CSC 165

indirect proof

Danny Heap

heap@cs.toronto.edu

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

office – BA4270 (4th floor, behind elevators)

$\forall n \in \mathbb{N}, P(n) \Rightarrow Q(n)$

implication not symmetrical

proving that $p \Rightarrow q$ involves finding a chain of intermediate results

$p \Rightarrow p_1 \Rightarrow \cdots \Rightarrow p_n \Rightarrow q$

what happens if your search is unlucky?

$p \Rightarrow q$

$\neg q \Rightarrow \neg p$

try reversing the search, use the contrapositive

recall that $p \Rightarrow q$ is true exactly when $\neg q \Rightarrow \neg p$

proving one proves the other

$\forall n \in \mathbb{N}$, n even $\Rightarrow n^2$ even

for example, how would you go about proving

$\forall n \in \mathbb{N}, n^2 \text{ odd } \Rightarrow n \text{ odd}$

direct proof difficult here

$\neg P$ or Q

You could get python to verify this for lots of natural numbers

```
for n in range(0,1000) :
    n * n % 2 == 0 or n % 2 == 1
```

$\underbrace{\texttt{n * n \% 2 == 0}}_{\neg n^2 \text{ odd}}$ or $\underbrace{\texttt{n \% 2 == 1}}_{n \text{ odd}}$

$\boxed{\text{but that's pretty lame}}$

Try as an exercise

need

2 divides $mn \in \mathbb{N}$

2 divides m

or 2 divides n

or, imitate the direct proof of the converse:

Assume $n \in \mathbb{N}$,

Assume n^2 is odd. Then $\exists k \in \mathbb{N}, n^2 = 2k + 1$ # definition of odd

hmmm...should we take the square root of $2k + 1$ or what????

$\vdots$

n is even

Prove $\forall n \in \mathbb{N}, \underbrace{n^2 \text{ odd} \Rightarrow n \text{ odd}}$

same as: Prove $\forall n \in \mathbb{N}, \underbrace{\neg n \text{ odd} \Rightarrow \neg n^2 \text{ odd}}$

Assume $n \in \mathbb{N}$ # generic elt 1D

Assume n even # assume antecedent $\mathbb{N}$ 11

Then $\exists k \in \mathbb{N}, n = 2k$ # defn of even

⋮

Then n^2 is even # consequent

So n even $\Rightarrow n^2$ even # assumed antecedent,

derived consequent

Conclude $\forall n \in \mathbb{N}, n$ even $\Rightarrow n^2$ even # n was # generic

Conclude $\forall n \in \mathbb{N}, n^2$ odd $\Rightarrow n$ odd # contrapos.

slide 4

scratch

getting contradictory

$p \stackrel{?}{\Rightarrow} q$

Euclid example.

what happens if you want to prove q,
so you'd like some well-known p to imply q,
but you can't decide which p is right for the job?

entire human facts

why not just take the entire sum of well-known facts as your antecedent
$p_0 \wedge p_1 \wedge p_2 \wedge \cdots \wedge p_n \Rightarrow q$

$\neg q \Rightarrow \neg p_0 \vee \neg p_1 \vee \cdots \vee \neg p_n$

how does this help? this is equivalent to saying that
$\neg q$ implies that some well-known fact is false — contradiction!
$\neg q \Rightarrow \neg p_0 \vee \neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n$

there are infinitely many prime numbers

$P = \{n \in \mathbb{N} \mid n$ has exact 2 factors in $\mathbb{N}\}$ w/ distinct

Claim SP: $\underbrace{\forall n \in \mathbb{N}, |P| > n.}$ Prove by contradiction.) try ~~prove~~ proving directly

assume $\neg SP$, $\exists n \in \mathbb{N}, |P| \leq n$

Then $\exists k \in \mathbb{N}, |P| = k$ # $0 \leq k \leq n$

let $k \in \mathbb{N}, |P| = k$ # since it exists

Then, can list $\{p_0 = 2, p_1 = 3, \ldots, p_{k-1}\}$

Then, $\exists r \in \mathbb{N}, r = p_0 p_1 \cdots p_{k-1}$ # finite prod.

Then $r > 1$ # product of 2, 3 + bigger stuff

So $r+1 > 1$, and $\exists p \in P$ that divides $r+1$) induction

some p divides $p_0 \cdot p_1 \cdots p_k + 1$!

$\vdots$

$\rightarrow \leftarrow$

scratch

format of contradiction

Assume $\neg q$

within the assumption, follow a chain of implications

$\vdots$

arrive at a contradiction of some already-known fact

Conclude q, since assuming $\neg q$ led to a contradiction.

coursework proposal

look over the proposed course calendar at

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

and be prepared to vote on Friday October 23rd

Was 6 exercises

3 Assignmen

scratch