Discrete Structures

Spring semester 2013

lectures:
Arjen Lenstra, INJ 330
akl at epfl dot ch

exercise sessions and homework coordination:

Anja Becker, INJ 334
anja dot becker at epfl dot ch

Alina Dudeanu, INJ 335
alina dot dudeanu at epfl dot ch

Andrea Miele, INJ 335
andrea dot miele at epfl dot ch

The book

Course is based on 7th edition of

"*Discrete Mathematics and its applications*"

by Kenneth H. Rosen
published by Mc-Graw Hill

unless you already have the 6th edition:

get the book!
(10% student discount at Librairie La Fontaine)

The purpose of this course

1. To remind all EPFL freshmen Computer Science and Communication Systems (of widely and wildly varying backgrounds) of the **basic mathematical concepts** that they are supposed to be familiar with
2. To introduce the very basics of
   - computational thinking
   - understanding if solutions scale or not

Remark

- Many subjects familiar from (the margin of) 1st semester course “Sciences de l’Information”
- Here we repeat some of those basic concepts
  - a bit more elaborately
  - often with a more “computational” focus

(from 2013-2014 academic year on
the two courses will be swapped)

Six well known and eternally confusing facts

1. Empty product equals 1; in particular: $0^0 = 1$
2. "$p \rightarrow q$" ("if p then q"): always true if p is false
3. "$p \leftrightarrow q$" ("p if and only if q")
   consists of "p if q" and "p only if q" parts:
   "$q \rightarrow p$" is the "p if q" part
   "$p \rightarrow q$" is "p only if q" part
4. "$\forall x \exists y \ldots$" in general not the same as "$\exists y \forall x \ldots$"
5. $\neg \forall x\, P(x) \equiv \exists x \neg P(x)$
6. $\neg \exists x\, P(x) \equiv \forall x \neg P(x)$

These will be explained & repeated at great length

What we will be doing, more or less

- look at “common” problems
- figure out a solution
- figure out how well the solution scales

without doing **any** actual programming

Requires *common sense* plus the basics of

- math reasoning & logic
- algorithms
- counting
- probability theory

What we will be doing, more or less

- look at "common" problems
- figure out a solution
- figure out how well the solution scales

without doing **any** actual programming

Requires *common sense* plus the basics of

- math reasoning & logic: *to understand proofs*
- algorithms: *to do useful stuff*
- counting: *to figure out algorithm speed*
- probability theory: *to know what to expect*

Example of algorithm

the medical internship problem

- medical schools rank prospective interns
- prospective interns rank medical schools

which interns to admit to which school
so that the resulting assignment is stable?

The same example, more inspiring

the stable marriage problem

- *n* girls and *n* boys
- each girl has a preference list of all boys
- each boy has a preference list of all girls

form *n* (girl,boy) pairs in such a way that:

no unmatched girl and boy prefer each other to their assigned partner (and thus run off together)

- does a stable matching always exist? *yes*
- if so, how to find one? *just let nature run its course*

Finding a stable bipartite matching

n girls and *n* boys

- each girl has a boys preference list
- each boy has a girls preference list

to find *male optimal* matching:

as long as there is an unmatched boy, say *B*:
B proposes to girl on top of his list *L*, say *G*

- if *G* is unmatched: *G* accepts *B*'s proposal
- if *G* is already matched, say to *O*:
  - if *G* prefers *O* to *B*: *B* removes *G* from *L*
  - if *G* prefers *B* to *O*: *G* dumps *O*, accepts *B*;
    and *O* removes *G* from his list

(note that girls only trade up)

Rough analysis

- algorithm results in matching:
  unmatched boy implies unmatched girl
- algorithm requires ≤ n^2 proposals:
  each boy proposes each girl at most once
- resulting matching is stable:
  if not, there is unmatched pair (B,G) where
  - B prefers G to his current partner G'
  - G prefers B to her current partner B'
    ⇒ B must have proposed G before G'
    ⇒ G must have (ultimately) rejected B

  "girls trade up" ⇒ G cannot end up with B'

More on stable matchings

outcome depends on who takes initiative:

- if boys "propose", resulting matching is male optimal and female pessimal, i.e., no boy can do better in stable matching

(and vice versa)

questions

- why does it (apparently, in real life) not work?
- what about "(fe)male-only" matchings? try 1:234, 2:314, 3:124, 4:…

Other simple examples of proofs

let k, m and n be integers

- if mn is odd, then m is odd and n is odd

  proof:

  if m is even or n is even, then mn is even

- for all k it is the case that

  if $m + n \geq 2k$, then $m \geq k$ or $n \geq k$

  proof:

  if there exists a k with $m + n \geq 2k$, $m < k$ and $n < k$, then $m + n < 2k$: contradiction

$\Rightarrow$ *what are the logic rules precisely?*

Chapter 1 of "Rosen"

Introduces

- different types of proofs
- formalization of underlying principles

Basic ingredients:

- *hypothesis*
- *conclusion*
- statement (theorem, lemma, proposition):

  " *if hypothesis then conclusion* "

  to truly understand proofs, we must

  be able to argue about truth values

Different types of proofs

(that a *hypothesis* leads to a *conclusion*):

- *Direct* proof: prove that the conclusion follows from the hypothesis
- Indirect proofs:
  - Proof by *contraposition*: prove that negation of conclusion leads to negation of hypothesis
  - Proof by *contradiction*: prove that hypothesis and negation of conclusion leads to “False”

More types of proofs

- Vacuous proof:
  hypothesis is known to be false
- Trivial proof:
  conclusion is known to be true anyhow
- Case-by-case analysis
- By (counter)example
- Constructive existence proof
- Non-constructive existence proof
  (such as based on pigeonhole principle)

proof examples done in class

- By (counter)example:
  not every general graph allows a stable matching
- Direct:
  - product of two odd integers is odd
  - inverse of a non-zero rational number is rational
- Contraposition: an even square is a square of an even number.
- Contradiction: $\sqrt{2}$ is irrational
- Constructive existence:
  there are primes of the form 12345678901234567890 1234 …
  (of 171, 277, 367, 561, 567, 18881, …?... Digits; cf. https://oeis.org/)
- Non-constructive existence:
  - There are irrational numbers x and y such that x^y is rational
  - For any integer n there is an integer multiple of n that
    consists of just ones and zeros

First sections of chapter 1

Formalization of different proof methods

proposition (p, q, r, ...): statement that is True or False (T or F, 1 or 0, Yes or No)

compound proposition: proposition consisting of other propositions and **logical operator(s)**:

$\neg$	"not"	(negation)
$\wedge$	"and"	(conjunction)
$\vee$	"or"	(disjunction)
$\oplus$	"xor"	(exclusive or)
$\rightarrow$	"implies"	(conditional, implication)
$\leftrightarrow$	"iff"	(biconditional)

justifying proof methods

let k, m and n be integers

- if mn is odd, then m is odd **and** n is odd

  proof:

  if m is even **or** n is even, then mn is even

introduced the tools to justify this proof

- **for all** k it is the case that

  if $m + n \geq 2k$, then $m \geq k$ **or** $n \geq k$

  proof:

  if **there exists** a k with $m + n \geq 2k$, $m < k$ **and** $n < k$, then $m + n < 2k$: contradiction

justification of this proof requires more tools

propositional functions (predicates)

a propositional function is a statement with variable(s) that becomes a proposition once all variable(s) have values

often denoted by capitals P, Q, …:

$P(x)$, $Q(x)$, … (“univariate”)

$R(x,y)$, $S(x,y)$, … (“bivariate”)

$T(x_1, x_2, \ldots, x_n)$, … (“n-ary”)

propositional functions

statement with variable(s) that becomes proposition once variable(s) have values

examples:

$P(x)$ is the propositional function "$x = 3$":

$P(3)$ = True, $P(0)$ = False

$R(x,y)$ is propositional function "$xy > 0$":

$R(3,2)$ = True, $P(3,0)$ = False

$T(x,y,z)$ is prop. function "$x^y + z$ is prime":

$T(5,1,0)$ = True, $T(1,1,0)$ = False

$T(0,0,6)$ = True, $T(0,1,6)$ = False

$T(5,1,z)$ or $T(5,z,0)$ are not propositions:
they are propositional functions (of z)

$T(8,1,\text{one})$ may make sense – nevertheless:
usually variables belong to an often only implicitly stated "domain of discourse"

For $T(x,y,z)$: x, y, z are integers, or reals
(with conflicts silently ignored)

$U(x,y)$ is propositional function "$xy > 0$"
$S(x,y)$ is propositional function "$xy \geq 0$"

$F(x)$ is propositional function $U(x,x)$: "$x^2 > 0$"
$G(x)$ is propositional function $S(x,x)$: "$x^2 \geq 0$"

consider real x, y (domain of discourse is **R**)

- for all x: $G(x)$ is true: $\forall x\, G(x)$
- → not for all x: $F(x)$ is true : $\neg \forall x\, F(x)$
- → not for all x: $F(x)$ is false: $\neg \forall x\, \neg F(x)$
- → there exist x: $F(x)$ is true : $\exists x\, F(x)$
- → there exist x: $F(x)$ is False : $\exists x\, \neg F(x)$
- there is just one x: $F(x)$ is False: $\exists! x\, \neg F(x)$

Quantifiers

for all x it is the case that $G(x)$ is true: $\forall\, x\, G(x)$

"$\forall$" is "**universal quantifier**"

there exists an x such that $F(x)$ is true: $\exists\, x\, F(x)$

"$\exists$" is "**existential quantifier**"

Negations of quantifiers

"it is not the case that for all x $G(x)$ is true"
is the same as
"there is an x such that $G(x)$ is false"
thus: $\neg \forall x\, G(x) \equiv \exists x\, \neg G(x)$

"it is not the case that there is x with $F(x)$ true"
is the same as
"for all x it is the case that $F(x)$ is false"
thus: $\neg \exists x\, F(x) \equiv \forall x\, \neg F(x)$

(note "De Morgan" proofs for finite domains)

$Q(x,y)$ is propositional function "$x = y$"

- for all x there is a y such that $Q(x,y)$ is True
  (take $y = x$)
  thus: $\forall\, x\, \exists\, y\, Q(x,y)$
  note: choice y depends on (and fixed by) x
- it is not the case that there is a y such that
  for all x it is the case that $Q(x,y)$ is True
  (suppose y exists, say y_0; take $x = y_0 + 1$,
  then $x \neq y_0$, and $Q(x,y_0)$ is False)
  thus: $\neg\, \exists\, y\, \forall\, x\, Q(x,y)$
  the latter equivalent to $\forall\, y\, \exists\, x\, \neg Q(x,y)$
  choice x depends on y (any $x \neq y$ works)

let $T(x,y,z)$ be "$x^y + z$ is prime",

define $R(y,z) = T(0,y,z)$ (for $y \geq 0$):

"$0^y + z$ is prime"

it is always the case that $R(y,0)$ is false:

$$\forall\, y\ \neg R(y,0)$$

but, there exists a y such that $R(y,4)$ is true

$$\exists\, y\ R(y,4)$$

the latter y is unique:

$$\exists!\, y\ R(y,4)$$

(note that this y equals 0)

let $R(y,z)$ be "$0^y + z$ is prime" (for $y \geq 0$)

from $\exists!\ y\ R(y,4)$ it follows that:

if that y is excluded, then $R(y,4)$ is false

$$\exists\, y\, [\, R(y,4) \wedge \forall\, y'\, ((\neg R(y',4)) \vee (y' = y))]$$

thus getting rid of "!" (for the purists)

note:

- $(\, (\neg R(y',4)) \vee (y' = y)\,) \equiv (\, R(y',4) \rightarrow (y' = y)\,)$
- $\forall y'(R(y',4) \rightarrow (y' = y))$ not equiv to $\exists!\ y\ R(y,4)$

$R(y,2)$ is always true: $\forall\ y\ R(y,2)$

actually: $\exists!\ z\ \forall\ y\ R(y,z)$

Summary of quantifier facts

- "for all x" expressed by "$\forall\, x$"
- "there exists an x" expressed by "$\exists\, x$"
- trivial extensions: $\forall\, x>0$, $\exists\, x\neq 0$, …
- negations:
  - $\neg \forall x\, Q(x) \equiv \exists x\, \neg Q(x)$
  - $\neg \exists x\, P(x) \equiv \forall x\, \neg P(x)$
  - $\neg \forall x\, \exists y\, R(x,y) \equiv \exists x \forall y\, \neg R(x,y)$
  - $\neg \exists x \forall y\, R(x,y) \equiv \forall x \exists y\, \neg R(x,y)$, …
- in general "$\forall x\, \exists y$" not same as "$\exists y\, \forall x$"
- but: $\exists y\, \forall x\, R(x,y) \rightarrow \forall x\, \exists y\, R(x,y)$

"**predicate calculus**": propositional functions with **quantifiers** and **logical operators**

back to still open proof example

let k, m and n be integers

- **for all** k it is the case that

  if $m + n \geq 2k$, then $m \geq k$ **or** $n \geq k$

  proof:

  if **there exists** a k with $m + n \geq 2k$, $m < k$ **and** $n < k$, then $m + n < 2k$: contradiction

let q be "$\forall k$: $m + n \geq 2k \rightarrow (m \geq k \vee n \geq k)$"

prove q by proving $\neg q \rightarrow \mathrm{F}$ (using $r \rightarrow s \equiv \neg r \vee s$):

$\neg q \equiv \exists k$: $\neg(m + n \geq 2k \rightarrow (m \geq k \vee n \geq k))$

$\equiv \exists k$: $\neg(\neg(m + n \geq 2k) \vee (m \geq k \vee n \geq k))$

$\equiv \exists k$: $(m + n \geq 2k \ \wedge \ (m < k \wedge n < k)) \rightarrow \mathrm{F}$

what is the negation of "$\exists!\ y\ S(y)$" ?

$\exists!\ y\ S(y) \equiv \exists\ y\ [\ S(y) \wedge \forall\ y'\ ((\neg\ S(y')) \vee (y' = y))]$ (cf. above)

thus: $\neg\ \exists!\ y\ S(y) \equiv \neg\ \exists\ y\ [\ S(y) \wedge \forall\ y'\ ((\neg\ S(y')) \vee (y' = y))]$

$\equiv \quad \forall\ y\ \neg\ [\ S(y) \wedge \forall\ y'\ ((\neg\ S(y')) \vee (y' = y))]$

$\equiv \quad \forall\ y\ [(\neg\ S(y)) \vee \neg(\forall\ y'\ (\ (\neg\ S(y')) \vee (y' = y)\ )\ )\ ]$

$\equiv \quad \forall\ y\ [(\neg\ S(y)) \vee (\exists\ y'\ \neg(\ (\neg\ S(y')) \vee (y' = y)\ )\ )\ ]$

$\equiv \quad \forall\ y\ [(\neg\ S(y)) \vee (\exists\ y'\ (\neg(\neg\ S(y')) \wedge \neg\ (y' = y)\ )\ )\ ]$

$\equiv \quad \forall\ y\ [(\neg\ S(y)) \vee (\exists\ y'\ (S(y') \wedge (y' \neq y)\ )\ )\ ]$

the latter implies that there is either no y for which $S(y)$ holds or there are at least two distinct y-values with $S(y)$:

"$\forall\ y\ [(\neg\ S(y))$" covers the "no y"-part. if, on the other hand, there exists at least one y for which $S(y)$ holds, take it, apply statement to it and conclude that the "$(\exists\ y'\ (S(y') \wedge (y' \neq y)\ )\ )$" must kick in, i.e., another y' (than y) with $S(y')$ = True.

exercise : let $F(x,y)$ be the statement "x can fool y", where the domain consists of all people in the world (but all below are supposed to refer to unique individuals)

use quantifiers to express each of the following statements

a) Everybody can fool Fred $\forall x\, F(x,\text{Fred})$

b) Evelyn can fool everybody $\forall y\, F(\text{Evelyn},y)$

c) everybody can fool somebody $\forall x \exists y\, F(x,y)$

d) there is no one who can fool everybody $\neg \exists x \forall y\, F(x,y)$

e) everyone can be fooled by somebody $\forall y \exists x\, F(x,y)$

f) no one can fool both Fred and Jerry $\neg \exists x(F(x,\text{Fred}) \wedge F(x,\text{Jerry}))$

g) Nancy can fool exactly two people

$\exists y \exists z(F(\text{Nancy},y) \wedge F(\text{Nancy},z) \wedge y \neq z \wedge \forall x(F(\text{Nancy},x) \rightarrow (x=y \vee x=z)))$

h) there is exactly one person whom everybody can fool $\exists! y \forall x\, F(x,y)$

i) no one can fool himself of herself $\neg \exists x\, F(x,x)$

j) there is someone who can fool exactly one person besides himself or herself $\exists x \exists y(x \neq y \wedge F(x,y) \wedge \forall z((F(x,z) \wedge x \neq z) \rightarrow y=z))$

k) Penny is the only person who can fool herself

$(\exists! x\, F(x,x)) \wedge F(\text{Penny},\text{Penny})$ or $F(\text{Penny},\text{Penny}) \wedge \forall x(F(x,x) \rightarrow x=\text{Penny})$

or $\forall x(F(x,x) \leftrightarrow x=\text{Penny})$

$\exists! x(F(x,x) \wedge x=\text{Penny})$ is incorrect: some y not Penny may satisfy F(y,y))

$\forall x(F(x,x) \rightarrow x=\text{Penny})$ is incorrect: $F(\text{Penny},\text{Penny})$ may still be false

Remember "Six well known confusing facts"?

we have seen them all already:

1. empty product equals 1; in particular: $0^0 = 1$
2. "$p \rightarrow q$", "if p then q": always true if p false
3. "$p \leftrightarrow q$", "p if and only if q" *"p si et seulement si q"*
   consists of "p if q" and "p only if q" parts:
   "$q \rightarrow p$" is the "p if q" part *"p si q"*
   "$p \rightarrow q$" is "p only if q" part *"p seulement si q"*
4. "$\forall x \exists y \ldots$" in general not same as "$\exists y \forall x \ldots$"
5. $\neg \forall x\, P(x) \equiv \exists x \neg P(x)$
6. $\neg \exists x\, P(x) \equiv \forall x \neg P(x)$

Propositional logic, rules of inference

dissecting proofs into smallest substeps

example: suppose following 2 facts are given:

1. if Eric does not have 8 legs,
   then Eric is no insect: $p \rightarrow q$
2. Eric is an insect : $\neg q$

may one conclude that Eric has 8 legs? $\rightarrow \neg p$

let p be proposition "Eric does not have 8 legs"
q proposition "Eric is no insect"

$((p \rightarrow q) \wedge \neg q) \rightarrow \neg p$ is a tautology

$p \rightarrow q$ and $\neg q$ are given thus $\neg p$ must follow

Propositional logic, rules of inference

dissecting proofs into smallest substeps

if we use just tautologies "… ∧ … → …"
then truth tables become irrelevant

such tautologies are **rules of inference**;
for historic reasons rules of inference

- have special names
- are denoted in a special way

$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$ is "*modus tollens*",
denoted $\neg q$

$\underline{p \rightarrow q}$

$\therefore \neg p$ ("$\therefore$" is " therefore")

Rules of inference

page 66 of Rosen

Rule of Inference	Name	Rule of Inference	Name
$p \to q$ p $\therefore q$	(Law of Detachment) Modus ponens	p q $\therefore p \wedge q$	Conjunction
$p \to q$ $\neg q$ $\therefore \neg p$	Modus tollens	$p \to q$ $q \to r$ $\therefore p \to r$	Hypothetical syllogism
p $\therefore p \vee q$	Addition	$p \vee q$ $\neg p$ $\therefore q$	Disjunctive syllogism
$p \wedge q$ $\therefore p$	Simplification	$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	Resolution

Rules of inference for quantified statements

page 71 (70) of Rosen

Rule of Inference	Name
$\forall x\, P(x)$ $\therefore P(d)$ if $d \in D$	Universal instantiation
$P(d)$ for every $d \in D$ $\therefore \forall x\ P(x)$	Universal generalization
$\exists x\, P(x)$ $\therefore P(d)$ for some $d \in D$	Existential instantiation
$P(d)$ for some $d \in D$ $\therefore \exists x\ P(x)$	Existential generalization

(D domain of discourse)

Using rules of inference, example

1. someone in this class visited the USA
2. anyone who visited USA likes hamburgers

$\Rightarrow$ someone in this class likes hamburgers

define: $C(x)$: "x is in this class"
$V(x)$: "x has visited the USA"
$L(x)$: "x likes hamburgers"

it is given that:

1. $\exists x\,(C(x) \wedge V(x))$
2. $\forall x\,(V(x) \rightarrow L(x))$

desired conclusion: $\exists x\,(C(x) \wedge L(x))$

Hamburger proof:

define: $C(x)$: "x is in this class"
$V(x)$: "x has visited the US"
$L(x)$: "x likes hamburgers"

given that

1. $\exists x\,(C(x) \wedge V(x))$
2. $\forall x\,(V(x) \rightarrow L(x))$

want to conclude
$\exists x(C(x) \wedge L(x))$

3. $\exists x\,(C(x) \wedge V(x))$, hypothesis (1)
4. $C(y) \wedge V(y)$, existential instantiation using (3)
5. $V(y)$, simplification using (4)
6. $C(y)$, simplification using (4)
7. $\forall x\,(V(x) \rightarrow L(x))$, hypothesis (2)
8. $V(y) \rightarrow L(y)$, universal instantiation using (7)
9. $L(y)$, modus ponens using (5) and (8)
10. $C(y) \wedge L(y)$, conjunction using (6) and (9)
11. $\exists x\,(C(x) \wedge L(x))$, existential generalization using (10)

Any questions?

Concludes some highlights of Chapter 1

Read Chapter 1
(7th edition only: better skip section 1.7)