CSE 15
Discrete Mathematics

Lecture 6 – Proposition Logic (6)

Announcement

- HW #3 out on Thursday (9/13)
  - Due **5pm** 9/21 (Fri) with 1 extra day of re-submission.

- Reading assignment
  - Ch. 2.1 of textbook

Proof by Contradiction

- Definition: The statement $\neg r \wedge r$ is a **contradiction**.
- Always False.

- Suppose we want to prove a statement p.
- We can prove that p is true if we can show that

$$\boldsymbol{\neg p \rightarrow (\neg r \wedge r)}$$

That is, if p is not true, then there is a contradiction.

Proof by Contradiction

- **Example**: Prove that $\sqrt{2}$ is irrational.

Solution: Suppose $\sqrt{2}$ is rational ($\neg$ **p**). Then there exists integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors (**r**). 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 (an exercise). Since a is even, $a = 2c$ for some integer c. Thus,

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

...Proof by Contradiction

- **Solution (cont.):**

- 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. ($\neg$ **r**)
- 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.

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

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

Equivalent theorems

- $p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n$
- For i and j with $1 \le i \le n$ and $1 \le j \le n$, p_i and p_j are equivalent.
- Can prove this by exploiting the tautology:

  $[p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n] \leftrightarrow [(p_1 \rightarrow p_2) \land (p_2 \rightarrow p_3) \land \ldots \land (p_n \rightarrow p_1)]$
- Proving the right side of this is more efficient than proving $p_i \rightarrow p_j$ for $i \ne j$ with $1 \le i \le n$ and $1 \le j \le n$.
- The order is not important as long as we have a chain.

Example

- Show that these statements about integer n are equivalent
  - P_1: n is even
  - P_2: n-1 is odd
  - P_3: n^2 is even
- Show that $p_1 \longrightarrow p_2$ and $p_2 \longrightarrow p_3$ and $p_3 \longrightarrow p_{1.}$
- $p_1 \longrightarrow p_2$: (direct proof) Suppose n is even, then n=2k for some k. thus n-1=2k-1=2(k-1)+1 is odd

Example

- $p_2 \longrightarrow p_3$: (direct proof) Suppose n-1 is odd, then n-1=2k+1 for some k. Hence n=2k+2, and $n^2=(2k+2)^2=4k^2+8k+4=2(2k^2+4k+2)$ is even
- $p_3 \longrightarrow p_1$: (proof by contraposition) That is, we prove that if n is not even, then n^2 is not even. This is the same as proving if n is odd, then n^2 is odd (which we have done)

Counterexample

- To show that a statement $\forall x p(x)$ is false, all we need to do is to find a **counterexample**, i.e., an example x for which p(x) is false.

Example

- Show that "Every positive integer is the sum of the squares of two integers" is false.
- An counterexample is 3 as it cannot be written as the sum of the squares to two integers.
- Note that the only perfect squares not exceeding 3 are $0^2=0$ and $1^2=1$.
- Furthermore, there is no way to get 3 as the sum of two terms each of which is 0 or 1.

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: What went wrong here: Step 5?

What is wrong with this proof?

- "Theorem": If n^2 is positive, then n is positive

  "Proof": Suppose n^2 is positive. As the statement "If n is positive, then n^2 is positive" is true, we conclude that n is positive
- $p \to q$ does not imply $q \to p$.
- Counterexample: n=-1.

What is wrong with this proof?

- "Theorem": If n is not positive, then n^2 is not positive

  "Proof": Suppose that n is not positive. Because the conditional statement "If n is positive, then n^2 is positive" is true, we can conclude that n^2 is not positive.
- $p \rightarrow q$ does not imply $\neg p \rightarrow \neg q$.

- Counterexample: n=-1.

Circular reasoning

- Is the following argument correct?

  Suppose n^2 is even. Then $n^2=2k$ for some integer k. Let $n=2y$ for some integer y. This shows that n is even
- No argument shows n can be written as 2y.
- Circular reasoning as this statement is equivalent to the statement to be proved.

Proof Methods and Strategy (Ch. 1.8)

- Proof by Cases
- Existence Proofs
  - Constructive
  - Nonconstructive
- Disproof by Counterexample
- Nonexistence Proofs
- Uniqueness Proofs
- Proof Strategies
- Proving Universally Quantified Assertions
- Open Problems

Proof by Cases

- To prove a conditional statement of the form:

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

- Use the tautology

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

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

Example

- Prove $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$
- Proof by <u>exhaustion</u> as we only need to verify $n=1,2,3$ and 4.
- For $n=1$, $(n+1)^3 = 8 \geq 3^1 = 3$
- For $n=2$, $(n+1)^3 = 27 \geq 3^2 = 9$
- For $n=3$, $(n+1)^3 = 64 \geq 3^3 = 27$
- For $n=4$, $(n+1)^3 = 125 \geq 3^4 = 64$

Proof by Cases

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

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

(a @ b) = a, a @ c = a, b @ c = b

Hence (a @ b) @ c = a = a @ (b @ c)

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.

Common mistakes in Proofs

- What is wrong with this "proof"

  "Theorem": If x is a real number, then x^2 is a positive real number.

  "Proof": Let p_1 be "x is positive" and p_2 be "x is negative", and q be "x^2 is positive".

  First show $p_1 \rightarrow q$, and then $p_2 \rightarrow q$. As we cover all possible cases of x, we complete this proof

...Common mistakes

- We missed the case x=0.
- When x=0, the supposed theorem is false.

(0 is not a positive real number.)

- We need to prove results with p_1, p_2, p_3 (where p_3 is the case that x=0).

$$((p_1 \vee p_2 \vee p_3) \rightarrow q) \leftrightarrow ((p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge (p_3 \rightarrow q))$$

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: y is even. Then $y = 2n$ for some integer n, so $x + y = (2m + 1) + 2n = 2(m + n) + 1$ is odd.

Case 2: y is odd. Then $y = 2n + 1$ for some integer n, so $x \cdot y = (2m + 1)\,(2n + 1) = 2(2m \cdot n + m + n) + 1$ is odd. ◀

We only cover the case where x is odd because the case where y is odd 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

$$1729 = 10^3 + 9^3 = 12^3 + 1^3 \quad ◀$$

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 $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = \sqrt{2}^{2} = 2$.

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

- Some theorems assert the existence of a unique element with a particular property, $\exists! x\, P(x)$. The two parts of a *uniqueness proof* are:
  - *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.

Uniqueness Proofs

- **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 $ar + b = as + b$, where $r = -b/a$. Subtracting b from both sides and dividing by a shows that $r = s$. ◀

Proof Strategies for proving $p \to q$

- 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 $p \to q$.

Example

- For two distinct positive real numbers x, y, their arithmetic mean is (x+y)/2, and their geometric mean is $\sqrt{xy}$. Show that the arithmetic mean is always larger than geometric mean.
- To show $(x+y)/2 > \sqrt{xy}$, we can work backward by finding equivalent statements :

$$(x+y)/2 > \sqrt{xy}$$

$$(x+y)^2/4 > xy$$

$$x^2 + 2xy + y^2 > 4xy$$

$$(x-y)^2 > 0$$

Example

- For two distinct real positive real numbers, x and y, $(x-y)^2>0$.
- Thus, $x^2-2xy+y^2>0$, $x^2+2xy+y^2>4xy$, $(x+y)^2>4xy$.
- So, $(x+y)/2>\sqrt{xy}$.
- We conclude that if x and y are distinct positive real numbers, then their arithmetic mean is greater than their geometric mean.

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.