR_a + nkj)) \bmod n \\ &= R_a R_b \bmod n \\ &= [(a \bmod n)(b \bmod n)] \bmod n\end{aligned}$$

- Q.E.D.

293

293

So, what is arithmetic mod n?

- Our "numbers" are equivalence classes 0, 1, 2, ..., n-1.
- We add, subtract as usual, but subtract or add n as necessary to get an answer between 0 and n-1.
- For multiplication, the process is similar; multiply the two numbers together, and then take the remainder after dividing by n.

294

294

Some examples mod n for n= 6

- $(28 + 3)\%6 = 31\%6 = 1 = 7\%6 = 4\%6 + 3\%6 = 28\%6 + 3\%6$
- $(13 - 15)\%6 = -2\%6 = 4 = 13\%6 - 15\%6$
- $(8 \times 7)\%6 = 56\%6 = 2 = 2 \times 1 = 8\%6 \times 7\%6$
- To efficiently compute $11^{19}\ \%6$:
  - $11 = 5\%6$
  - Thus, $11^2 = 5^2\ \%6 = 1\%6$
  - Thus, $11^{19} = 11 \times (11^2)^9 = 5 \times 1^9\ \%6 = 5\%6$
- Exercise: Show $11^k = (-1)^k\ \%6$
- Exercise: Show that

  if $a^k = 1\%m$ then $a^n = a^{n\%k}\ \%m$
- Note that 1=19%2 in the above example.
- We will return efficient modular exponentiation later.

295

295

Division mod n for n=6

- To divide %6, all numbers need a multiplicative inverse %6.
- But the prime factors of 6 do not possess multiplicative inverses %6.
- Suppose otherwise, i.e., that 2 and 3 do have multiplicative inverses %6.
- Note that 1 is the multiplicative identity also for mod arithmetic, so that z is the multiplicative inverse of x mod6 iff $xz = 1\%6$.
- So, we are supposing that
  - there is a z such that $z \times 2 = 1\%6$, and
  - there is y such that $y \times 3 = 1\ \%6$.
- Thus, $z \times 2 \times y \times 3 = 1 \times 1\ \%6 = 1\%6$.
- However, $z \times 2 \times y \times 3 = 6zy = 0\ \%6$.
- This is a contradiction, so our assumption that the prime factors of 6 have a multiplicative inverse mod6 is false.
- Exercise: Repeat this argument for %9.

296

296

We will see that we can divide mod p if p is a prime.

- From now on, our modulus (divisor) will be a prime p.
- We will show how to divide in arithmetic mod p by using the **extended** Euclidean algorithm.
- Recall that the Euclidean algorithm finds the greatest common divisor (gcd) of two integers a and b…

297

297

Recall basic Euclidean Algorithm to find gcd

1. Initial data: integers n_0 , n_1 s.t. $0 \neq |n_0| \geq |n_1|$
2. set $a \leftarrow |n_0|$
3. set $b \leftarrow |n_1|$ $(\leq a)$
4. while $b > 0$ do
   $r \leftarrow a \bmod b$, with $0 \leq r < b$
   $a \leftarrow b$
   $b \leftarrow r$
5. return $a = \gcd(n_0, n_1)$

- Again, as the while loop executes, $b \geq 0$ strictly decreases and gcd(a,b) does not change - recall the well-ordering principle re. convergence of the Euclidean algorithm in finite time.
- The working of Euclid's Algorithm is made clearer by considering the **extended** Euclidean algorithm that will give integers s and t such that

$$s\, n_0 + t\, n_1 = \gcd(n_0, n_1)$$

298

298

Extended Euclidean Algorithm

1. Initial data: integers n_0 , n_1 s.t. $n_0 \geq n_1 > 0$
2. index k=1
3. If $n_1 \mid n_0$ then { Return $n_1 = \gcd(n_0,n_1) = n_0 - (-1+n_0/n_1)\, n_1$ } else:
4. while $n_k > 0$ do
   - $n_{k+1} = n_{k-1} \bmod n_k$ with $0 \leq n_{k+1} < n_k$
   - if $n_{k+1} > 0$ then
     - $n_{k+1} = n_{k-1} - q_k n_k$ with quotient $q_k > 0$
     - $= s_k n_0 + t_k n_1$ by recursive substitution (see below)
   - k++
5. Return $n_{k-1} = \gcd(n_0,n_1)$ and
6. Return integers (s_{k-2}, t_{k-2}) s.t. $s_{k-2} n_0 + t_{k-2} n_1 = \gcd(n_0,n_1)$

- Note that $s_1 = 1$ and $t_1 = -q_1$
- **Exercise:** write the pseudo-code for the recursive substitution (see the following examples).

299

299

Extended Euclidean Algorithm – Example 1

- If $n_0 = 21$ and $n_1 = 15$ then the EEA will return s=-2 and t=3, so that $s\, n_0 + t\, n_1 = 3 \cdot 15 - 2 \cdot 21 = 3 = \gcd(n_0 , n_1)$
- The steps for the EEA of this example are:

1. $6 = 21 \bmod 15$ $\Rightarrow 6 = -1 \cdot 15 + 1 \cdot 21$
2. $3 = 15 \bmod 6$ $\Rightarrow 3 = -2 \cdot 6 + 1 \cdot 15 = 3 \cdot 15 - 2 \cdot 21$ (sub 6 from step 1)
3. $0 = 6 \bmod 3$
4. Stop
5. Return $\gcd(21,15) = 3 = 3 \cdot 15 - 2 \cdot 21$

300

300

Extended Euclidean Algorithm – Example 2

- When $n_0 = 256$ and $n_1 = 100$, the steps for the EEA are:

1. $56 = 256 \bmod 100$ $\Rightarrow 56 = -2 \cdot 100 + 1 \cdot 256$
2. $44 = 100 \bmod 56$ $\Rightarrow 44 = 1 \cdot 100 - 1 \cdot 56 = 3 \cdot 100 - 1 \cdot 256$ (sub 56 of step 1)
3. $12 = 56 \bmod 44$ $\Rightarrow 12 = 1 \cdot 56 - 1 \cdot 44 = -5 \cdot 100 + 2 \cdot 256$ (sub 56,44 of steps 1,2)
4. $8 = 44 \bmod 12$ $\Rightarrow 8 = 1 \cdot 44 - 3 \cdot 12 = 18 \cdot 100 - 7 \cdot 256$ (sub 44,12 of steps 2,3)
5. $4 = 12 \bmod 8$ $\Rightarrow 4 = 1 \cdot 12 - 1 \cdot 8 = -23 \cdot 100 + 9 \cdot 256$ (sub 12,8 of steps 3,4)
6. $0 = 8 \bmod 4$
7. Stop
8. Return gcd(256,100)= 4 $= -23 \cdot 100 + 9 \cdot 256$

301

301

Division mod p for prime p – multiplicative inverse mod p

- By proof of convergence of the Extended Euclidean Algorithm in a finite number of iterations: if a and b have no common factors >1 (i.e., they are "relatively prime"), then there exist integers s, t such that
  $as + bt = 1$.
- Again, given a,b, the integers s,t are found by the EEA.
- So, for all integers b without prime factor p, we can find integers s,t such that
  $ps + bt = 1$,
  where t is called the **multiplicative inverse** of b (modulo p).
- That is, $1 = (bt)\%p = (b\%p)(t\%p)\%p$.
- The multiplicative inverse t can be reduced to a unique element of {1,2,…,p-1} by suitably selecting s. (uniqueness proved by contradiction)
- Restricting our attention to the range {1,2,…,p-1}, we have proved:

- **Theorem**: For all prime p and b∈{1,2,…,p-1}, there is a unique multiplicative inverse t ∈{1,2,…,p-1} of b such that
  $1 = (bt)\%p$

302

302

Division mod p for prime p

Theorem:
For all prime p and integers a and y without factor p but with factor x, if a%p = y then (a/x)%p = (y/x).

Proof:

- Note that x also does not have factor p by transitivity of divisibility.
- Let s ∈{1,2,…,p-1} be the mod p multiplicative-inverse of x, i.e., 1 = sx%p = (s%p) (x%p) %p
- So, (as)%p = (a/x)%p and (ys)%p = (y/x)%p.
- If a mod p = y then by multiplicative property of modulo arithmetic: (as)%p = ys.
- Q.E.D.

303

303

Modular division - example

- What is 5 ÷ 3mod11?
- Note 11 is prime.
- We need to multiply 5 by the **inverse** of 3 mod 11
- By simple arithmetic, if you multiply a number by its (multiplicative) inverse then the answer is 1 (the multiplicative identity), e.g., the multiplicative inverse of 2 is ½ since 2 × ½ = 1
- So, the inverse of 3mod11 is 4 since 3 × 4=12=1 mod 11
- Thus 5 ÷ 3mod11 = 5 × 4 mod11 = 9

304

304

Fermat's Little Theorem

Theorem: If a does not have prime factor p, then $a^{p-1} \bmod p = 1$.

Proof:

- The numbers a,2a,3a,…,(p-1)a have different remainders mod p (easily proven by contradiction).
- So, {1,2,…,p-1} and {a,2a,…,(p-1)a} are the same set of numbers mod p.
- So, the products are the same mod p, i.e.,

  $(p-1)! = a \cdot 2a \cdot 3a \ldots \cdot (p-1)a \bmod p$

  $= a^{p-1} (p-1)! \bmod p$
- Finally, since p is prime, we can divide this equation by (p-1)!.
- Q.E.D.

305

305

Chinese Remainder Theorem

- If the integers $m_1, m_2, m_3, \ldots m_k$ and $a_1, a_2, a_3, \ldots a_k$ are such that
  - the m_i are positive, pairwise relatively prime, and
  - the $a_i < m_i$ are also positive integers,
- then there exists an integer r such that $\forall i, m_i \mid r - a_i$, i.e.,

  $\forall i , a_i = r \,\%m_i$
- If we require that $r < \prod_i m_i$, then this r is unique.

306

306

Proof of Chinese Remainder Theorem

- Suffices to take k=2 because the general k≥2 is then easily proved by induction.
- Thus, we need to prove that, for $0 < a_1 < m_1$ and $0 < a_2 < m_2$ if m_1 and m_2 are relatively prime, there exists a unique r between 0 and m_1m_2 such that
  $r\%m_1 = a_1$ and $r\%m_2 = a_2$
- Since m_1 and m_2 are relatively prime, there exist integers s and t such that
  $sm_1 + tm_2 = 1$ (*).
- $r := a_2 sm_1 + a_1tm_2 \% m_1m_2$ satisfies all of the conditions.
- In particular, note that by definition of r there is an integer q such that
  $a_2 sm_1 + a_1tm_2 = qm_1m_2 + r$;
- so,
  $r\%m_1 = a_1tm_2\%m_1 = a_1(1-sm_1) \%m_1 = a_1$,
  where we used (*) for the second equality.
- Q.E.D.

Exercise: Check that the defined r satisfies the other required properties of the CRT, and prove the more general result for k>2.

307

307

The RSA Theorem

Theorem: If p and q are two different primes and the integer a is relatively prime to p and q such that $1 \le a \le pq - 1$, then for all positive integers k,

$$a^{1+k(p-1)(q-1)} = a \bmod (pq)$$

Proof:

- By Fermat's Little Theorem, $a^{p-1} = 1 \bmod p$.
- Thus, $a^{k(p-1)(q-1)} = (a^{p-1})^{k(q-1)} = 1 \bmod p$ (since mod distributes over product).
- Thus, $a^{1+k(p-1)(q-1)} = a \bmod p$ (ditto).
- Similarly, $a^{1+k(p-1)(q-1)} = a \bmod q$.
- That is, $q \mid a^{1+k(p-1)(q-1)} - a$ and $p \mid a^{1+k(p-1)(q-1)} - a$.
- So, $(pq) \mid a^{1+k(p-1)(q-1)} - a$.
- Q.E.D.

308

308

How RSA works to send confidential messages

- An individual A wishes to be able securely communicate with others (even potentially untrustworthy strangers) over an insecure communication medium.
- Take two large primes, p and q.
- Let n=pq.
- Chose an integer e, relatively prime to (p-1)(q-1).
- Using the extended Euclidean algorithm, find a d such that
  $de - k(p-1)(q-1) = 1$.
- That is, $de = 1+k(p-1)(q-1)$.
- "Publish" (n, e) as a public key, i.e., securely disseminate the public key through a trustworthy Key Distribution Center (KDC), a critical component of the public key infrastructure (PKI).
- That is, individuals are reliably "bound" to their public keys by the KDC.
- Retain (n,d) as a private key.
- Now, another individual B may encrypt a plain-text binary message "m" to A by raising m to the e^{th} power, and transmitting the cypher-text
  $m^e \%n$.
- Upon receipt, A will decrypt the cypher-text by raising it to the d^{th} power and thereby recover $m = (m^e \%n)^d = m^{ed} \%n$. Ex.: Prove.

309

309

How RSA works to sign messages

- Suppose B wishes to receive a message m from A that is signed by A in a way that cannot be later repudiated by A or easily forged by another party.
- Using its *private* key (d,n=pq), A signs the message by sending to B
  $m^d \%n$
  together with the message m (or its cypher)
- Having received this signature from A, B can "check" it by decrypting it using A's *public* key and comparing the result to the plaintext message m, i.e.,
  $(m^d \%n)^e \%n = m$
- B cannot forge A's signature without factoring n=pq and A cannot later repudiate its signature for the same reason.

310

310

Strength of RSA

- The strength of RSA public-key cryptography lies in the difficulty in factoring n to find p and q.
- That is, a third party intercepting the cypher-text a^e will also have the public key of A, particularly n, but will need to factor n to find p and q and hence d.
- So, typically, p and q are very large primes so that factoring n is difficult, though recently proved to be of polynomial complexity in the size of n.
- As of this writing, the largest prime number yet found is of the form 2^k-1 (a Mersenne prime) with k = 57,885,161.
- Fewer than 50 Mersenne primes are known.
- Exercise: Show that this prime number will be 17,425,170 decimal digits long.

311

311

"Efficient" exponentiation to compute a^n

- power(a,n):
  - set r:= 1
  - if n = 0, return r
  - while n>1 do
    - If n is odd, set r:= ar and n:=n-1
    - n:= n/2 and r:= r^2
  - return ar
- Exercise: Prove the correctness of this algorithm, i.e., that it returns a^n, by induction. What is the complexity of the algorithm?
- Recall: if j<k and $1=a^j \bmod n$, then $a^k \bmod n = a^{k \bmod j} \bmod n$.
- Recall: for primes p≠q and all a,k, $1=a^{k(q-1)(p-1)} \bmod (pq)$.

312

312

Another Crypto-system: Diffie-Hellman key exchange

- Let p be a large prime, s a number between 2 and p-2; p and s are "publicly known".
- Suppose two people wish to securely communicate and each person has a private key, respectively a and b.
- They first send each other numbers, respectively

  $x=s^a \bmod p$ and $y=s^b \bmod p$,

  i.e., employing their own private keys.
- They raise the number they receive to their private key power mod p, and thereby have a common exchange key k for a symmetric crypto-system, i.e.,

  $k = y^a \bmod p = x^b \bmod p$.

313

313

Another Crypto System: El-Gamal

- As before, let p be a large (publicly known) prime number, s some number between 2 and p-2.
- Each person chooses a private key e and "publishes"

  $E = s^e \bmod p$.
- To send message m, we first generate a "session key" k, and send $t = s^k \bmod p$ and $c = (E^k m) \bmod p$
- We decrypt by computing $t^{-e} c = m \bmod p$

314

314

Note: Symmetric Key Cryptography

- Such an asymmetric key cryptography system (Public Key Infrastructure or PKI) can be used to exchange symmetric private keys between communicating parties.
- Thereafter, a framework such as the Advanced Encryption Standard (AES) can be used to encrypt and decrypt (decipher) messages.
- AES uses multiple stages of message permutation key-based encryption and permutation.

315