COT 3100C: INTRODUCTION TO DISCRETE STRUCTURES

SUMMER 2024

The Foundations: Logic and Proofs

Part-5

Mesut Ozdag, Ph.D.
mesut.ozdag@ucf.edu

*Because learning changes everything.**

Outline

- Propositional Logic
  - The Language of Propositions.
  - Applications.
  - Logical Equivalences.
- Predicate Logic
  - The Language of Quantifiers.
  - Logical Equivalences.
  - Nested Quantifiers.
- Proofs
  - Rules of Inference.
  - Proof Methods.
  - Proof Strategy.

*Mc Graw Hill

Section

Introduction to Proofs

Section Summary

Mathematical Proofs.

Forms of Theorems.

Direct Proofs.

Indirect Proofs.

- Proof of the Contrapositive.
- Proof by Contradiction.

Definitions

A ***proof*** is a valid argument that establishes the truth of a statement.

A ***theorem*** is a statement that can be shown to be true using:

- definitions.
- other theorems.
- *axioms* (statements which are given as true).
- rules of inference.

A ***lemma*** is a 'helping theorem' or a result which is needed to prove a theorem.

A ***corollary*** is a result which follows directly from a theorem.

A ***conjecture*** is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.

Proving Theorems

Many theorems have the form: $\forall x\big(P(x)\rightarrow Q(x)\big)$

To where c is an arbitrary element of the domain, $P(c)\rightarrow Q(c)$

By **universal generalization,** the truth of the original formula follows.

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

So, we must prove something of the form: $p \rightarrow q$

Proving Conditional Statements: $p \rightarrow q$

Trivial Proof: If we know q is true, then $p \rightarrow q$ is true as well.
"If it is raining then 1=1."

Vacuous Proof: If we know p is false then $p \rightarrow q$ is true as well.
"If I am both rich and poor then 2 + 2 = 5."

Example:
Let P(n) be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$," where the domain consists of all nonnegative integers. Show that P(0) is true.

Solution:
"If $a \geq b$, then $a^0 \geq b^0$." **Because $a^0 = b^0 = 1$**, the conclusion of the conditional statement "If $a \geq b$, then $a^0 \geq b^0$" is true. Hence, this conditional statement, which is P(0), is true. *(trivial proof)*

Even and Odd Integers

Definition: The integer n is even if there exists an integer k such that $n = 2k$, and

n is odd if there exists an integer k, such that $n = 2k + 1$.

Note that every integer is either even or odd and no integer is both even and odd.

Proving Conditional Statements: $p \rightarrow q$[1]

***Direct Proof*:** Assume that p is true. Use rules of inference, axioms, and logical equivalences to show that q must also be true.

Example: Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."

Solution: Assume that n is odd. Then $n = 2k + 1$ for an integer k. Squaring both sides of the equation, we get:

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2r + 1,$$

where $r = 2k^2 + 2k$, an integer.

We have proved that if n is an odd integer, then n^2 is an odd integer.

QED

Proving Conditional Statements: $p \rightarrow q_2$

Definition: The real number r is ***rational*** if there exist integers p and q where $q \neq 0$ such that $r = p/q$.

Example: Prove that the sum of two rational numbers is rational.

Solution*:* Assume r and s are two rational numbers. Then there must be integers p, q and also t, u such that

$$r = p/q, \quad s = t/u, \quad u \neq 0, \quad q \neq 0$$

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu} = \frac{v}{w}$$

where $v = pu + qt$

$w = qu \neq 0$

Therefore, the sum is rational.

QED

Proving Conditional Statements: $p \rightarrow q$ 3

Proof by Contraposition: Assume $\neg q$ and show $\neg p$ is true also. This is sometimes called an *indirect proof* method. If we give a direct proof of $\neg q \rightarrow \neg p$ then we have a proof of $p \rightarrow$ q.

Example: Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Solution: Assume n is even. So, $n = 2k$ for some integer k. Thus

$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j$ for $j = 3k + 1$.

Therefore $3n + 2$ is even. Since we have shown $\neg q \rightarrow \neg p$;

$p \rightarrow q$ must hold as well. If n is an integer and $3n + 2$ is odd (not even), then n is odd (not even).

Proving Conditional Statements: $p \rightarrow q$ 4

Example: Prove that for an integer n, if n^2 is odd, then n is odd.

Solution: Use proof by contraposition. Assume n is even (i.e., not odd). Therefore, there exists an integer k such that $n = 2k$. Hence,

$$n^2 = 4k^2 = 2\left(2k^2\right)$$

and n^2 is even(i.e., not odd).

We have shown that if n is an even integer, then n^2 is even. Therefore, by contraposition, for an integer n, if n^2 is odd, then n is odd.

Proving Conditional Statements: $p \rightarrow q$

Proof by Contradiction: (AKA *reductio ad absurdum*).

Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that ¬p → q is true. Because q is false, but ¬p → q is true, we can conclude that ¬p is false, which means that p is true.

Example: Prove that if you pick 22 days from the calendar, at least 4 must fall on the same day of the week.

Solution: p: "At least four of 22 chosen days fall on the same day of the week."

Suppose that ¬p is true: At most three of the 22 days fall on the same day of the week. Because there are seven days of the week, this implies that at most 21 days could have been chosen.

This contradicts the premise that we have 22 days under consideration.

Proof by Contradiction[1]

Example: Use a proof by contradiction to give a proof that $\sqrt{2}$ is irrational.

Solution: Suppose $\sqrt{2}$ is rational. Then there exists integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors. Then

$$2 = \frac{a^2}{b^2} \qquad 2b^2 = a^2$$

Therefore a^2 must be even. If a^2 is even then a must be even.
Since a is even, $a = 2c$ for some integer c. Thus,

$$2b^2 = 4c^2 \qquad b^2 = 2c^2$$

Therefore b^2 is even. Again, then b must be even as well.

But then 2 must divide both a and b. This contradicts our assumption that a and b have no common factors. We have proved by contradiction that our initial assumption must be false and therefore $\sqrt{2}$ is irrational.

Theorems that are Biconditional Statements

To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true. $(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$.

Example: Prove the theorem: "If n is an integer, then n is odd iff n^2 is odd."

Solution: We have already shown (previous slides) that both $p \rightarrow q$ and $q \rightarrow p$. Therefore, we can conclude $p \leftrightarrow q$.

What is wrong with this?

"Proof" that *1* = *2*

Step	**Reason**
1. $a=b$	Premise
2. $a^2=a\times b$	Multiply both sides of (1) by a
3. $a^2-b^2=a\times b-b^2$	Subtract b^2 from both sides of (2)
4. $(a-b)(a+b)=b(a-b)$	Algebra on (3)
5. $a+b=b$	Divide both sides by $a-b$
6. $2b=b$	Replace a by b in (5) because $a=b$
7. $2=1$	Divide both sides of (6) by b

Solution: Step 5. a − b = 0 by the premise and division by 0 is undefined.

Section:

Proof Methods and Strategy

Section Summary

Proof by Cases.

Exhaustive Proofs.

Existence Proofs.

- Constructive.
- Nonconstructive.

Disproof by Counterexample.

Uniqueness Proofs.

Proof Strategies.

Proving Universally Quantified Assertions.

Proof by Cases[1]

To prove a conditional statement of the form:

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$$

Use the tautology

$$\left[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q\right] \leftrightarrow \left[(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)\right]$$

Each of the implications $p_i \rightarrow q$ is a *case*.

Proof by Cases 2

Example: Let $a @ b = \max\{a, b\} = a$ if $a \geq b$, otherwise

$a @ b = \max\{a, b\} = b$.

Show that for all real numbers a, b, c;

$$(a @ b) @ c = a @ (b @ c)$$

(This means the operation @ is associative.)

Proof: Let a, b, and c be arbitrary real numbers.

Then one of the following 6 cases must hold.

1. $a \geq b \geq c$
2. $a \geq c \geq b$
3. $b \geq a \geq c$
4. $b \geq c \geq a$
5. $c \geq a \geq b$
6. $c \geq b \geq a$

Continued on next slide →

Proof by Cases 3

Case 1: $a \geq b \geq c$.

$(a \mathbin{@} b) = a$, $a \mathbin{@} c = a$, $b \mathbin{@} c = b$.

Hence $(a \mathbin{@} b) \mathbin{@} c = a \mathbin{@} c = a$.

$$a \mathbin{@} (b \mathbin{@} c) = a \mathbin{@} b = a.$$

Therefore, the equality holds for the first case.

A complete proof requires that the equality be shown to hold for all 6 cases. But the proofs of the remaining cases are similar. Try them.

Exhaustive Proofs

Some theorems can be proved by examining a relatively small number of examples. Such proofs are called *exhaustive proofs*, or ***proofs by exhaustion***.

Example: Prove that $(n + 1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Solution:

$(n + 1)^3 \geq 3n$ when n = 1, 2, 3, and 4.

$(n + 1)^3 = 2^3 =$ **8** and $3^n = 3^1 =$ **3**;

$(n + 1)^3 = 3^3 =$ **27** and $3^n = 3^2 =$ **9**;

$(n + 1)^3 = 4^3 =$ **64** and $3^n = 3^3 =$ **27**;

$(n + 1)^3 = 5^3 =$ **125** and $3^n = 3^4 =$ **81**.

QED

Without Loss of Generality

Example: Show that if x and y are integers and both $x \cdot y$ *and* $x+y$ are even, then both x and y are even.

Proof: Use a proof by contraposition. Suppose x and y are not both even. Then, one or both are odd. Without loss of generality, assume that x is odd. Then $x = 2m + 1$ for some integer m.

Case 1: x is odd, y is even. Then $y = 2n$ for some integer n, so

$$x + y = (2m + 1) + 2n = 2(m + n) + 1 \text{ is odd.}$$

Case 2: *x is odd,* y is odd. Then $y = 2n + 1$ for some integer n, so

$$x \cdot y = (2m + 1) \cdot (2n + 1) = 2(2m \cdot n + m + n) + 1 \text{ is odd.}$$

We only cover the case where "x is odd, y is even" because the case where "y is odd, x is even" is similar. The use phrase *without loss of generality* (WLOG) indicates this.

Existence Proofs

Proof of theorems of the form $\exists x P(x)$.

Constructive existence proof:

- Find an explicit value of *c*, for which *P(c)* is true.
- Then $\exists x P(x)$ is true by Existential Generalization (EG).

Example: Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways:

Proof: 1729 is such a number since

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

Nonconstructive Existence Proofs

In a *nonconstructive* existence proof, we assume no *c* exists which makes *P(c)* true and derive a contradiction.

Example: Show that there exist irrational numbers *x* and *y* such that x^y is rational.

Proof: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$

If it is rational, we have two irrational numbers x and y with x^y rational, namely $x = \sqrt{2}$ and $y = \sqrt{2}$.

But if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$

so that $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\left(\sqrt{2}\sqrt{2}\right)} = \sqrt{2}^{2} = 2.$

Counterexamples

Recall $\exists x \neg P(x) \equiv \neg \forall x P(x)$.

To establish that $\neg \forall x P(x)$ is true (or $\forall x P(x)$ is false) find a c such that $\neg P(c)$ is true or $P(c)$ is false.

In this case c is called a *counterexample* to the assertion $\forall x P(x)$.

Example: "Every positive integer is the sum of the squares of 3 integers." The integer 7 is a counterexample. So, the claim is false.

Uniqueness Proofs

The two parts of a *uniqueness proof:*

- *Existence*: We show that an element x with the property exists.
- *Uniqueness*: We show that if $y \neq x$, then y does not have the property.

Example: Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Solution:

- Existence: The real number $r = -b/a$ is a solution of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$.
- Uniqueness: Suppose that s is a real number such that $as + b = 0$. Then $\boldsymbol{ar + b = as + b}$, where $r = -b/a$. Subtracting $\boldsymbol{b}$ from both sides and dividing by $\boldsymbol{a}$ shows that $\boldsymbol{r = s}$.

Proof Strategies for proving $p \rightarrow q$

Choose a method.

1. First try a direct method of proof.
2. If this does not work, try an indirect method (e.g., try to prove the contrapositive).

For whichever method you are trying, choose a strategy.

1. First try *forward reasoning.* Start with the axioms and known theorems and construct a sequence of steps that end in the conclusion. Start with p and prove q, or start with $\neg q$ and prove $\neg p$.
2. If this doesn't work, try *backward reasoning*. When trying to prove q, find a statement p that we can prove with the property $p \rightarrow q$.

Backward Reasoning

Example: Given two positive real numbers x and y, their arithmetic mean is (x + y)/2 and their geometric mean is √xy. When we compare the arithmetic and geometric means of pairs of *distinct* positive real numbers, we find that the arithmetic mean is always greater than the geometric mean. [For example, when x = 4 and y = 6, we have 5 = (4 + 6)/2 > $\sqrt{4 \cdot 6} = \sqrt{24}$.] Can we prove that this inequality is always true?

Solution:

$$(x + y)/2 > \sqrt{xy},$$
$$(x + y)^2/4 > xy,$$
$$(x + y)^2 > 4xy,$$
$$x^2 + 2xy + y^2 > 4xy,$$
$$x^2 - 2xy + y^2 > 0,$$
$$(x - y)^2 > 0.$$

Because $(x - y)^2 > 0$ when x != y, it follows that the final inequality is true. Therefore,
it follows that (x + y)/2 > √xy when x != y.

Now, reverse the steps to construct a proof using forward reasoning:

Suppose that x and y are distinct positive real numbers. Then $(x - y)^2 > 0$.

$(x - y)^2 = x^2 - 2xy + y^2$,	this implies that:
$x^2 - 2xy + y^2 > 0$.	Adding 4xy to both sides:
$x^2 + 2xy + y^2 > 4xy$.	(NOTE: $x^2 + 2xy + y^2 = (x + y)^2$)
$(x + y)^2 \geq 4xy$.	Dividing both sides of this equation by 4:
$(x + y)^2/4 > xy$.	Finally, taking square roots of both sides:
(x + y)/2 > √xy.	

We conclude that if x and y are distinct positive real numbers, then their arithmetic mean (x + y)/2 is greater than their geometric mean √xy. QED

Backward Reasoning

Example: Suppose that two people play a game taking turns removing, 1, 2, or 3 stones at a time from a pile that begins with 15 stones. The person who removes the last stone wins the game. Show that the first player can win the game no matter what the second player does.

Proof: Let *n* be the last step of the game.

Step n: Player_1 can win if the pile contains $1,2$, or 3 stones.

Step n-1: Player_1 **will have to leave such a pile if the pile that he/she is faced with has 4 stones.**

Step n-2: Player_1 can leave 4 stones when there are $5,6$, or 7 stones left at the beginning of his/her turn.

Step n-3: Player_2 **must leave such a pile, if there are 8 stones .**

Step n-4: Player_1 has to have a pile with $9,10$, or 11 stones to ensure that there are 8 left.

Step n-5: Player_2 needs to be faced with 12 stones to be forced to leave $9,10$, or 11.

Step n-6: Player_1 **can leave 12 stones by removing 3 stones.**

Now reasoning forward, the first player can ensure a win by removing 3 stones and leaving 12.

Universally Quantified Assertions 1

To prove theorems of the form $\forall x P(x)$, assume x is an arbitrary member of the domain and show that $P(x)$ must be true. Using UG it follows that $\forall x P(x)$.

Example: An integer x is even if and only if x^2 is even.

Solution: The quantified assertion is

$$\forall x \left[x \text{ is even} \leftrightarrow x^2 \text{ is even} \right]$$

We assume x is arbitrary.

Recall that $P \leftrightarrow q$ is equivalent to $(P \rightarrow q) \wedge (q \rightarrow p)$

So, we have two cases to consider. These are considered in turn.

Continued on next slide →

Universally Quantified Assertions 2

Case 1. We show that if x is even then x^2 *is* even using a direct proof (the *only if* part or *necessity*).

If x is even then $x = 2k$ for some integer k.

Hence $x^2 = 4k^2 = 2\left(2k^2\right)$ which is even since it is an integer divisible by 2.

This completes the proof of case 1.

Case 2 on next slide →

Universally Quantified Assertions 3

Case 2. We show that x^2 is even then x must be even (the *if* part or *sufficiency*). We use a proof by contraposition.

Assume x is not even and then show that x^2 is not even.

If x is not even, then it must be odd. So, $x = 2k + 1$ for some k. Then $x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

which is odd and hence not even. This completes the proof of case 2.

Since x was arbitrary, the result follows by UG.

Therefore, we have shown that x is even if and only if x^2 is even.

MESUT OZDAG, PH.D.
MESUT.OZDAG@UCF.EDU

UCF