Proof Techniques

Prof. Forrest

02/10/2026

Warm up

1. Discuss with your neighbors which is better:
   chocolate or peanut butter

2. Suppose that the domain of the predicate $P(x)$ is $\{-2, -1, 0, 1, 2\}$.
   Write out each of these formula of predicate logic using $\vee, \wedge, \neg$

   (a) $\exists x \neg P(x)$

   (b) $\neg \exists x P(x)$

$P(-2)$

$P(-1)$

$\neg P(-2) \vee \neg P(-1) \vee \neg P(0) \vee$

$\neg P(1) \vee \neg P(2)$

$\neg P(-2) \wedge \neg P(-1) \ldots$

Logisitics

- If you got unsatisfactory in first Qeb, you may resubmit

$\forall p_1 \in P$: ColgateStudent(p_1)

quantifier — variables — domain — predicate boolean function — takes a variable

"Everyone in your class is friendly"

(a) domain is students in your class

(b) domain is the set of all people

"Everyone in your class is friendly"

(a) domain is students in your class

(b) Domain is the set of all people

$P := \{\text{all people}\}$

(a) $\forall s_1 \in C : \text{friendly}(s_1)$

for everyone all

C: Set of students in your class

(b) $\forall p \in P : \text{InClass}(p) \rightarrow \text{friendly}(p)$

~~$(\text{InClass}(p) \wedge \text{friendly}(p))$~~

not what we want

```
has IT = false
x = 'cat'
for i in ['cat', 'dog', 'lizard']:
    if i == x:
        has IT = True
```

free bound

$\forall i \in \{\text{'cat'}, \text{'dog'}, \text{'lizard'}\} : hasIF(x, i)$

Theorem: A fully quantified expression of predicate logic that is true for every assignment

$\forall p \in S : F(p)$

how do show this is wrong/false

to find a p in S such that

$F(p)$ is false

$\neg (\forall p \in S : F(p)) \equiv \exists p \in S : \neg F(p)$

$\exists x\, P(x)$

Disprove this $\forall x \neg P(x)$

$\neg(\exists x\, P(x)) \equiv \forall x \neg P(x)$

Prove this true

Find an example

$\forall p_1 \in P : \exists p_2 \in P : \text{like}(p_1, p_2)$

how do we disprove this theorem?

show ~~there~~ is a person who ~~likes everyone~~ no good

there is some person who doesn't like anyone.

$$\neg\left(\exists p_2 \in P : \forall p_1 \in P : likes(p_1, p_2)\right)$$

candidate 1: $\exists p_2 \in P : \forall p_1 \in P : \neg likes(p_1, p_2)$

wrong :(

$$\forall p_2 \in P : \exists p_1 \in P : \neg likes(p_1, p_2)$$

1. Direct proofs

2. Proofs by contraposition (contrapositive)

3. Proofs by cases

4. proofs by contradiction

Direct proof

$$\frac{p \to q \qquad p}{\therefore q}$$

Claim: if $p \to q$

Assume: p is true

steps { show that q follows logically

$\longrightarrow$ q is true

Conclusion: $p \to q$ is true

Sum of two odd integers is even

$\forall p, q \in \mathbb{Z} : (\text{odd}(p) \wedge \text{odd}(q)) \rightarrow \text{Even}(p+q)$

Assume: $\text{odd}(p) \wedge \text{odd}(q)$ is true

$5 := 2(2)+1$

p & q from $\mathbb{Z}$

$p := 2k+1$ (↑ Some integer)

$q := 2m+1$ (↑ Some integer)

Want to show: $\text{Even}(p+q)$

An integer is even if it is representable as $n := 2\ell$ for some integer ℓ

$6 := 2(3)$

$\uparrow$

same integer

$p + q = 2k+1 + 2m+1$

$= 2k + 2m + 2$

$= 2(k+m+1)$

integer

□

Even $(p+q)$ is true

Conclusion: if p and q are odd then p+q is even

Prove that if $m+n$ and $n+p$ are both even and $m, n,$ and p are integers, then $m+p$ is even

direct proof, so we assume that $m+n$ and $n+p$ are even and $m, n,$ and p are integers

Want to show: $m+p$ is even

$m+n = 2s$ $\qquad$ $n+p = 2k$

$m+n+n+p = 2s+2k$

$m+p+2n = 2s+2k$

$m+p = 2s+2k-2n$

$= 2(s+k-n)$

Proof by cases

prove some P is true. we need to show 2 sets of facts.

(1) in every case, P is true

(2) one of these cases has to hold

Let n be an integer, then $n(n+1)^2$ is even.

① n is even, $n = 2k$

$$2k(2k+1)^2 = 2k(4k^2+4k+2)$$
$$= 2\underbrace{(4k^3+4k^2+2k)}_{\text{integer}}$$

even

multiply a number by even
the whole thing is even

② n is odd. then $n+1$ is even

$n(n+1)^2$ is even

□

Proof by contraposition

$$\forall x : P(x) \Rightarrow Q(x) \equiv \forall x \neg Q(x) \rightarrow \neg P(x)$$

P	q	$\neg q$	$\neg p$	$\neg q \rightarrow \neg p$
T	T	F	F	T
T	F	T	F	F
F	T	F	T	T
F	F	T	T	T

assume $\neg Q$

$\neg P$

with a proof by contraposition, we want to eliminate the row in red. That is, we want to show that whenever $\neg q$ is true then $\neg p$ is true meaning $\neg q \rightarrow \neg p$ can never be false.

if $|x|+|y| \neq |x+y|$ then $xy < 0$

P $\quad$ q

prove by contraposition

$xy \geq 0 \rightarrow |x|+|y| = |x+y|$

assume this is true

$x, y \geq 0$ $\quad$ or $\quad$ $x, y \leq 0$

case 1 $\quad$ case 2

if $x \geq 0$ and $y \geq 0$

$|x| + |y| = x + y$

$|x+y| = x+y$ ✓

if $x \leq 0$ and $y \leq 0$

$|x| + |y| = ?$

$-x + -y$

$|x+y| = -(x+y) = -x + -y$ ✓

for both cases $|x|+|y| = |x+y|$

and $xy \geq 0$ if and only if

x and $y \geq 0$

or x and $y \leq 0$

therefore, we have shown that

the contrapositive holds. this means

the original statement holds

Pick up next class with Proof by contradiction and encryption motivation.