CSC236 fall 2016

Theory of computation

Danny Heap

heap@cs.toronto.edu / BA4270 (behind elevators)

http://www.cdf.toronto.edu/~csc236h/fall/

416-978-5899

include "csc236" in subject & realize there are many of you

face-to-face is best.

also good

sometimes works...

check often

use Introduction to the Theory of Computation, Section 1.2

very solid background

Outline

Introduction

chaper 1, simple induction

Notes

why reason about computing?

- more than just hacking
  - a computer scientist analyzes as well as codes
- testing isn't enough
  - can't test every input integer, string, ...
- careful, you might get to like it (?!*)
  - weird, but true.

how to reason about computing

- it's messy... - pencil + paper
  - try out guesses, check various values
  - make many drafts.
- it's art...
  - aim for extreme clarity, readability, humor, pathos, ...
  - work on an editor/word processor to allow polishing

how to do well

- read the course information sheet as a two-way promise

  ↗ becomes policy after add date.

- question, answer, record, synthesize

  – print blank slide + annotate yourself
  – write proofs that improve on mine

- collaborate with respect, e.g. registered study group

  – annotation on your transcript!

you should already know...

- Chapter 0 material from *Introduction to Theory of Computation*

  sets, functions, etc.

- CSC165 material, especially the mathematical prerequisites (Chapter 1.5), proof techniques (Chapter 3), and the introduction to big-Oh (Chapter 4).

  – If you got less than C+ on CSC165, you may need to do extra work

- But you can relax the structure (more on this later)

  – see my induction outline

- recursion, efficiency material from CSC148

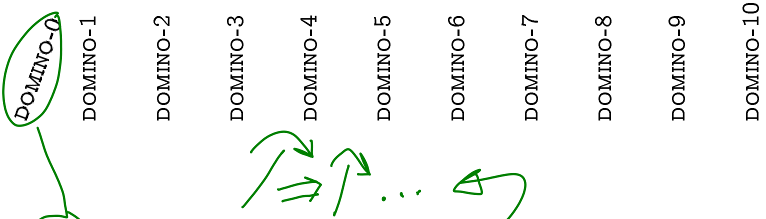
  – big-Oh

you'll know by December...

- understand, and use, several flavours of induction
  - simple
  - complete
  - structural
  - well-ordering
- complexity and correctness of programs both recursive and iterative
- formal languages, regular languages, regular expressions

  FSAs & regexes over binary strings

domino fates foretold



$$[P(0) \wedge (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1))] \Rightarrow \forall n \in \mathbb{N}, P(n)$$

Prose can be just as precise as symbols!

If the initial case works,

and each case that works implies its successor works,

then all cases work

simple induction outline

You will also see:
State claim — P(n)
base case first
H(n) → P(n)
C(n) → P(n+1)

inductive step: state inductive hypothesis $H(n)$

derive conclusion $C(n)$: show that $C(n)$ follows from $H(n)$, indicating where you use $H(n)$ and why that is valid

verify base case(s): verify that the claim is true for any cases not covered in the inductive step

this outline works for simple, complete, and (small mod) structural induction

in simple induction $H(n)$ is the claim you intend to prove about n, and $C(n)$ is the same claim about $n+1$ "simple" because the reasoning moves from n to $n+1$.

how many subsets of a set?

Subsets of {}:

{} — 1

- list the subsets of $\{7\}$

{}, {7} — 2

- now list the subsets of $\{7, 13\}$

{}, {7}, {13}, {7, 13} — 4

- is there a connection between the lists that helps you count them?

Every set with n elements has exactly 2^n subsets...

scratch work: check a few more sets...

$\{7, 13, 17\}$:

$\{\}$, $\{7\}$

$\{13\}$, $\{7, 13\}$

$\{17\}$, $\{7, 17\}$

$\{13, 17\}$, $\{7, 13, 17\}$

8

Every set with n elements has exactly 2^n subsets...

use the simple induction outline

Inductive step: Let n be an arbitrary natural number.

Assume $H(n)$: Every set with n elements has 2^n subsets.

Show $H(n)$ implies $C(n)$: Every set with $n+1$ elements has 2^{n+1} subsets.

Let S be an arbitrary set with $n+1$ elements.

Let $x \in S$ # since $n+1 > 0$, S is not empty.

Partition the subsets of S into $\wp^+$, those that x is an element of, and $\wp^-$, those that x is not an element of.

Notice that $\wp^-$ is the set of subsets of $S - \{x\}$, a set with n elements.

$|\wp^-| = 2^n$ # according to $H(n)$

$\longrightarrow$

Every set with n elements has exactly 2^n subsets...

use the simple induction outline

... continued

Notice also that there is a 1-1 correspondence between the subsets in $\mathcal{P}^-$ and those in $\mathcal{P}^+$ — subsets are matched by adding/removing x.

$|\mathcal{P}^+| = |\mathcal{P}^-| = 2^n$

Since these are all the subsets of S, S has

$2^n + 2^n = 2 \times 2^n = 2^{n+1}$ subsets.

$C(n)$ follows from $H(n)$

<u>verify base case:</u> A set with 0 elements is the empty set, and it has $1 = 2^0$ subsets, namely $\{\}$

$3^n \geq n^3$?

scratch work: check for a few values of n

$3^0 = 1 \geq 0 = 0^3$

$3^1 = 3 \geq 1 = 1^3$

$3^2 = 9 \geq 8 = 2^3$

$3^3 = 27 \geq 27 = 3^3$

$3^4 = 81 \geq 64 = 4^3$

$3^{-1} = 1/3 \geq -1 = -1^3$

$3^{-2} = \frac{1}{9} \geq -8 = -2^3$

$\vdots$

$3^{2.5} \not\geq 2.5^3$!

prove the result for natural numbers.

$3^n \geq n^3$

use the simple induction outline

Proof (simple induction)

induction step: Assume $n \in \mathbb{N}$ and $n \geq 3$, assume $H(n)$: $3^n \geq n^3$

Show that $H(n) \Rightarrow C(n)$: $3^{n+1} \geq (n+1)^3$

$$3^{n+1} = 3 \times 3^n \geq 3 \times n^3 \quad \# \text{ by } H(n)$$
$$= n^3 + n^3 + n^3$$
$$\geq n^3 + 3n^2 + 9n \quad \# \; n \geq 3$$
$$= n^3 + 3n^2 + 3n + 6n$$
$$\geq n^3 + 3n^2 + 3n + 1 \quad \# \; n \geq 3 > \frac{1}{6}$$
$$= (n+1)^3 \quad \# \text{ binomial theorem.}$$

$C(n)$ follows from $H(n)$ ⟶

$3^n \geq n^3$

use the simple induction outline

verify base case: $3^3 = 27 \geq 27 = 3^3$, so the claim holds for natural number 3.

also $3^0 = 1 \geq 0 = 0^3$ and $3^1 = 3 \geq 1 = 1^3$ and $3^2 = 9 \geq 8 = 2^3$, so the claim holds for natural numbers 0, 1, 2.

For every $n \in \mathbb{N}$, $12^n - 1$ is a multiple of 11

scratch work: substitute a few values for n

$$12^0 - 1 = 1 - 1 = 11 \times 0$$

$$12^1 - 1 = 12 - 1 = 11 \times 1$$

$$12^2 - 1 = 144 - 1 = 11 \times 13$$

For every $n \in \mathbb{N}$, $12^n - 1$ is a multiple of 11

use the simple induction outline

Proof by simple induction

Inductive step: Let n be an arbitrary natural number.

Assume $H(n)$: $12^n - 1$ is a multiple of 11.

Show $H(n) \Rightarrow C(n)$: $12^{n+1} - 1$ is a multiple of 11

Let $k \in \mathbb{Z}$ such that $11k = 12^n - 1$

by H(n) such a k exists

$12^{n+1} - 1 = 12(12^n - 1) + 11 = 12(11k) + 11$

$= 11(12k + 1)$

$12k + 1 \in \mathbb{Z}$ # 12, 1, $k \in \mathbb{Z}$ + $\mathbb{Z}$ closed under

+, ×

$12^{n+1} - 1$ is a multiple of 11.

C(n) follows from H(n)

→

For every $n \in \mathbb{N}$, $12^n - 1$ is a multiple of 11

use the simple induction outline

Verify base case $12^0 - 1 = 1 - 1 = 0 = 11 \times 0$, so claim holds for natural number 0.

The units digit of 3^n is either 1, 3, 7, or 9

scratch work: substitute a few values for n

exercise to reader.

The units digit of 3^n is either 1, 3, 7, or 9

use the simple induction outline

The units digit of 3^n is either 1, 3, 7, or 9

use the simple induction outline

What about: the units digit of 3^n is either 1, 2, 3, 7, or 9

use the simple induction outline

is the claim still true? What happens if you add this other case to the inductive step?

Notes