Proof Techniques Introduction to Engineering Mathematics

Prof. Joris Vankerschaver

Overview

- Logical statements
 - Implication
 - Equivalence
 - Single statement
- Proof techniques
 - 1 Direct proof
 - Proof by contraposition
 - **3** Proof by contradiction
 - 4 Case enumeration
 - Induction

Proving an implication

- "If p is true, then q is also true."
- Notation: $p \Rightarrow q$

For example:

- If n is an odd number, then 2n is an even number.
- If it rains, then the ground gets wet.

Caveat

$$p \Rightarrow q$$
 does not mean that $q \Rightarrow p!$

For example:

- If the ground is wet, it doesn't necessarily mean that it's raining.
- For n = 10, 2n = 20 is even, but 10 is not odd.

Technique 1: direct proof

- Start from *p*, then work your way to *q*.
- This is how we've constructed most proofs so far.

Example:

- In words: For each positive real number x, there exists a real number y such that y(y + 1) = x.
- Mathematically: $\forall x > 0 \in \mathbb{R} \Rightarrow \exists y \in \mathbb{R} : y(y+1) = x.$

Technique 2: Proof by contraposition

- "If p then q" is logically equivalent to "if not q then not p".
- Start from "not q", work towards "not p".
- Mind the direction of the implication!

Example: Show that if n^2 is even (for n a natural number), then n is also even.

Caveat: negating a logical statement

De Morgan's laws:

- not (p and q) = (not p) or (not q)
- not (p or q) = (not p) and (not q)

Example: Show that if $x^2 \neq 1$, then $x \neq \pm 1$.

Technique 3: Proof by contradiction

- Assume that q is not true, start from p, and work towards a contradiction.
- If a contradiction is found, our starting assumption must have been false, and therefore q is true.

Example: Prove that if $x^2 = 2x$ and $x \neq 0$, then x = 2.

Proving an equivalence

- "p holds if and only if (iff) q holds."
- Notation: $p \Leftrightarrow q$

Proving an equivalence means proving two implications: $p \Rightarrow q$ and $q \Rightarrow p.$

Example: Prove that n^2 is even if and only if n is even.

Proving a single statement

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

Technique 4: Proof by case enumeration

- Split statement into subcases, prove each case separately.
- Don't forget any subcases!

Example: Show that for all $x, y \in \mathbb{R}$, |xy| = |x||y|.

Technique 5: Proof by induction

- Prove that a statement ${\cal P}(n)$ holds for every natural number $n. \label{eq:prove}$
- Proceeds in two steps:
 - Prove a *base case*, usually P(1).
 - Prove the induction step: if ${\cal P}(k)$ holds, then ${\cal P}(k+1)$ holds too.

Example: Show that the sum of the first n numbers is equal to $\frac{n(n+1)}{2}$:

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}.$$

Example

Show that the sum of the first n odd numbers is equal to n^2 :

$$1 + 3 + 5 + \dots + (2n - 1) = n^2.$$

Exam problem

10. For a homework assignment, a student has to come up with a proof by contraposition for the following theorem: For all integers n, if n^2 is even, then n is also even. As she is running out of time, she asks ChatGPT, an advanced AI model, to come up with a proof for her. Unfortunately, the proof provided by ChatGPT contains a number of errors.

Read the proposed proof below.

(a)	Indicate which proof steps are incorrect, and describe why.	[6 marks]
(b)	Provide a corrected proof by contraposition.	[6 marks]

Proposed proof by contraposition:

- Step 1. Assume that n^2 is odd. We will show that n is also odd.
- Step 2. Since n^2 is odd, we can say that $n^2 1$ is even.
- Step 3. Factoring, we get that (n+1)(n-1) is even.
- Step 4. Since the product of any two even numbers is also even, we can conclude that both n + 1 and n 1 are even.
- Step 5. Since n 1 is even, n is odd.

Proof technique X: proof by intimidation



Proof technique Y: proof by bluffing



Gokul Swamy @g_k_swamy

new proof technique just dropped: bluffing

tain a .801-approximation algorithm for MAX 3SAT. The best result that could be obtained previously, by combining the technique of [5, 6] and the bound of [3], was .7704. (This is not mentioned explicitly anywhere but why would we lie. See also the .769-approximation algorithm in the paper of Ono, Hirata, and Asano [8].) Finally, our reductions have implications for probabilistically checkable proof systems. Let $PCP_{c,s}[\log, q]$ be the class of languages that admit membership proofs that can be checked by a probabilistic verifier that

1:37 AM · Jan 11, 2023 · 4,533 Views