Today's topics

- Proof techniques
  - Indirect, by cases, and direct
  - Rules of logical inference
  - Correct & fallacious proofs
- Reading: Section 1.5
- Upcoming
  - Sets and Functions

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

Inference Rules - General Form

- An *Inference Rule* is
  - A pattern establishing that if we know that a set of *antecedent* statements of certain forms are all true, then we can validly deduce that a certain related *consequent* statement is true.
- $\boxed{\begin{array}{l} \textit{antecedent 1} \\ \underline{\textit{antecedent 2 …}} \\ \therefore \textit{ consequent} \end{array}}$

"∴" means "therefore"

Inference Rules & Implications

- Each valid logical inference rule corresponds to an implication that is a tautology.
- $\begin{array}{l} \textit{antecedent 1} \\ \textit{antecedent 2 ...} \\ \hline \therefore \textit{consequent} \end{array}$ Inference rule
- Corresponding tautology:

  $((\textit{ante. 1}) \wedge (\textit{ante. 2}) \wedge \ldots) \rightarrow \textit{consequent}$

Some Inference Rules

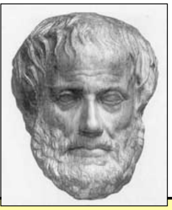
- $\begin{array}{c} p \\ \hline \therefore p \vee q \end{array}$ Rule of Addition
- $\begin{array}{c} p \wedge q \\ \hline \therefore p \end{array}$ Rule of Simplification
- $\begin{array}{c} p \\ q \\ \hline \therefore p \wedge q \end{array}$ Rule of Conjunction

Modus Ponens & Tollens

- $\begin{array}{c} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$ Rule of *modus ponens* (a.k.a. *law of detachment*) "the mode of affirming"
- $\begin{array}{c} \neg q \\ p \rightarrow q \\ \hline \therefore \neg p \end{array}$ Rule of *modus tollens* "the mode of denying"

Syllogism Inference Rules

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



Aristotle (ca. 384-322 B.C.)

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 previously-proven statements (*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

- 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.

Inference Rules for Quantifiers

- $\dfrac{\forall x\, P(x)}{\therefore P(o)}$ Universal instantiation (substitute *any* specific 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

Common Fallacies

- A *fallacy* is an inference rule or other proof method that is not logically valid.
  - A fallacy 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."
  - Circular reasoning is used in this proof. Where?

A Correct Proof

We know that n must be either odd or even. If n were odd, then n^2 would be odd, since an odd number times an odd number is always an odd number. Since n^2 is even, it is not odd, since no even number is also an odd number. Thus, by modus tollens, n is not odd either. Thus, by disjunctive syllogism, n must be even. ■

A More Verbose Version

Uses some number theory we haven't defined yet.

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 $ac \equiv bd$ (mod 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.

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 $p \rightarrow (a \vee b)$, 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.
- **Theorem:** Every integer is either odd or even.
  - This can be proven from even simpler axioms.
- **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

- **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 $\neg(n \text{ is odd}) \rightarrow \neg(3n+2 \text{ is odd})$, thus its contra-positive $(3n+2 \text{ is odd}) \rightarrow (n \text{ is odd})$ is also true. □

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. □

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

- A method for proving p.
- Assume $\neg p$, and prove both q and $\neg q$ for some proposition q. (Can be anything!)
- Thus $\neg p \rightarrow (q \land \neg q)$
- $(q \land \neg q)$ is a trivial 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

$\sqrt{2}$

- **Theorem:** $\sqrt{2}$ is irrational.
  - **Proof:** Assume $2^{1/2}$ were rational. This means there are integers i,j with no common divisors such that $2^{1/2} = i/j$. Squaring both sides, $2 = i^2/j^2$, so $2j^2 = i^2$. So i^2 is even; thus i is even. Let $i=2k$. So $2j^2 = (2k)^2 = 4k^2$. Dividing both sides by 2, $j^2 = 2k^2$. Thus j^2 is even, so j is even. But then i and j have a common divisor, namely 2, so we have a contradiction. □

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*.

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 $\{j,k\} \neq \{l,m\}$
- **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 ?

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.

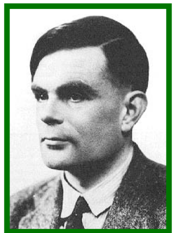
Nonconstructive Existence Proof

- **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, $\exists$ 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 is prime)∨(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 mod x = 1. So $p>n$, and we're done.

The Halting Problem (Turing'36)



Alan Turing
1912-1954

- 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 $Halts(P,I)$:≡ the truth value of this statement:
  - *"Program P, given input I, eventually terminates."*
- **Theorem:** *Halts* is uncomputable!
  - I.e., There does *not* exist *any* algorithm *A* that computes *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 halting problem: writing `doesHalt`

```
public class ProgramUtils
    /**
     * Returns true if progname halts on input,
     * otherwise returns false (progname loops)
     */
    public static boolean doesHalt(String progname,
                                   String input){
    }
}
```

- A compiler is a program that reads other programs as input
  - Can a word counting program count its own words?
- The `doesHalt` method might simulate, analyze, ...
  - One program/function that works for *any* program/input

Consider the class *`Confuse.java`*

```
public static void main(String[] args){
     String prog = "Foo.java";
     if (ProgramUtils.doesHalt(prog,prog)) {
          while (true) {
               // do nothing forever
          }
     }
}
```

- We want to show writing `doesHalt` is impossible
  - Proof by contradiction:
  - Assume possible, show impossible situation results

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).

More Proof Examples

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

Another example

- Quiz question 2b: Correct or incorrect: At least one of the 9 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)

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