Module #2: Basic Proof Methods

Rosen 5th ed., §1.5 & 3.1
29 slides, ~2 lectures
Module #2 - Proofs

Nature & Importance of Proofs

• In mathematics, a proof is:
  – a correct (well-reasoned, logically valid) and complete (clear, detailed) argument that rigorously & undeniably establishes the truth of a mathematical statement.
• Why must the argument be correct & complete?
  – Correctness prevents us from fooling ourselves.
  – Completeness allows anyone to verify the result.
• In this course (& throughout mathematics), a very high standard for correctness and completeness of proofs is demanded!!

Overview of §§ 1.5 & 3.1

• Methods of mathematical argument (i.e., 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.
Module #2 - Proofs

Applications of Proofs

• An exercise in clear communication of logical arguments in any area of study.
• The fundamental activity of mathematics is the discovery and elucidation, through proofs, of interesting new theorems.
• Theorem-proving has applications in program verification, computer security, automated reasoning systems, etc.
• Proving a theorem allows us to rely upon its correctness even in the most critical scenarios.

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.
Module #2 - Proofs

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.)
- **Theory** – The set of all theorems that can be proven from a given set of axioms.

Module #2 - Proofs

Graphical Visualization

A Particular Theory

The Axioms of the Theory

Various Theorems

A proof
Module #2 - Proofs

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”

Module #2 - Proofs

Inference Rules & Implications

• Each logical inference rule corresponds to an implication that is a tautology.

 uganda. 1
  - **antecedent 2** …
  - **∴ consequent**

• Corresponding tautology:
  
  \((\text{ante. } 1) \land (\text{ante. } 2) \land \ldots ) \rightarrow \text{consequent}\)
Module #2 - Proofs

Some Inference Rules

- Rule of Addition
  \[ \frac{p}{\therefore p \lor q} \]
- Rule of Simplification
  \[ \frac{p \land q}{\therefore p} \]
- Rule of Conjunction
  \[ \frac{p}{q} \quad \frac{q}{\therefore p \land q} \]

Module #2 - Proofs

Modus Ponens & Tollens

- Rule of *modus ponens* (a.k.a. *law of detachment*)
  \[ \frac{p}{p \rightarrow q} \quad \frac{p \rightarrow q}{\therefore q} \]

- Rule of *modus tollens*
  \[ \frac{\neg q}{p \rightarrow q} \quad \frac{p \rightarrow q}{\therefore \neg p} \]

“the mode of affirming”

“the mode of denying”
Module #2 - Proofs

Syllogism Inference Rules

- \[ \frac{p \rightarrow q}{q \rightarrow r} \] \[ \therefore p \rightarrow r \] Rule of hypothetical syllogism

- \[ \frac{p \lor q}{\neg p} \] \[ \therefore q \] Rule of disjunctive syllogism

Aristotle (ca. 384–322 B.C.)

Module #2 - Proofs

Formal Proofs

- A formal proof of a conclusion \( C \), given premises \( p_1, p_2, \ldots, p_n \) consists of a sequence of steps, each of which applies some inference rule to premises or to 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.
Module #2 - Proofs

Formal Proof Example

- Suppose we have the following 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 the theorem “We will be home early” using inference rules.

Proof Example cont.

- Let us adopt the following abbreviations:
  - sunny = “It is sunny”;
  - cold = “It is cold”;
  - swim = “We will swim”;
  - canoe = “We will canoe”; early = “We will be home early”.
- Then, the premises can be written as:
  1. ¬sunny ∧ cold
  2. swim → sunny
  3. ¬swim → canoe
  4. canoe → early
Module #2 - Proofs

Proof Example \textit{cont.}

<table>
<thead>
<tr>
<th>Step</th>
<th>Proved by</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ( \neg\text{sunny} \land \neg\text{cold} )</td>
<td>Premise #1.</td>
</tr>
<tr>
<td>2. ( \neg\text{sunny} )</td>
<td>Simplification of 1.</td>
</tr>
<tr>
<td>3. ( \text{swim}\rightarrow\text{sunny} )</td>
<td>Premise #2.</td>
</tr>
<tr>
<td>4. ( \neg\text{swim} )</td>
<td>Modus tollens on 2,3.</td>
</tr>
<tr>
<td>5. ( \neg\text{swim}\rightarrow\text{canoe} )</td>
<td>Premise #3.</td>
</tr>
<tr>
<td>6. \text{canoe}</td>
<td>Modus ponens on 4,5.</td>
</tr>
<tr>
<td>7. ( \text{canoe}\rightarrow\text{early} )</td>
<td>Premise #4.</td>
</tr>
<tr>
<td>8. ( \text{early} )</td>
<td>Modus ponens on 6,7.</td>
</tr>
</tbody>
</table>

Inference Rules for Quantifiers

- \( \forall x P(x) \)
  - Universal instantiation (substitute any object \( o \))
  \[ \therefore P(o) \]

- \( P(g) \)
  - Universal generalization (for \( g \) a general element of u.d.)
  \[ \therefore \forall x P(x) \]

- \( \exists x P(x) \)
  - Existential instantiation (substitute a new constant \( c \))
  \[ \therefore P(c) \]

- \( P(o) \)
  - Existential generalization (substitute any extant object \( o \))
  \[ \therefore \exists x P(x) \]
Common Fallacies

- A *fallacy* is an inference rule or other proof method that is not logically valid.
  - May yield a false conclusion!
- Fallacy of *affirming the conclusion*:
  - “$p \rightarrow q$ is true, and $q$ is true, so $p$ must be true.”
    (No, because $F \rightarrow T$ is true.)
- Fallacy of *denying the hypothesis*:
  - “$p \rightarrow q$ is true, and $p$ is false, so $q$ must be false.”
    (No, again because $F \rightarrow T$ is true.)

Circular Reasoning

- The fallacy of (explicitly or implicitly) assuming the very statement you are trying to prove in the course of its proof. Example:
- 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 first assuming $n$ is even?*
Removing the Circularity

Suppose \( n^2 \) is even .\( \therefore 2|n^2 \). Of course \( n \mod 2 \) 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 \( n^2 \mod 2 = 1 \). So by the hypothetical syllogism rule, \( (n \mod 2 = 1) \) implies \( (n^2 \mod 2 = 1) \). Since we know \( n^2 \mod 2 = 0 \neq 1 \), by modus tollens we know that \( n \mod 2 \neq 1 \). So by disjunctive syllogism we have that \( n \mod 2 = 0 \). \( \therefore 2|n \). \( \therefore n \) is even.

Proof Methods for Implications

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 \( p \rightarrow (a \lor b) \), and \( (a \rightarrow q) \) and \( (b \rightarrow q) \).
Module #2 - Proofs

Direct Proof Example

- **Definition:** An integer \( n \) is called *odd* iff \( n = 2k + 1 \) for some integer \( k \); \( n \) is *even* iff \( n = 2k \) for some \( k \).
- **Axiom:** Every integer is either odd or even.
- **Theorem:** (For all numbers \( n \)) If \( n \) is an odd integer, then \( n^2 \) is an odd integer.
- **Proof:** 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. □

Module #2 - Proofs

Indirect Proof Example

- **Theorem:** (For all integers \( n \))
  
  If \( 3n+2 \) is odd, then \( n \) is odd.

- **Proof:** 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 integer \( j = 3k+1 \). So \( 3n+2 \) is not odd. We have shown that \( \neg(n \text{ is odd}) \implies \neg(3n+2 \text{ is odd}) \), thus its contrapositive \( (3n+2 \text{ is odd}) \implies (n \text{ is odd}) \) is also true.
Module #2 - Proofs

Vacuous Proof Example

• **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. □

Module #2 - Proofs

Trivial Proof Example

• **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 antecedent. Thus the implication is true trivially. □
Proof by Contradiction

- Assume $\neg p$, and prove both $q$ and $\neg q$ for some proposition $q$.
- 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.

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.
- Next: Constructive and nonconstructive existence proofs.
Module #2 - 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*.

Constructive Existence Proof

- **Theorem:** There exists a positive integer $n$ that is the sum of two perfect cubes in two different ways:
  - equal to $j^3 + k^3$ and $l^3 + m^3$ where $j, k, l, m$ are positive integers, and $\{j,k\} \not\subseteq \{l,m\}$
- **Proof:** Consider $n = 1729$, $j = 9$, $k = 10$, $l = 1$, $m = 12$. Now just check that the equalities hold.
Another Constructive Existence Proof

• **Theorem:** For any integer \( n > 0 \), there exists a sequence of \( n \) consecutive composite integers.

• Same statement in predicate logic:
  \[ \forall n > 0 \exists x \forall i (1 \leq i \leq n) \rightarrow (x + i \text{ is composite}) \]

• Proof follows on next slide…

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, \( (i+1)|(x+i) \).
• \[\therefore x + i \text{ is composite.} \]
• \[\therefore \forall n \exists x \forall 1 \leq i \leq n : x + i \text{ is composite. Q.E.D.} \]
Nonconstructive Existence Proof

- **Theorem:**
  “There are infinitely many prime numbers.”
- Any finite set of numbers must contain a maximal element, so we can prove the theorem if we can just show that there is *no* largest prime number.
- *I.e.*, show that for any prime number, there is a larger number that is *also* prime.
- More generally: For *any* number, *∃* a larger prime.
- Formally: Show \( \forall n \exists p > n : p \) is prime.

The proof, using *proof by cases*...

- Given \( n > 0 \), prove there is a prime \( p > n \).
- Consider \( x = n! + 1 \). Since \( x > 1 \), we know \((x \text{ is prime}) \lor (x \text{ is composite})\).
- **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 \( p \mod x = 1 \). So \( p > n \), and we’re done.
The Halting Problem (Turing‘36)

- The halting problem was the first mathematical function proven to have no algorithm that computes it!
  - We say, it is uncomputable.
- The desired function is $\text{Halts}(P,I)$:
  - the truth value of this statement:
    - “Program $P$, given input $I$, eventually terminates.”
- **Theorem:** $\text{Halts}$ is uncomputable!
  - I.e., There does not exist any algorithm $A$ that computes $\text{Halts}$ correctly for all possible inputs.
- Its proof is thus a non-existence proof.
- **Corollary:** General impossibility of predictive analysis of arbitrary computer programs.

The Proof

- Given any arbitrary program $H(P,I)$,
- Consider algorithm $\text{Breaker}$, defined as:
  
  \[
  \text{procedure } \text{Breaker}(P: \text{ a program})
  \]
  
  \[
  \text{halts} := H(P,P)
  \]
  
  \[
  \text{if} \ \text{halts} \ \text{then while } T \ \text{begin} \ \text{end}
  \]
  
  - Note that $\text{Breaker}(\text{Breaker})$ halts iff $H(\text{Breaker},\text{Breaker}) = \text{F}$.
  
  - So $H$ does not compute the function $\text{Halts}$!
Module #2 - Proofs

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.
  - \( \forall n=2 \exists \text{ primes } p,q: n=(p+q)/2. \)
- There are true statements of number theory (or any sufficiently powerful system) that can never be proved (or disproved) (Gödel).

Module #2 - Proofs

More Proof Examples

- Quiz question 1a: Is this argument correct or incorrect?
  - “All TAs compose easy quizzes. Ramesh is a TA. Therefore, Ramesh composes easy quizzes.”
- First, separate the premises from conclusions:
  - Premise #1: All TAs compose easy quizzes.
  - Premise #2: Ramesh is a TA.
  - Conclusion: Ramesh composes easy quizzes.
Module #2 - Proofs

Answer

Next, re-render the example in logic notation.

• Premise #1: All TAs compose easy quizzes.
  – Let U.D. = all people
  – Let $T(x) \equiv \text{“} x \text{ is a TA} \text{”}
  – Let $E(x) \equiv \text{“} x \text{ composes easy quizzes} \text{”}$
  – Then Premise #1 says: $\forall x, T(x) \implies E(x)$

Module #2 - Proofs

Answer cont…

• Premise #2: Ramesh is a TA.
  – Let $R \equiv \text{Ramesh}$
  – Then Premise #2 says: $T(R)$
  – And the Conclusion says: $E(R)$

• The argument is correct, because it can be reduced to a sequence of applications of valid inference rules, as follows:
The Proof in Gory Detail

- Statement
  1. \( \forall x, T(x) \implies E(x) \) (Premise #1)
  2. \( T(\text{Ramesh}) \implies E(\text{Ramesh}) \) (Universal instantiation)
  3. \( T(\text{Ramesh}) \) (Premise #2)
  4. \( E(\text{Ramesh}) \) (Modus Ponens from statements #2 and #3)

Another example

- Quiz question 2b: Correct or incorrect: At least one of the 280 students in the class is intelligent. Y is a student of this class. Therefore, Y is intelligent.
- First: Separate premises/conclusion, & translate to logic:
  - Premises: (1) \( \exists x \text{ InClass}(x) \land \text{Intelligent}(x) \) (2) \( \text{InClass}(Y) \)
  - Conclusion: \( \text{Intelligent}(Y) \)
Module #2 - Proofs

Answer

• 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 X in the class, and X $\neq$ Y.
  – Then the premise $\exists x \text{ InClass}(x) \land \text{Intelligent}(x)$ is true, by existential generalization of
    $\text{InClass}(X) \land \text{Intelligent}(X)$
  – But the conclusion $\text{Intelligent}(Y)$ is false, since X is the only intelligent student in the class, and Y $\neq$ X.
• Therefore, the premises do not imply the conclusion.

Module #2 - Proofs

Another Example

• Quiz question #2: Prove that the sum of a rational number and an irrational number is always irrational.
• First, you have to understand exactly what the question is asking you to prove:
  – “For all real numbers $x, y$, if $x$ is rational and $y$ is irrational, then $x+y$ is irrational.”
  – $\forall x, y: \text{Rational}(x) \land \text{Irrational}(y) \not\implies \text{Irrational}(x+y)$
Module #2 - Proofs

Answer

• Next, think back to the definitions of the terms used in the statement of the theorem:
  
  \[ \forall r : \text{Rational}(r) \]
  \[ \exists i, j : \text{Integer}(i) \land \text{Integer}(j) : r = i/j. \]
  \[ \forall r : \text{Irrational}(r) \] \[ \neg \text{Rational}(r) \]

• You almost always need the definitions of the terms in order to prove the theorem!

• Next, let’s go through one valid proof:

Module #2 - Proofs

What you might write

• **Theorem:**
  \[ \forall x, y : \text{Rational}(x) \land \text{Irrational}(y) \rightarrow \neg \text{Irrational}(x+y) \]

• **Proof:** Let \( x, y \) be any rational and irrational numbers, respectively. ... (universal generalization)

• Now, just from this, what do we know about \( x \) and \( y \)? You should think back to the definition of rational:

• ... Since \( x \) is rational, we know (from the very definition of rational) that there must be some integers \( i \) and \( j \) such that \( x = i/j \). So, let \( i_x, j_x \) be such integers ...

• We give them unique names so we can refer to them later.
What next?

- What do we know about $y$? Only that $y$ is irrational: $\neg \exists \text{integers } i,j: y = i/j$.
- But, it’s difficult to see how to use a direct proof in this case. We could try indirect proof also, but in this case, it is a little simpler to just use proof by contradiction (very similar to indirect).
- So, what are we trying to show? Just that $x+y$ is irrational. That is, $\neg \exists i,j: (x + y) = i/j$.
- What happens if we hypothesize the negation of this statement?

More writing...

- Suppose that $x+y$ were not irrational. Then $x+y$ would be rational, so $\exists \text{integers } i,j: x+y = i/j$. So, let $i_s$ and $j_s$ be any such integers where $x+y = i_s/j_s$.
- Now, with all these things named, we can start seeing what happens when we put them together.
- So, we have that $(i_x/j_x) + y = (i_s/j_s)$.
- Observe! We have enough information now that we can conclude something useful about $y$, by solving this equation for it.
Module #2 - Proofs

Finishing the proof.

• Solving that equation for $y$, we have:
  $y = (i_s/j_s) - (i_x/j_x)$
  $= (i_s j_x - i_x j_s) / (j_s j_x)$

Now, since the numerator and denominator of this expression are both integers, $y$ is (by definition) rational. This contradicts the assumption that $y$ was irrational.

Therefore, our hypothesis that $x+y$ is rational must be false, and so the theorem is proved.

Module #2 - Proofs

Example wrong answer

• $1$ is rational. $\sqrt{2}$ is irrational. $1 + \sqrt{2}$ is irrational. Therefore, the sum of a rational number and an irrational number is irrational. (Direct proof.)

• Why does this answer merit no credit?
  – The student attempted to use an example to prove a universal statement. **This is always wrong!**
  – Even as an example, it’s incomplete, because the student never even proved that $1 + \sqrt{2}$ is irrational!