Introduction to Proofs

Jing Yang
September 24, 2010

Review

- What is covered in this course?
  - Basic tools and techniques
  - Precise and rigorous mathematical reasoning
- Why are proofs necessary?
- What is a (valid) proof in Mathematics?
- What details do you include or skip?

What is a proof?

- In Math, a proof is a step-by-step demonstration that a conclusion follows from some hypotheses.
- In a each step use hypotheses, axioms, previously proven theorems, rules of inference, and logical equivalences such that the intermediate conclusion follows from previous step

Terminology

- Theorem: A statement that can be proved to be true
- Axiom: A statement which is given to be true
- Lemma: A ‘pre-theorem’ that is needed to prove a theorem
- Corollary: A ‘post-theorem’ that follows from a theorem

Rules of Inference

- In order to infer new facts using facts we already have
- Rules of Inference are important in proofs, although they are sometimes used without being mentioned

Rules of Inference

- Recall the **tautologies** in previous sections of the chapter, which have the form:

$$H_1 \wedge H_2 \wedge \ldots \wedge H_n \rightarrow C$$

H_i :Hypotheses

Conclusion

- As a rule of inference they take the symbolic form:

$$\begin{array}{l} H_1 \\ H_2 \\ \ldots \\ H_n \\ \hline \therefore C \end{array}$$

∴ means 'therefore' or 'it follows that'

Modus Ponens (Law of Detachment)

- From $p \rightarrow q$ and p is TRUE, we can infer that q is TRUE.

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

$$((p \rightarrow q) \land p) \rightarrow q$$

Tautology

Universal Instantiation

- From $\forall x P(x)$ is true we can infer that $P(c)$ is true, where c is a particular member of the domain

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Universal Generalization

- From P(c) is true for an **arbitrary** c in the domain, we can infer that $\forall x P(x)$ is true.

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

More Rules of Inference

- Read rules on page 66 and 70.
- Understanding is required, memorization is not.

Types of Proofs

- Direct proof (including proof by cases)
- Proof by contraposition
- Proof by contradiction
- Proof by construction
- Proof by induction
- Other techniques

} Indirect proof

Direct Proof

- Leads from hypothesis to the conclusion
- How to prove p→q?
  - Assume p is true

These steps are constructed using:
- Rules of inference
- Axioms
- Lemmas
- Definitions
- Proven theorems
- ...

  - q must be true
  - Q.E.D. (used to signal the end of a proof)

Direct Proof (example)

If n is an odd integer, then n^2 is odd.

Proof:

- Assume n is an odd integer
- By definition, $n=2k+1$ for some integer k
- $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$
- Let $m = 2k^2+2k$, $n^2 = 2m+1$
- By definition, n^2 is odd
- Q.E.D.

Definition:
n is an odd integer if $n=2k+1$ for some integer k

Proof by Contraposition

$$p \rightarrow q \equiv \neg q \rightarrow \neg p$$

- Leads from the negation of conclusion to the negation of hypothesis
- How to prove $p \rightarrow q$?
  - Assume $\neg q$ is true
  - $\neg p$ must be true
  - Q.E.D.

These steps are constructed using:

- Rules of inference
- Axioms
- Lemmas
- Definitions
- Proven theorems
- ...

Proof by Contraposition (example)

If n^2 is an even integer, then n is even.

Proof (by contraposition):

- Assume n is an odd integer. Then $n=2k+1$ (k is integer)
- $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$
- Let integer $m = (2k^2+2k)$, then $n^2=2m+1$.
- So n^2 is odd.
- Q.E.D.

Proof by Contradiction

$$p \rightarrow q \equiv p \wedge \neg q \rightarrow FALSE$$

- Leads from the hypothesis and the negation of conclusion to a contradiction
- How to prove $p \rightarrow q$?
  - Assume p and $\neg q$ is true
  - Contradiction!
  - Q.E.D.

These steps are constructed using:

- Rules of inference
- Axioms
- Lemmas
- Definitions
- Proven theorems
- …

Proof by Contradiction (example)

$\sqrt{2}$ is irrational.

Proof (by contradiction):

- Assume $\sqrt{2}$ is rational. Then $\sqrt{2}=a/b$ such that a and b have no common factors (definition)
- Squaring and transposing: $2=a^2/b^2$, $a^2=2b^2$.
- a^2 is even, so a is even (previous slide). i.e. $\exists k\ a=2k$
- $a^2 = 4k^2 = 2b^2$, so $b^2 = 2k^2$
- b^2 is even, so b is even (previous slide). i.e. $\exists m\ b=2m$
- a and b have common factor 2 -- Contradiction!

Reading and Notes

- Skim Sec 1.5, read Sec 1.6
- Master the basic proof methods: direct proof, proof by contraposition, proof by contradiction
- Recommended exercises: 1.5: 3,15,19,23; 1.6: 1,11,17