COSC 290 Discrete Structures

Lecture 8: Direct proof and proof by counter example

Prof. Michael Hay

Friday, Feb. 9, 2018

Colgate University

Plan for today

1. Logistics
2. Practice: nested and negated quantifiers
3. Proofs
4. Proof technique: direct proof
5. Proof technique: counter example

Logistics

Logistics

Next topic on schedule: proofs!

Reading does not align neatly with lecture plan.

We will spend some time (roughly 1 lecture each) on several proof techniques:

- direct proof
- proof by contrapositive
- proof by contradiction
- proof by cases

We will *return* to Ch. 4.2 to apply these techniques to Hamming codes.

Practice: nested and negated quantifiers

True love, expressed mathematically

Predicate $loves(p_1, p_2)$ means "p_1 loves p_2." We can express the loves predicate visually using a graph.

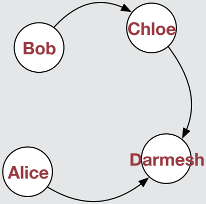
Nodes are individuals. Edge from p_1 to p_2 indicates $loves(u, v)$.

Example

The proposition

$$loves(Alice, Darmesh) \wedge loves(Bob, Chloe) \wedge loves(Chloe, Darmesh)$$

can be shown as.

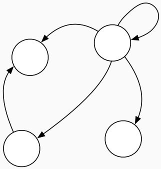


Poll: nested quantifiers, part 1

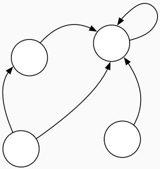
Predicate *loves*(p_1, p_2) means "p_1 loves p_2," shown by an arrow from p_1 to p_2.

For which figure(s) is the following proposition true:

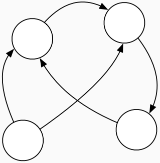
$$\forall p_1 \in P : \exists p_2 \in P : loves(p_1, p_2)$$



(a)



(b)



(c)

More than one/ None of the above

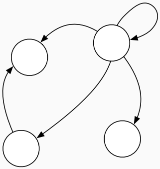
(d)

Poll: nested quantifiers, part 2

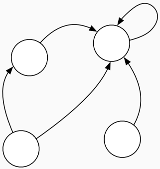
Predicate *loves*(p_1, p_2) means "p_1 loves p_2," shown by an arrow from p_1 to p_2.

For which figure(s) is the following proposition true:

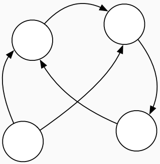
$$\exists p_2 \in P : \forall p_1 \in P : loves(p_1, p_2)$$



(a)



(b)



(c)

More than one/ None of the above

(d)

Poll: showing a proposition is false

Consider the following proposition

$$\forall p_1 \in P : \exists p_2 \in P : \mathit{loves}(p_1, p_2)$$

How could we show that this proposition is false?

A) Show there is a person who loves everyone
B) Show there is a person who loves no one
C) Show there is a person who nobody loves
D) Show there is a person who everyone loves
E) Other/more/none

Poll: negating nested quantifiers

Consider the following proposition

$$\varphi := \exists p_2 \in P : \forall p_1 \in P : \mathit{loves}(p_1, p_2)$$

What is the correct negation of φ? In other words, which of the following is logically equivalent to $\neg\varphi$?

A) $\forall p_2 \forall p_1 \neg \mathit{loves}(p_1, p_2)$

B) $\forall p_2 \exists p_1 \neg \mathit{loves}(p_1, p_2)$

C) $\exists p_2 \forall p_1 \neg \mathit{loves}(p_1, p_2)$

D) $\forall p_2 \exists p_1 \neg \mathit{loves}(p_2, p_1)$

E) Other/more/none

Proofs

Proof

A proof is a convincing argument that a proposition is true.

Proof

A proof is a convincing argument that a proposition is true.

A good proof has three characteristics:

- readable
- valid
- fluent use of appropriate concepts/terminology

Proof

A proof is a convincing argument that a proposition is true.

A good proof has three characteristics:

- readable
- valid
- fluent use of appropriate concepts/terminology

Over next few weeks, we will study many proof techniques (styles of argument): direct, contrapositive, contradiction, cases, induction, strong induction, structural induction, counter example, etc.

Proof technique: direct proof

Poll: two propositions

Consider the following two propositions.

$$\exists x \in S : (P(x) \wedge Q(x)) \implies (\exists x \in S : P(x)) \wedge (\exists x \in S : Q(x))$$

and

$$(\exists x \in S : P(x)) \wedge (\exists x \in S : Q(x)) \implies \exists x \in S : (P(x) \wedge Q(x))$$

Which of the above propositions is *always* true, regardless of the meaning of the predicates P and Q?

A) first one only
B) second one only
C) both first and second
D) neither: their truth values depends on P and Q which haven't been defined

Proving an "if ... then ..." proposition

If we have a proposition of the form $A \implies B$, we can employ a *direct proof* strategy where we assume the antecedent.

Terminology: with an "if A, then B" statement, the A part is the *antecedent* and the B part is the *consequent*.

Proof strategy of assuming the antecedent: assume that A is true, show that B must be true also.

Truth table for implication

Recall truth table for implication: $p \implies q$.

p	q	$p \implies q$	
T	T	T	
T	F	F	*Rule this row out!*
F	T	T	
F	F	T	

The implication has one F row: when p is T and q is F.

To prove that a specific proposition $A \implies B$ is true, we must show that, given the particular meanings of A and B, the F row *cannot* happen.

Direct Proof Template

- **Claim**: *Write the claim to be proved, "If p, then q"*
- **Proof**: We will prove this directly.
  - **Given**: Assume that p is true.
  - **Want to show**: *restate q*
  - *Write main body of proof... show how q logically follows from p*
  - *The body should lead reader to conclusion... "and therefore [restate q] is true."*
  - *End by restating claim or simply* $\square$

Example Proof

- **Claim**: The proposition $\exists x \in S : (P(x) \land Q(x)) \implies (\exists x \in S : P(x)) \land (\exists x \in S : Q(x))$ is true, regardless of the meaning of the predicates P and Q
- **Proof**: We will prove this directly.

Example Proof

- **Claim**: The proposition $\exists x \in S : (P(x) \wedge Q(x)) \implies (\exists x \in S : P(x)) \wedge (\exists x \in S : Q(x))$ is true, regardless of the meaning of the predicates P and Q
- **Proof**: We will prove this directly.
    - **Given**: Assume that $\exists x \in S : (P(x) \wedge Q(x))$ is true.

Example Proof

- **Claim**: The proposition $\exists x \in S : (P(x) \land Q(x)) \implies (\exists x \in S : P(x)) \land (\exists x \in S : Q(x))$ is true, regardless of the meaning of the predicates P and Q
- **Proof**: We will prove this directly.
    - **Given**: Assume that $\exists x \in S : (P(x) \land Q(x))$ is true.
    - **Want to show**: $(\exists x \in S : P(x)) \land (\exists x \in S : Q(x))$ must be true.

Example Proof

- **Claim**: The proposition $\exists x \in S : (P(x) \land Q(x)) \implies (\exists x \in S : P(x)) \land (\exists x \in S : Q(x))$ is true, regardless of the meaning of the predicates P and Q
- **Proof**: We will prove this directly.
  - **Given**: Assume that $\exists x \in S : (P(x) \land Q(x))$ is true.
  - **Want to show**: $(\exists x \in S : P(x)) \land (\exists x \in S : Q(x))$ must be true.

  Since we are given that $\exists x \in S : (P(x) \land Q(x))$, let x_0 be an element in S such that $P(x_0) \land Q(x_0)$.
  Given that $P(x_0) \land Q(x_0)$ is true, we know that $P(x_0)$ is true (because $p \land q$ is true only when both p and q are true).
  Since $P(x_0)$ is true and $x_0 \in S$, then $\exists x \in S : P(x)$.
  Using the same argument, we can show that $\exists x \in S : Q(x)$.
  Since both $(\exists x \in S : P(x))$ is true and $(\exists x \in S : Q(x))$ is true, we can conclude that $(\exists x \in S : P(x)) \land (\exists x \in S : Q(x))$ $\square$

Proof technique: counter example

Proving a claim is false

To show that proposition is false, present a counter example.

A counter example is a specific, concrete example that demonstrates that claim does not hold.

Proving a claim is false

To show that proposition is false, present a counter example.

A counter example is a specific, concrete example that demonstrates that claim does not hold.

Example

The claim $\forall x \in \mathbb{Z} : \mathit{isPrime}(x)$ is false. Proof by counter example: the number 6 is in $\mathbb{Z}$ and yet $\mathit{isPrime}(6)$ is false because 2 divides 6.

Example: Proof that claim is false

- **Claim**: The claim that $(\exists x \in S : P(x)) \land (\exists x \in S : Q(x)) \implies \exists x \in S : (P(x) \land Q(x))$ is true, regardless of the meaning of the predicates P and Q, is false.
- **Proof**: We will prove this using a counter example.

Example: Proof that claim is false

- **Claim**: The claim that $(\exists x \in S : P(x)) \wedge (\exists x \in S : Q(x)) \implies \exists x \in S : (P(x) \wedge Q(x))$ is true, regardless of the meaning of the predicates P and Q, is false.
- **Proof**: We will prove this using a counter example.
  Let S be the set of all Colgate students, let $P(x)$ be that student x is at least 6 feet tall; let $Q(x)$ be that student x is less than 6 feet tall.
  Looking around the room, we can see that $(\exists x \in S : P(x))$ and $(\exists x \in S : Q(x))$ are both true.
  Yet clearly $\exists x \in S : (P(x) \wedge Q(x))$ is false because someone can have only one height.

Poll: setting up a proof

Claim: The sum of any two odd numbers is even.

In the proof, what is "Given" and what do you "Want to Show" (WTS)?

A) Given: Assume the sum of two odd numbers is even. WTS: This follows from axioms of algebra.
B) Given: Assume x and y are odd numbers. WTS: x + y is even.
C) Given: Assume 3 and 5[1] are odd. WTS: sum of 3 and 5 is even.
D) You cannot use direct proof template, because claim is not of the form "if ... then ..."

[1] You can pick something else, but we chose 3 and 5

Formalizing claim

Background:

- $\mathbb{Z}$ is the set of all integers
- $Even(x) \coloneqq \exists k \in \mathbb{Z} : x = 2k$
- $Odd(x) \coloneqq \exists \ell \in \mathbb{Z} : x = 2\ell + 1$

Let's formalize the claim:

Claim: $Odd(x) \wedge Odd(y) \implies Even(x + y)$

Formalizing claim

Background:

- $\mathbb{Z}$ is the set of all integers
- $Even(x) := \exists k \in \mathbb{Z} : x = 2k$
- $Odd(x) := \exists \ell \in \mathbb{Z} : x = 2\ell + 1$

Let's formalize the claim:

Claim: $Odd(x) \wedge Odd(y) \implies Even(x + y)$

Let's be even more formal:

Claim: $\forall x \in \mathbb{Z} : \forall y \in \mathbb{Z} : (Odd(x) \wedge Odd(y) \implies Even(x + y))$