Module #10:
Proof Strategies

Rosen 5th ed., §3.1

~28 slides, ~1 lecture

Overview of Section 3.1

- Methods of mathematical argument (proof methods) can be formalized in terms of *rules of logical inference*.
- Mathematical *proofs* can themselves be represented formally as discrete structures.
- We will review both correct & fallacious inference rules, & several proof methods.

Applications of Proofs

- An exercise in clear communication of logical arguments in any area.
- The fundamental activity of mathematics is the discovery and elucidation of proofs of interesting new theorems.
- Theorem-proving has applications in program verification, computer security, automated reasoning systems, *etc*.

Proof Terminology

- *Theorem* - A statement that has been proven to be true.
- *Axioms*, *postulates*, *hypotheses*, *premises* - Assumptions (often unproven) defining the structures about which we are reasoning.
- *Rules of inference* - Patterns of logically valid deductions from hypotheses to conclusions.

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.)

Inference Rules - General Form

- *Inference Rule* - Pattern establishing that if we know that a set of *antecedent* statements of certain forms are all true, then a certain related *consequent* statement is true.
- *antecedent 1*
  antecedent 2 …

  ———————————

  ∴ *consequent* "∴" means "therefore"

Inference Rules & Implications

- Each logical inference rule corresponds to an implication that is a tautology.
- *antecedent 1* Inference rule
  antecedent 2 …

  ———————————

  ∴ *consequent*
- Corresponding tautology: ((*antecedent 1*) ∧ (*antecedent 2*) ∧ …) → *consequent*

Some Inference Rules

- $\dfrac{p}{\therefore p \vee q}$ Rule of Addition
- $\dfrac{p \wedge q}{\therefore p}$ Rule of Simplification
- $\dfrac{p \quad q}{\therefore p \wedge q}$ Rule of Conjunction

Modus Ponens & Tollens

- $\dfrac{p \quad p \rightarrow q}{\therefore q}$ Rule of *modus ponens*
- $\dfrac{\neg q \quad p \rightarrow q}{\therefore \neg p}$ Rule of *modus tollens*

Syllogism Inference Rules

- $\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$ Rule of hypothetical syllogism
- $\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$ Rule of disjunctive syllogism

Formal Proofs

- A formal proof of a conclusion C, given premises p_1, p_2,…,p_n consists of a sequence of *steps*, each of which applies some inference to premises or previously-proven statements (as antecedents) to yield a new true statement (the consequent).
- A proof demonstrates that if the premises are true, then the conclusion is true.

Formal Proof Example

- Premises:
  "It is not sunny and it is cold."
  "We will swim only if it is sunny."
  "If we do not swim, then we will canoe."
  "If we canoe, then we will be home early."
- Given these premises, prove "We will be home early" using inference rules.

Proof Example *cont.*

- Let *sunny*="It is sunny"; *cold*="It is cold;" *swim*="We will swim;" *canoe*="We will canoe;" *early*="We will be home early."
- Premises:

  (1) $\neg sunny \wedge cold$ (2) $swim \rightarrow sunny$

  (3) $\neg swim \rightarrow canoe$ (4) $canoe \rightarrow early$

Proof Example *cont.*

Step	Proved by
1. $\neg sunny \wedge cold$	Premise #1.
2. $\neg sunny$	Simplification of 1.
3. $swim \rightarrow sunny$	Premise #2.
4. $\neg swim$	Modus tollens on 2,3.
5. $\neg swim \rightarrow canoe$	Premise #3.
6. $canoe$	Modus ponens on 4,5.
7. $canoe \rightarrow early$	Premise #4.
8. $early$	Modus ponens on 6,7.

Common Fallacies

- A *fallacy* is an inference rule or other proof method that is not logically valid.
- Fallacy of *affirming the conclusion*: "$p \rightarrow q$ is true, and q is true, so p must be true." (Consider F$\rightarrow$T.)
- Fallacy of *denying the hypothesis*: "$p \rightarrow q$ is true, and p is false, so q must be false." (Consider F$\rightarrow$T.)

Circular Reasoning

- The fallacy of (explicitly or implicitly) assuming the very statement you are trying to prove in the course of its proof.
- Prove that an integer n is even if n^2 is even.
- Attempted proof: "Assume n^2 is even. Then $n^2=2k$ for some integer k. Dividing both sides by n gives $n=(2k)/n=2(k/n)$. So there is an integer j (namely k/n) such that $n=2j$. Therefore n is even."

Begs the question: How do you show that $j=k/n=n/2$ is an integer, without assuming n is even?

Removing the Circularity

Suppose n^2 is even $\therefore 2|n^2 \therefore n^2 \bmod 2 = 0$. Of course $n \bmod 2$ is either 0 or 1. If it's 1, then $n \equiv 1 \pmod 2$, so $n^2 \equiv 1 \pmod 2$, using the theorem that if $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then $ac \equiv bd \pmod m$, with $a=c=n$ and $b=d=1$. Now $n^2 \equiv 1 \pmod 2$ implies that $n^2 \bmod 2 = 1$. So by the hypothetical syllogism rule, $(n \bmod 2 = 1)$ implies $(n^2 \bmod 2 = 1)$. Since we know $n^2 \bmod 2 = 0 \neq 1$, by *modus tollens* we know that $n \bmod 2 \neq 1$. So by disjunctive syllogism we have that $n \bmod 2 = 0 \therefore 2|n \therefore n$ is even.

Inference Rules for Quantifiers

- $\dfrac{\forall x\, P(x)}{\therefore P(o)}$ **Universal instantiation** (substitute *any* object o)
- $\dfrac{P(g)}{\therefore \forall x\, P(x)}$ (for g a *general* element of u.d.) **Universal generalization**
- $\dfrac{\exists x\, P(x)}{\therefore P(c)}$ **Existential instantiation** (substitute a *new constant* c)
- $\dfrac{P(o)}{\therefore \exists x\, P(x)}$ (substitute any extant object o) **Existential generalization**

Proof Methods

For proving implications $p \rightarrow q$, we have:

- *Direct* proof: Assume p is true, and prove q.
- *Indirect* proof: Assume $\neg q$, and prove $\neg p$.
- *Vacuous* proof: Prove $\neg p$ by itself.
- *Trivial* proof: Prove q by itself.
- Proof by cases: Show $p \rightarrow (a \vee b)$ and $(a \rightarrow q)$ and $(b \rightarrow q)$.

Proof by Contradiction

- A method for proving p.
- Assume $\neg p$, and prove both q and $\neg q$ for some proposition q.
- Thus $\neg p \rightarrow (q \wedge \neg q)$
- $(q \wedge \neg q)$ is a trivial contradition, equal to **F**
- Thus $\neg p \rightarrow \mathbf{F}$, which is only true if $\neg p = \mathbf{F}$
- Thus p is true.

Review: Proof Methods So Far

- *Direct*, *indirect*, *vacuous*, and *trivial* proofs of statements of the form $p \rightarrow q$.
- *Proof by contradiction* of any statements.
- *Constructive* and *nonconstructive existence proofs*.

Proving Existentials

- A proof of a statement of the form $\exists x\, P(x)$ is called an *existence proof*.
- If the proof demonstrates how to actually find or construct a specific element a such that $P(a)$ is true, then it is a *constructive* proof.
- Otherwise, it is *nonconstructive*.

A Constructive Existence Proof

(Example 23, p.179)

- Show that for any $n>0$ there exists a sequence of n consecutive composite integers.
- Same statement in predicate logic:
  $\forall n>0\ \exists x\ \forall i\ (1\leq i\leq n)\rightarrow(x+i \text{ is composite})$

The proof...

- Given $n>0$, let $x = (n + 1)! + 1$.
- Let $i \geq 1$ and $i \leq n$, and consider $x+i$.
- Note $x+i = (n + 1)! + (i + 1)$.
- Note $(i+1)|(n+1)!$, since $2 \leq i+1 \leq n+1$.
- Also $(i+1)|(i+1)$. So, $(i+1)|(x+i)$.
- $\therefore$ $x+i$ is composite.
- $\therefore$ $\forall n\, \exists x\, \forall 1 \leq i \leq n : x+i$ is composite. Q.E.D.

Nonconstructive Existence Proof

(Example 24, p. 180)

- Show that there are infinitely many primes.
- Show there is no largest prime.
- Show that for any prime number, there is a larger number that is also prime.
- Show that for any number, $\exists$ a larger prime.
- Show that $\forall n \, \exists p > n : p$ is prime.

Da proof...

- Given $n>0$, prove there is a prime $p>n$.
- Consider $x=n!+1$. Since $x>1$, we have (x is prime)$\vee$(x is composite).
- Case 1: x is prime. Obviously $x>n$, so let $p=x$ and we're done.
- Case 2: x has a prime factor p. But if $p\leq n$, then $p \bmod x = 1$. So $p>n$, and we're done.

The Halting Problem (Turing‘36)

- Involves a *non*-existence proof.
- The first mathematical function proven to have *no* algorithm that computes it!
- The desired function is *Halts*(*P*,*I*) = the truth value of the statement ‘Program *P*, given input *I*, eventually halts’.
- Implies general impossibility of predictive analysis of arbitrary computer programs.

The Proof

- Given any *arbitrary* program $H(P,I)$,
- Consider algorithm *Breaker*, defined as:
  procedure *Breaker*(*P*: a program)
  halts **:=** $H(P,P)$
  if *halts* **then while T begin end**
- Note that *Breaker*(*Breaker*) halts iff $H(Breaker,Breaker) =$ **F**.
- So *H* does **not** compute the function *Halts*!

Limits on Proofs

- Some very simple statements of number theory haven't been proved or disproved!
  - *E.g. Goldbach's conjecture*: Every integer $n>2$ is exactly the average of some two primes.
  - $\forall n>2 \; \exists$ primes $p,q : n=(p+q)/2$.
- There are true statements of number theory (or any sufficiently powerful system) that can *never* be proved (or disproved) (Gödel).