CSC 165

proof structure

asymptotics

week 8, lecture 1

Danny Heap

heap@cs.toronto.edu

www.cdf.toronto.edu/~heap/165/F09

for now: cut and paste,
after Nov 18th: cut to the chase

At this point we insist on a proof structure where
each assumption that is introduced is matched by explicitly stating
the conclusions you arrive at using that assumption

In about three weeks (after assignment 2) we allow,
but don't require, some relaxation of the structure.
I can illustrate this best through a few examples.

Prove: $\forall m \in \mathbb{N}, \forall n \in \mathbb{N}, (m \bmod 7 = 3 \wedge n \bmod 7 = 4) \Rightarrow mn \bmod 7 = 5$

Assume $m, n \in \mathbb{N}$ # generic natural number $(m,n) \in \mathbb{N}^2$
Assume $m \bmod 7 = 3 \wedge n \bmod 7 = 4$ # antecedent
Then $\exists k' \in \mathbb{N}, 7k'+3 = m$ # assumed $m \bmod 7 = 3$
let $k \in \mathbb{N}, 7k+3 = m$ # instantiating exist.
Then $\exists k' \in \mathbb{N}, 7k'+4 = n$ # assumed
Pick $q \in \mathbb{N}, 7q+4 = n$ # inst. exist
Then $mn = (7k+3)(7q+4)$
$= 7(7kq + 4k + 3q + 1) + 5$ # algebra
Then $\exists k' \in \mathbb{N}, mn = 7k' + 5$ # since $k' =$
$7kq + 4k + 3q + 1$
$\in \mathbb{N}$, since $7,3,4,1,k,q \in \mathbb{N}$
and $\mathbb{N}$ closed under
$+, *$

Then $mn \bmod 7 = 5$ # since $7 > 5 \geq 0$ &
remainder is unique

Then $(m \bmod 7 = 3 \wedge n \bmod 7 = 4) \Rightarrow mn \bmod 7 = 5$
introduced implication
Conclude $\forall m, n \in \mathbb{N}, (m \bmod 7 = 3 \wedge n \bmod 7 = 4) \Rightarrow mn \bmod 7 = 5$.

scratch

structural transformations

Pages 48–49 of the notes list some standard transformations used in proofs. These have the virtue that many proof practitioners will recognize them when you use them.

Work back over proofs to find:

- implication introduction — assume ant, derive cons.
- universal introduction
- existential introduction
- existential elimination

asymptotics

It probably takes you more than 4 times as long to sort a 13-card bridge hand than it takes you to sort a 5-card euchre hand.
Some people have bigger hands or more nimble fingers, but insertion sort and selection sort grow roughly as the square of their input

If you were to count the number of steps (finger or computer) for several algorithms and express them as functions of input size n, as $f(n) = n^2$, $g(n) = 3n^2$, $h(n) = 3n^2 + 1$, and $j(n) = 3n^2 + n$, a computer scientist would say they are all the "same" size: $\mathcal{O}(n^2)$.

pinning down intuition

We know, or have heard, that polynomials of the same degree grow at "roughly" the same speed

We want to make this "roughly" explicit

Here's how we define $\mathcal{O}(n^2)$, functions that eventually grow no more quickly than n^2

$$\mathcal{O}(n^2) = \{f : \mathbb{N} \mapsto \mathbb{R}^{\geq 0} \mid \exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow f(n) \leq cn^2\}$$

The definition says that there's a multiplier, c, such that if you go far enough to the right, B, the graph of f is bounded above by the graph of cn^2

Prove: $3n^2 + 2n \in \mathcal{O}(n^2)$

scratch

scratch