Discrete Structures

Introduction to Proofs

Vibhavari Kamble
Asst. Prof. CoEP Pune

Quick Quiz 5.2:

- **Correct or incorrect:**

"At least one of the 20 students in the class is intelligent. John is a student of this class. Therefore, John is intelligent."

To submit answer visit moodle

- **Step 1:**

  Separate premises from conclusion

Premises:

1. *At least one of the 20 students in the class is intelligent.*
2. *John is a student of this class.*

Conclusion:

John is intelligent.

- **Step 2:**

  Translate the example in logic notation.

- ***Premise 1:*** *At least one of the 20 students in the* class is intelligent. (Let the domain = all people)

  C(x) = "x is in the class"

  I(x) = "x is intelligent"

  Then *Premise 1 says:* $\exists x(C(x) \land I(x))$

- ***Premise 2:*** *John is a student of this class.*

  Then *Premise 2 says:* ***C(John)***

- ***Conclusion:*** ***John is intelligent.***

  And the *Conclusion says:* ***I(John)***

- **Step 2:**

  Translate the example in logic notation.

- ***Premise 1:*** *At least one of the 20 students in the* class is intelligent. (Let the domain = all people)

  C(x) = "x is in the class"

  I(x) = "x is intelligent"

  Then *Premise 1 says:* $\exists \boldsymbol{x(C(x) \land I(x))}$

- ***Premise 2:*** *John is a student of this class.*

  Then *Premise 2 says:* ***C(John)***

- ***Conclusion:*** ***John is intelligent.***

  And the *Conclusion says:* ***I(John)***

$$\begin{array}{l} \exists x\,(C(x) \land I(x)) \\ C(John) \\ \hline \therefore\ I(John) \end{array}$$

$$\begin{array}{l} \exists x\,(C(x) \land I(x)) \\ C(John) \\ \hline \therefore I(John) \end{array}$$

- No, the argument is invalid;

  we can disprove it with a counter-example, as follows:
- Consider a case where there is only one intelligent student A in the class, and A ≠ John.
  - Then by existential instantiation of the premise **$\exists x$ *(C(x) ⋀ I(x)) ⋀ C(A) -> I(A) is true,***
  - But the conclusion ***I(John) is false,*** *since A is* the only intelligent student in the class, and John ≠ A.
- Therefore, the premises *do not imply the* conclusion.

Proof Terminology

- A ***proof*** is a valid argument that establishes the truth of a mathematical statement
- ***Axiom** (or **postulate):*** a statement that is assumed to be true
- ***Theorem***

  A statement that has been proven to be true
- ***Hypothesis, premise***

  An assumption (often unproven) defining the structures about which we are reasoning

More Proof Terminology

- ***Lemma***

  A minor theorem used as a stepping-stone to proving a major theorem.

- ***Corollary***

  A minor theorem proved as an easy consequence of a major theorem.

- ***Conjecture***

  A statement whose truth value has not been proven. (A conjecture may be widely believed to be true, regardless.)

Methods of Proving Theorems

Example:

To prove a theorem of the form $\forall x(P(x) \rightarrow Q(x))$

Note:

"If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$"

really means

"For all positive real numbers x and y, if $x > y$, then $x^2 > y^2$."

Proof Methods

- For proving implications $p \rightarrow q$, *we have:*
- ***Trivial proof:*** *Prove q by itself.*
- ***Direct proof:*** *Assume p is true, and prove q.*
- ***Indirect proof:***

    Proof by Contraposition $(\neg q \rightarrow \neg p)$***:***

    Assume $\neg q$, *and prove* $\neg p$.

    Proof by Contradiction:

    Assume $p \land \neg q$, *and show this leads to a* contradiction. (i.e. prove $(p \land \neg q) \rightarrow \mathbf{F}$)
- ***Vacuous proof:*** *Prove* $\neg p$ *by itself.*

Direct Proof Example

- Starting with the hypothesis and leading to the conclusion.
- **E.g.**
- **Definition:** An integer *n is called odd iff n=2k+1* for some integer *k; n is even iff n=2k for some k.*

- **Theorem:** Every integer is either odd or even, but not both.

  This can be proven from even simpler axioms.

- **Theorem:**

(For all integers *n*) *If n is odd, then* n^2 *is odd.*

- **Proof: To prove P(n)->Q(n) assume P(n) is true.**

If *n is odd, then* $n = 2k + 1$ *for some integer k.*

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

Therefore n^2 *is of the form* $2j + 1$ *(with j the integer* $2k^2 + 2k$*), thus* n^2 *is odd.*

Quick Quiz 6.1

Let the statement be "If n is not an odd integer then square of n is not odd.", then if P(n) is "n is an not an odd integer" and Q(n) is "(square of n) is not odd." For direct proof we should prove ________

Visit moodle to submit answer

Indirect Proof : Proof by Contraposition

- That do not start with the premises and end with the conclusion, are called **indirect proofs.**

- An extremely useful type of indirect proof is known as **proof by contraposition.**

- The conditional statement $p \rightarrow q$ *can be proved by* showing that its contrapositive, $\sim q \rightarrow \sim p$, *is true.*

- ***Note:*** we take ¬q as a premise

Indirect Proof Example: Proof by Contraposition

- **Theorem: (For all integers *n*)**

  If $3n + 2$ *is odd, then n is odd.*

- **Proof:**

  (Contrapositive: If n is even, then $3n + 2$ is even)

  Suppose that the conclusion is false, *i.e.*, that n is even.

  Then $n = 2k$ for some integer k.

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

  Thus $3n + 2$ is even, because it equals $2j$ for an integer $j = 3k + 1$. So $3n + 2$ is not odd.

  We have shown that $\neg(n \text{ is odd}) \rightarrow \neg(3n + 2 \text{ is odd})$, thus its contrapositive $(3n + 2 \text{ is odd}) \rightarrow (n \text{ is odd})$ is also true. ■

Vacuous Proof Example

- Show $\neg p$ *(i.e. p is false) to prove $p \rightarrow q$ is true.*
- ***E.g.***
- **Theorem:** (For all n) If n is both odd and even, then $n^2 = n + n$.

- **Theorem:** (For all n) If n is both odd and even, then $n^2 = n + n$.
- **Proof:**

  The statement "n is both odd and even" is necessarily false, since no number can be both odd and even. So, the theorem is vacuously true. ■

Trivial Proof Example

- Show *q (i.e. q is true) to prove* $p \rightarrow q$ *is true.*

- **Theorem:** (For integers n) If n is the sum of two prime numbers, then either *n is odd or n* is even.

- **Proof:**

  Any integer n is either odd or even. So the conclusion of the implication is true regardless of the truth of the hypothesis. Thus the implication is true trivially.

Proof by Contradiction

A method for proving *p.*

- Assume $\neg p$, *and prove both q and* $\neg q$ *for* some proposition *q. (Can be anything!)*
- Thus $\neg p \rightarrow (q \land \neg q)$
- $(q \land \neg q)$ *is a trivial contradiction, equal to* ***F***
- Thus $\neg p \rightarrow$ ***F,*** *which is only true if* $\neg p$ **= *F***
- Thus *p is true*

Rational Number

- **Definition:**

  The real number *r is rational if there exist* integers *p and q with q ≠ 0 such that r = p/q. (p/q is in lowest terms i.e. no common factors)* A real number that is not rational is called *irrational.*

Proof by Contradiction: Example

Theorem: $\sqrt{2}$ is irrational.

Proof by Contradiction: Example

Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

Solution:

- *Let p :"$\sqrt{2}$ is irrational."*
- Suppose that $\sim p$= "$\sqrt{2}$ *is rational" is true.* (leads to a contradiction.)
- *So* $\sqrt{2} = a/b$*, where* $b \neq 0$ *and a and b have no common factors.*
- Both sides of this equation are squared $2b^2 = a^2$.
- It follows that *a is even. so assume* $a = 2c$
- $2b^2 = 4c^2$ this means that *b2 is even.*
- our assumption of $\sim p$ *leads to the* contradiction , So$\sim p$ *must be false.*
- *"$\sqrt{2}$ is irrational." is true.*

Quick Quiz 6.2

A proof that $p \rightarrow q$ is true based on the fact that q is true, such proofs are known as __________

Visit moodle to submit answer

Summary: Proof by Contradiction

- Proving implication $p \rightarrow q$ *by contradiction*
- Assume $\neg q$, *and use the premise* p *to* arrive at a contradiction, i.e. $(\neg q \land p) \rightarrow \mathbf{F}$

  $(p \rightarrow q \equiv (\neg q \land p) \rightarrow \mathbf{F})$
- How does this relate to the proof by contraposition?
- ***Proof by Contraposition*** $(\neg q \rightarrow \neg p)$***:***

  Assume $\neg q$, *and prove* $\neg p$.

Mathematical Induction

- A powerful, rigorous technique for proving that a statement $P(n)$ is true for ***every*** positive integers n, no matter how large.
- Essentially a "domino effect" principle.
- Based on a predicate-logic inference rule:

$$\begin{array}{l} P(1) \\ \forall k \geq 1\ [P(k) \rightarrow P(k+1)] \\ \hline \therefore \forall n \geq 1\ P(n) \end{array}$$

"The First Principle of Mathematical Induction"

Mathematical Induction

- **PRINCIPLE OF MATHEMATICAL INDUCTION:**

To prove that a statement $P(n)$ is true for all positive integers n, we complete two steps:

- **BASIS STEP**: Verify that $P(1)$ is true
- **INDUCTIVE STEP**: Show that the conditional statement $\underbrace{P(k)}_{\text{Inductive Hypothesis}} \rightarrow P(k+1)$ is true for all positive integers k

Induction Example

- Show that, for $n \geq 1$

$$\boxed{1 + 2 + \cdots + n = \frac{n(n+1)}{2}}$$

- Proof by induction
  - $P(n)$: the sum of the first n positive integers is $n(n+1)/2$, i.e. $P(n)$ is
  - ***Basis step***: Let $n = 1$. The sum of the first positive integer is 1, i.e. $P(1)$ is true.

$$1 = \frac{1(1+1)}{2}$$

- ***Inductive step***: Prove $\forall k \geq 1$: $P(k) \rightarrow P(k+1)$.
  - Inductive Hypothesis, $P(k)$:

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}$$

  - Let $k \geq 1$, assume $P(k)$, and prove $P(k+1)$, i.e.

$$1 + 2 + \cdots + k + (k+1) = \frac{(k+1)[(k+1)+1]}{2}$$

$$= \frac{(k+1)(k+2)}{2}$$

This is what you have to prove

$P(k+1)$

- ***Inductive step*** continues…

By inductive hypothesis P(k)

$$\underbrace{1+2+\cdots+k+(k+1)}_{P(k+1)} = \frac{k(k+1)}{2}+(k+1)$$

$$= \frac{k(k+1)}{2}+\frac{2(k+1)}{2}$$

$$= \frac{k^2+3k+2}{2}$$

$$= \frac{(k+1)(k+2)}{2}$$

- Therefore, by the principle of mathematical induction *P*(*n*) is true for all integers *n* with *n*≥1