CSC 165

proof by cases

week 7, lecture 3

Danny Heap

heap@cs.toronto.edu

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

Assignment 1 graded, pick up at end of lecture

T2 I have some.

Assignment 2 posted, due November 13th.

Tutorials — all about proof structure

proof by cases

mathematic prerequisites

You can prove by induction (CSC236) that:

$$\forall m \in \mathbb{N}, \forall n \in \mathbb{N}, n \neq 0 \Rightarrow \exists! q \in \mathbb{N}, \exists! r \in \mathbb{N}, m = qn + r \text{ and } n > r \geq 0$$

$\exists!$ is a compact way of saying there exists exactly one.

q and r are called the quotient and remainder, respectively. We also denote r by $m \bmod n = r$

integer division — same as / % for non-neg m, n

"implementation dependent"

A consequence is that any natural number n has a remainder of either 0, 1, or 2 after division by 3. What possible remainders are there for perfect squares after division by 3?

$0^2 \bmod 3 = 0$
$1^2 \bmod 3 = 1$
$2^2 \bmod 3 = 1$
$3^2 \bmod 3 = 0$

$4^2 \bmod 3 = 1$
$5^2 \bmod 3 = 1$
$6^2 \bmod 3 = 0$

Prove: $\forall n \in \mathbb{N}, n^2 \bmod 3 \neq 2$

I think you'll need cases for different possible results of n mod 3

Assume $n \in \mathbb{N}$ # generic
Then $n \bmod 3 \in \{0, 1, 2\}$ # defn of mod 3

Case 1, assume $n \bmod 3 = 0$

Then $\exists q' \in \mathbb{N}, n = 3q' + 0$ # defn of $n \bmod 3 = 0$
Pick $q \in \mathbb{N}, n = 3q$ # since it exists
Then $n^2 = 3(3q^2)$ # algebra
Then $\exists q' \in \mathbb{N}, n^2 = 3q' + 0$ # $3q^2$, since $3, q \in \mathbb{N}$ and # $\mathbb{N}$ is closed under $*$
Then $n^2 \bmod 3 = 0 \neq 2$

Case 2, assume $n \bmod 3 = 1$

Then $\exists q' \in \mathbb{N}, n = 3q' + 1$ # defn of $n \bmod 3 = 1$

.
.
.

Then $n^2 \bmod 3 = 1 \neq 2$

scratch

Case 3, assume $n \bmod 3 = 2$

Then $\exists\, q' \in \mathbb{N},\ n = 3q' + 2$ # defn.

Pick $q \in \mathbb{N},\ n = 3q + 2$ # since it exists.

Then $n^2 = 9q^2 + 12q + 4$ # algebra.

$= 3(3q^2 + 4q + 1) + 1$ # more algebra

So $\exists\, q' \in \mathbb{N},\ n^2 = 3q' + 1$

$q' = (3q^2 + 4q + 1)$
$\in \mathbb{N}$, since $\mathbb{N}$
closed $\times, +$
and $3, 4, 1, q \in \mathbb{N}$

Then $n^2 \bmod 3 = 1 \neq 2$

Conclude $\forall\, n \in \mathbb{N},\ n^2 \bmod 3 \neq 2$ # since true # in all possible cases.

more modular arithmetic

Performing arithmetic on integers, and then taking the remainder,
can be interchanged with taking the remainder and then performing the arithmetic.
Number theory and cryptography use many such techniques.

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

An important step is to remember that $m \bmod 7 = 3$ means there are natural numbers
q and r such that $m = 7q + 3$.

$\forall m, n \in \mathbb{N}$

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 pair in $\mathbb{N}$.

Assume $(m \bmod 7 = 3 \wedge n \bmod 7 = 4)$. # antecedent

scratch

Then $mn \bmod 7 = 5$

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

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
- universal introduction
- existential introduction
- existential elimination