Module #2 – Part 2:
Proofs: Terminology and Methods

Rosen 6th ed., § 1.6 - 1.7

~ 33 slides, ~2 lectures

Proof Terminology

- *Theorem*

  is a statement that has been proven to be true.

- A theorem is shown to be true with a *proof*.

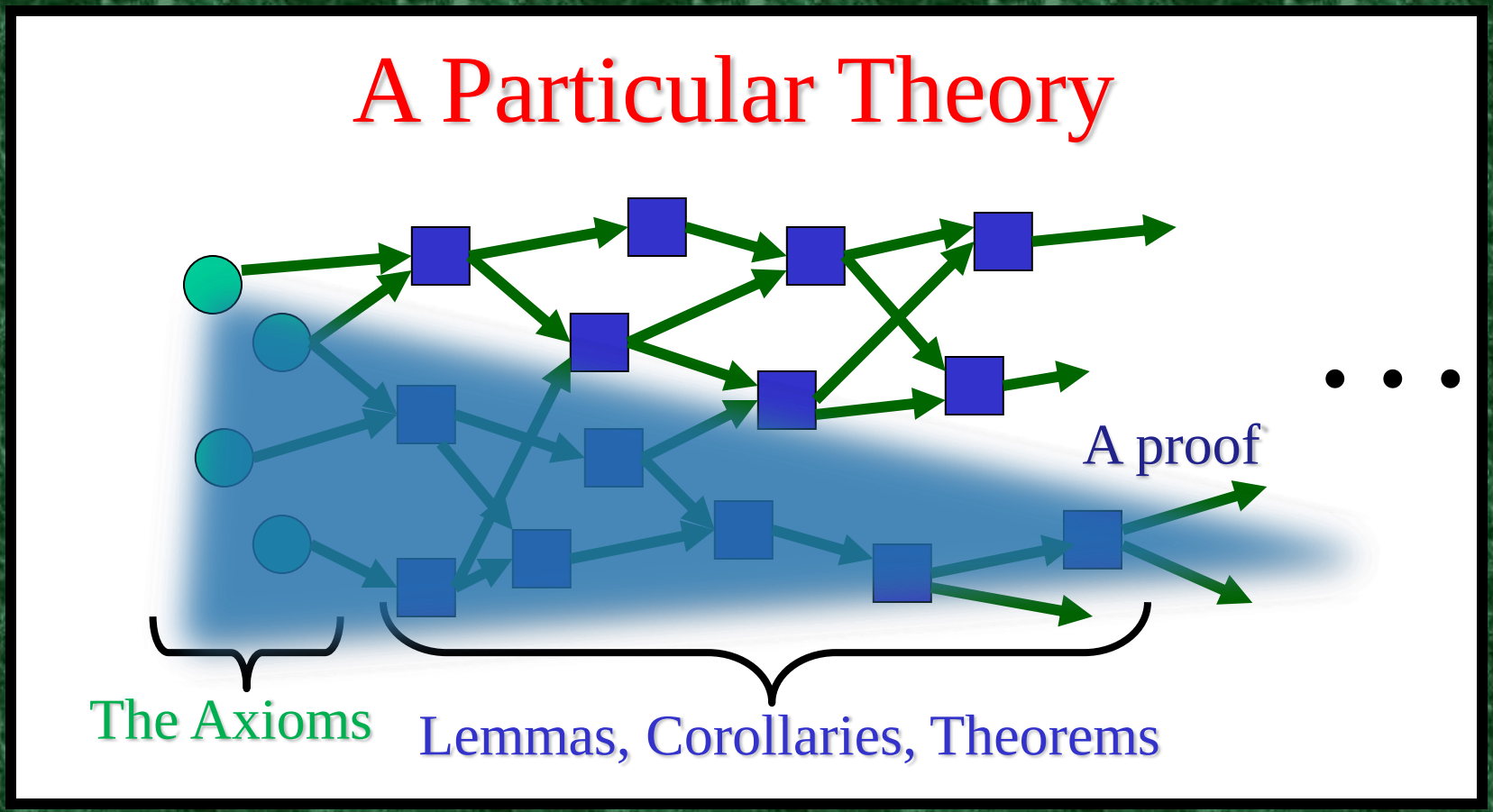
- *Axioms*, *postulates*, *premises*

  are assumptions (often unproven) that are taken as true. They help us to define the structures about which we are reasoning.

More Proof Terminology

- *Lemma* - A less important theorem that is helpful in the proof of a major theorem.
- *Corollary* - A minor theorem that can be easily established from a previously proven theorem.
- *Conjecture* - A statement whose truth value has not been proven. (A conjecture may be widely believed to be true, by the way.)
- *Theory* - The set of all theorems that can be proven from a given set of axioms.

Graphical Visualization



Proof Methods

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

- *Direct* proof: Assume p is true, and prove q.
- *Indirect* proof: Proofs other than *direct* proof.
- *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 $(b \rightarrow q)$.

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. □

Indirect Proof Example
Proof by Contraposition

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 $j = 3k+1$. □

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.

Another Type of Indirect Proof: Proof by Contradiction

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

Proof by Contradiction Example

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

Definition: A number n is *rational* when there exist integers a and b with $n=a/b$ where a and b have no common factors.

Axiom: A number is either rational or irrational.

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

Proof Strategy: Assume $\neg p$ is true and find a contradiction. This means $\neg p$ is false and p is true.

Proof by Contradiction Example

Proof: Assume $\neg p$ is true. I.e. $\sqrt{2}$ is rational.

If $\sqrt{2}$ is rational, there exists integers a and b with $\sqrt{2} = a/b$ where a and b have no common factors.

$2 = a^2/b^2$, $2b^2=a^2$, implies a^2 is even and a is even.

Define c such that $a=2c$ because a is even.

$2b^2=4c^2$, $b^2=2c^2$ implies b^2 is even and b is even.

Therefore, a and b have a common factor (2).
Contradicts with the rational number definition.
So, $\neg p$ is false, p is true. □

Proof by Contradiction (cont'd)

- Proof by contradiction can also be used to prove conditional statements like $r \rightarrow s$.
- If $p \Leftrightarrow r \rightarrow s$, then $\neg p \Leftrightarrow \neg(r \rightarrow s)$.
- Go with $\neg(r \rightarrow s)$ or $(r \wedge \neg s)$, find a contradiction.

Example

Construct a proof by contradiction that for all real numbers x, if , $x^2-2x \neq -1$, then $x \neq 1$.

- r is $x^2-2x \neq -1$ and s is $x \neq 1$.
- We assume $\neg p \Leftrightarrow r \wedge \neg s$ and find a contradiction.
- $r \wedge \neg s \Leftrightarrow (x^2-2x \neq -1) \wedge x = 1$
- If $x = 1$ then $x^2-2x = -1$. Therefore both sides of $\wedge$ can not be true at the same time. This is a contradiction.

Vacuous Proof Example

- **Theorem:** P(0) is true where
  P(n): If $n>1$ then $n^2>n$ for all integers..
- **Proof:** The statement "$n>1$" is false for number 0. So, the theorem is vacuously true.

  I.e. p is F, so $p \rightarrow q$ is T.

  Another example: *If I am both rich and poor then there exists a elephant that can fly.*

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 premise. Thus the implication is true trivially.

Proof by Cases

- Given n is an integer, prove $n^2 \geq n$.
- We consider 3 cases: when $n = 0$, when $n \geq 1$ and when $n \leq -1$.
- **Case 1:** $n = 0$. Because $0^2 = 0$, $0^2 \geq 0$.
- **Case 2:** $n \geq 1$. We multiply both sides of the inequality by n. $n \cdot n \geq n \cdot 1$, then $n^2 \geq n$.
- **Case 3:** $n \leq -1$. $n^2 \geq 0$. It follows $n^2 \geq n$.

The Proofs of Equivalences

- To prove a biconditional statement $p \leftrightarrow r$, you need to prove $p \rightarrow r$ and $r \rightarrow p$ separately.
- E.g. "n is odd if and only if n^2 is odd." can be proven by proving
  1. "If n is odd then n^2 is odd".
  2. "If n^2 is odd then n is odd".

Mistakes in Proofs

What is wrong with the following proof?

1. $a = b$
2. $a^2 = ab$
3. $a^2 - b^2 = ab - b^2$
4. $(a - b)(a + b) = b(a - b)$
5. $a + b = b$
6. $2b = b$
7. $2 = 1$

Circular Reasoning

- This fallacy occurs when one or more steps of a proof are based on the truth of the statement that is being proved. 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 such that $n=2j$. So, n is even."

Fallacy (circular reasoning): How do you show that $j=k/n$ is an integer, without first proving n is even?

Review: Proof Methods So Far

- *Direct*, *indirect*, *vacuous*, and *trivial* proofs of statements of the form $p \rightarrow q$.
- *Proof by contraposition.*
- *Proof by contradiction.*
- *Proof by cases.*
- Next: *Constructive* and *non-constructive existence proofs*.

Existence Proofs

- A proof of a statement of the form $\exists x\, P(x)$ is called an *existence proof*.
- If the proof demonstrates for a specific element a such that $P(a)$ is true, then it is a *constructive* proof.
- Otherwise, it is *non-constructive*.

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 $\{j,k\} \neq \{l,m\}$
- **Proof:** Consider $n = 1729$, $j = 9$, $k = 10$, $l = 1$, $m = 12$. Check if the equalities hold.

Another Constructive Existence Proof

- **Theorem:** For any integer $n>0$, there exists a sequence of n consecutive composite integers.

  Note: 'Composite' is the opposite of 'prime' number.

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

Another Constructive Existence Proof

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.

Nonconstructive Existence Proof

- **Theorem:** There exist irrational numbers x and y such that x^y is rational.
- **Axiom:** $\sqrt{2}$ is irrational
- **Proof:** Consider $\sqrt{2}^{\sqrt{2}}$. If it is rational, we have two irrational numbers x and y with x^y is rational.

If $\sqrt{2}^{\sqrt{2}}$ is irrational, then let $x=\sqrt{2}^{\sqrt{2}}$ and $y=\sqrt{2}$, so that $x^y = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = (\sqrt{2})^2 = 2$, which is rational.

- We did not find a specific (x,y) pair. But we showed either $(\sqrt{2},\sqrt{2})$ or $(\sqrt{2}^{\sqrt{2}}, \sqrt{2})$ has the desired property.

Limits on Proofs

- Some very simple statements of number theory haven't been proved or disproved!
  - *E.g. Goldbach's conjecture*: Every integer $n \geq 2$ is exactly the average of some two primes.
  - $\forall n \geq 2 \; \exists$ 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).

Proof example

- Question: Valid or invalid?

  At least one of the 65 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) $\exists x$ InClass(x) $\wedge$ Intelligent(x)
    (2) InClass(Y)
  - Conclusion: Intelligent(Y)

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≠Y.
  - Then the premise $\exists x$ **InClass(*x*)** $\wedge$ **Intelligent(*x*)** is true, by existential generalization of **InClass(X)** $\wedge$ **Intelligent(X)**
  - But the conclusion **Intelligent(Y)** is false, since X is the only intelligent student in the class, and Y≠X.

Another Example

- Question: 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."
  - $\forall x,y$: Rational(x) $\wedge$ Irrational(y) $\rightarrow$ Irrational($x+y$)

Answer

- Next, consider the definitions/axioms that can be used in the statement of the theorem:
  - $\forall r$: Rational(r) $\leftrightarrow \exists$ integers $i,j : r = i/j$.
  - $\forall r$: Irrational(r) $\leftrightarrow \neg$Rational(r)
- Theorem:
  $\forall x,y$: Rational(x) $\wedge$ Irrational(y) $\rightarrow$ Irrational($x+y$)
- Try direct proof:
  If x is rational, there must be some integers i and j such that $x = i/j$. So, let i_x,j_x be such integers.
  If y is irrational, then $\neg\exists$ integers i,j: $y = i/j$.
  It's difficult to see how to use a direct proof.

What next?

- We can try indirect proof!
- Let's try proof by contraposition.

Original theorem was:

Rational(x) $\wedge$ Irrational(y) $\rightarrow$ Irrational(x+y)

Theorem becomes:

Rational(x+y) $\rightarrow$ $\neg$Rational(x) $\vee$ $\neg$ Irrational(y)

Rational(x+y) $\rightarrow$ Irrational(x) $\vee$ Rational(y)

(Opposite of being irrational is being rational).

- We start with $(x + y)$ is rational: $\exists i,j$: $(x + y) = i/j$.

What next?

Rational(x+y) → Irrational(x) ∨ Rational(y)

If x is irrational, then this part is T ∨ .. ≡ T

If x is rational, we need to check if Rational(y) becomes true.

- If x+y is rational, so ∃ i,j: x+y = i/j. Let i_s and j_s be any such integers where x+y = i_s/ j_s.
- We give them unique names i_x , i_s etc. So, we can refer to them later.

More writing…

- When x is rational, $x + y = (i_x/j_x) + y = (i_s/j_s)$.
- Now, we have an equation that we can solve for y.
- Solving that equation for y, we have:

$$y = (i_s/j_s) - (i_x/j_x)$$
$$= (i_s j_x - i_x j_s)/(j_s j_x)$$

Since the numerator and denominator of this expression are both integers, y is rational.

- Therefore, we proved the contraposition.
- Why? $\underbrace{\text{Irrational}(x) \vee \text{Rational}(y)}$

became $\quad F \vee T \equiv T$

Selecting a method

Which method would you use to prove:

- "If n is an integer and n^3+5 is odd, then n is even."
- "There is no largest prime number."
- "Prove that $n^2+1 \geq 2^n$ when $1 \leq n \leq 4$."
- "Prove that there are 100 consecutive positive integers that are not perfect squares."