CHAPTER 3

Methods of Proofs

1. Logical Arguments and Formal Proofs

1.1. Basic Terminology.

- An **axiom** is a statement that is given to be true.
- A **rule of inference** is a logical rule that is used to deduce one statement from others.
- A **theorem** is a proposition that can be proved using definitions, axioms, other theorems, and rules of inference.

Discussion

In most of the mathematics classes that are prerequisites to this course, such as calculus, the main emphasis is on using facts and theorems to solve problems. Theorems were often stated, and you were probably shown a few proofs. But it is very possible you have never been asked to prove a theorem on your own. In this module we introduce the basic structures involved in a mathematical proof. One of our main objectives from here on out is to have you develop skills in recognizing a valid argument and in constructing valid mathematical proofs.

When you are first shown a proof that seemed rather complex you may think to yourself "How on earth did someone figure out how to go about it that way?" As we will see in this chapter and the next, a proof must follow certain *rules of inference*, and there are certain strategies and methods of proof that are best to use for proving certain types of assertions. It is impossible, however, to give an exhaustive list of strategies that will cover all possible situations, and this is what makes mathematics so interesting. Indeed, there are conjectures that mathematicians have spent much of their professional lives trying to prove (or disprove) with little or no success.

1.2. More Terminology.

- A **lemma** is a "pre-theorem" or a result which is needed to prove a theorem.
- A **corollary** is a "post-theorem" or a result which follows from a theorem (or lemma or another corollary).

Discussion

The terms "lemma" and "corollary" are just names given to theorems that play particular roles in a theory. Most people tend to think of a theorem as the main result, a lemma a smaller result needed to get to the main result, and a corollary as a theorem which follows relatively easily from the main theorem, perhaps as a special case. For example, suppose we have proved the Theorem: "If the product of two integers m and n is even, then either m is even or n is even." Then we have the Corollary: "If n is an integer and n^2 is even, then n is even." Notice that the Corollary follows from the Theorem by applying the Theorem to the special case in which $m = n$. There are no firm rules for the use of this terminology; in practice, what one person may call a lemma another may call a theorem.

Any mathematical theory *must* begin with a collection of undefined terms and axioms that give the properties the undefined terms are assumed to satisfy. This may seem rather arbitrary and capricious, but any mathematical theory you will likely encounter in a serious setting is based on concrete ideas that have been developed and refined to fit into this setting. To justify this necessity, see what happens if you try to define every term. You define a in terms of b, and then you define b in terms of c, etc. If a, b, c, ... are all different terms, you are lead to an infinite chain of definitions; otherwise, one of them is repeated and you are left with a circular chain of definitions. Neither of these alternatives is logically acceptable. A similar criticism can be made for any attempt to prove every assertion. Here are a few important examples of mathematical systems and their basic ingredients.

In plane geometry one takes "point" and "line" as undefined terms and assumes the five axioms of Euclidean geometry.

In set theory, the concept of a "set" and the relation "is an element of," or "$\in$", are left undefined. There are five basic axioms of set theory, the so-called Zermelo-Fraenkel axioms, which we will use informally in this course, rather than giving them a rigorous exposition. In particular, these axioms justify the "set builder" notation we discussed in *Module 1.1: Sets* and the existence of the "power set" of a set, which we shall discuss later in *Module 4.1: Set Operations*.

The real number system begins with the four Peano Postulates for the positive integers, taking the elements, "numbers," in the set of positive integers as undefined, as well as the relation "is a successor of" between positive integers. (To say "x is a successor of y" turns out to mean that $x = y + 1$.) The fourth Peano Postulate is the Principle of Mathematical Induction, which we shall use extensively in the next module. From these modest beginnings, and with a little help from set theory, one can construct the entire set of real numbers, including its order and completeness properties. As with our treatment of set theory, we shall, with the one exception mentioned above, use these axioms informally, assuming the familiar model of the real

number line together with its important subsets, the natural numbers, the integers, and the rational numbers.

Once we have the undefined terms and axioms for a mathematical system, we can begin defining new terms and proving theorems (or lemmas, or corollaries) within the system.

1.3. Formal Proofs. To prove an argument is valid:

- Assume the hypotheses are true.
- Use the rules of inference and logical equivalences to show that the conclusion is true.

Discussion

What is a proof?

A proof is a demonstration, or argument, that shows beyond a shadow of a doubt that a given assertion is a logical consequence of our axioms and definitions. Thus, in any problem in which you are asked to provide a proof, your solution will not simply be a short answer that you circle. There are certain rules that must be followed (which we will get to shortly), and certain basic knowledge must be assumed. For example, one may assume the axioms and any previously stated theorems (unless the instructions state otherwise). A large number of proofs simply involve showing that a certain definition is satisfied.

In almost every case, the assertions we will be proving are of the form "if p, then q", where p and q are (possibly compound) propositions. The proposition p is the *hypothesis* and q is the *conclusion*. It is almost always useful to translate a statement that must be proved into an "if ..., then ..." statement if it is not already in that form. To begin a proof we assume the hypotheses. For example, consider the argument

Every dog will have his day.
Fido is a dog.
Therefore, Fido will have his day.

The hypotheses of this argument are "Every dog will have his day" and "Fido is a dog." The conclusion is "Fido will have his day."

1.4. Rules of Inference.

Modus Ponens or the Law of Detachment	p $p \to q$ $\therefore q$
Disjunction Introduction	p $\therefore p \vee q$
Conjunction Elimination	$p \wedge q$ $\therefore p$
Modus Tollens	$\neg q$ $p \to q$ $\therefore \neg p$
Hypothetical Syllogism	$p \to q$ $q \to r$ $\therefore p \to r$
Disjunctive Syllogism	$p \vee q$ $\neg p$ $\therefore q$
Conjunction Introduction	p q $\therefore p \wedge q$
Constructive Dilemma	$(p \to q) \wedge (r \to s)$ $p \vee r$ $\therefore q \vee s$

Discussion

An argument is **valid** if it is uses only the given hypotheses together with the axioms, definitions, previously proven assertions, and the *rules of inference*, which are listed above. In those rules in which there is more than one hypothesis, the order

of the hypotheses is not important. For example, *modus tollens* could be just as well stated:

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

The notation used in these slides is commonly used in logic to express an argument symbolically. The proposition(s) before the horizontal line are the hypotheses and the proposition below the line is the conclusion. The symbol $\therefore$ is a common shorthand for "therefore."

Each of the rules of inference is a tautology expressed in a different form. For example, the rule of *modus ponens*, when stated as a propositional form, is the tautology

$$[p \wedge (p \to q)] \to q.$$

(This can be verified using a truth table.)

REMARK 1.4.1. *An argument of the form*

$$\begin{array}{l} h_1 \\ h_2 \\ \vdots \\ h_n \\ \hline \therefore c \end{array}$$

is valid if and only if the proposition $[h_1 \wedge h_2 \wedge \cdots \wedge h_n] \to c$ *is a tautology.*

1.5. Example 1.5.1.

EXAMPLE 1.5.1. *The following is a valid logical argument:*

1. *If the dog eats the cat food or scratches at the door, then the parrot will bark.*
2. *If the cat eats the parrot, then the parrot will not bark.*
3. *If the cat does not eat the parrot, then it will eat the cat food.*
4. *The cat did not eat the cat food.*
5. *Therefore, the dog does not eat the cat food either.*

Discussion

Here is how the hypotheses give us the conclusion:

1. Assign propositional variables to the component propositions in the argument:
   - d – the dog eats the cat food
   - s – the dog scratches at the door
   - p – the parrot will bark
   - c – the cat eats the parrot
   - e – the cat eats the cat food
2. Represent the formal argument using the variables:
   $(d \vee s) \rightarrow p$
   $c \rightarrow \neg p$
   $\neg c \rightarrow e$
   $\neg e$
   $\therefore \neg d$
3. Use the hypotheses, the rules of inference, and any logical equivalences to prove that the argument is valid:

	Assertion	Reason
1.	$\neg c \rightarrow e$	hypothesis 3
2.	$\neg e$	hypothesis 4
3.	c	steps 1 and 2 and *modus tollens*
4.	$c \rightarrow \neg p$	hypothesis 2
5.	$\neg p$	steps 3 and 4 and *modus ponens*
6.	$(d \vee s) \rightarrow p$	hypothesis 1
7.	$\neg(d \vee s)$	steps 5 and 6 and *modus tollens*
8.	$\neg d \wedge \neg s$	step 7 and De Morgan's law
9.	$\neg d$	step 8 and conjunction elimination

We could also determine if the argument is valid by checking if the proposition $[((d \vee s) \rightarrow p) \wedge (c \rightarrow \neg p) \wedge (\neg c \rightarrow e) \wedge (\neg e)] \rightarrow (\neg d)$ is a tautology. In practice, though, it is more useful to recognize if the rules of inference have been applied appropriately or if one of the common fallacies have been used to determine if an argument is valid or not. It will serve you better later on to understand the two column proof of a valid argument and to recognize how the rules of inference are applied.

EXERCISE 1.5.1. *Give a formal proof that the following argument is valid. Provide reasons.*

$a \vee b$

$\neg c \rightarrow \neg b$

$\neg a$

$\therefore c$

EXERCISE 1.5.2. *Determine whether the following argument is valid. Give a formal proof. Provide reasons.*

$\neg(\neg p \vee q)$

$\neg z \rightarrow \neg s$

$s \rightarrow (p \wedge \neg q)$

$\neg z \vee r$

$\therefore r$

1.6. Rules of Inference for Quantifiers.

Universal Instantiation	$\dfrac{\forall x P(x)}{\therefore P(c)}$
Universal Generalization	$\dfrac{P(c) \text{ for arbitrary member, } c, \text{ of the universe}}{\therefore \forall x P(x)}$
Existential Generalization	$\dfrac{P(c) \text{ for some member, } c, \text{ of the universe}}{\therefore \exists x P(x)}$
Existential Instantiation	$\dfrac{\exists x P(x)}{\therefore P(c)}$

Discussion

Here is the list of additional rules of inference related to quantifiers. The symbol c represents some particular element from the universe of discourse for the variable x.

In Universal Instantiation, c may be any element from the universe of discourse for x. For example, suppose the universe of discourse is the set of real numbers, and $P(x)$ is the predicate $x^2 \geq 0$. Since $x^2 \geq 0$ for all x, we may conclude $(a-b)^2 \geq 0$ for arbitrary real numbers a and b. Here, $c = a - b$. We may also conclude $(-\pi)^2 \geq 0$.

In Existential Instantiation, c must be chosen so that $P(c)$ is true. For example, suppose the universe of discourse is the set of integers, and let $P(x)$ be the predicate, "x is a divisor of 17283 and $1 < x < 17283$." Then $\exists x P(x)$ is a true statement (e.g., $P(3)$). We may then assume c is a divisor of 17283 and $1 < c < 17283$ for some integer c.

Sometimes we may know a statement of the form $\exists x P(x)$ is true, but we may not know exactly for what x in the domain of discourse gives us that this is true. In a proof when we know the truth of $\exists x P(x)$ we can define a variable, say c, to stand for a fixed element of the domain where $P(c)$ is true. This is what Existential Instantiation gives you. An example in which we have this situation is by using the Intermediate Value Theorem from algebra.

Let $f : \mathbb{R} \to \mathbb{R}$ be the polynomial $f(x) = -3x^4 + x^3 + 2x + 1$. Since $f(1) = 1$, $f(2) = -35$, and f is continuous, there must be a solution to $f(x) = 0$ in the interval $[1, 2]$. It may not possible to find this solution algebraically, though, and may only be possible to numerically approximate the root. However, if we needed to use the solution for some purpose we could simply say let $c \in [1, 2]$ be such that $f(c) = 0$ and this fixes c as the solution we know exists in $[1, 2]$.

Universal Generalization is a subtle and very useful rule and the meaning may not be clear to you yet. The variable x stands for any arbitrary element of the universe of discourse. You only assume x is a member of the universe and do not place any further restrictions on x. If you can show $P(x)$ is true, then it will also be true for any other object satisfying the same properties you've claimed for x. In other words, $P(x)$ is true for all the members of the universe, $\forall x P(x)$. You will see a standard approach in proving statements about sets is to use Universal Generalization.

1.7. Example 1.7.1.

EXAMPLE 1.7.1. *Here is a simple argument using quantifiers.*

1. *Every dog will have his day.*
2. *Fido is a dog.*
3. *Therefore, Fido will have his day.*

Discussion

To verify this is a valid argument we use the same technique as before.

Define the predicates

- $M(x)$: x is a dog
- $D(x)$: x has his day

and let F represent Fido, a member of the universe of discourse.

The argument becomes

$\forall x[M(x) \to D(x)]$
$M(F)$
$\therefore D(F)$

The proof is

1.	$\forall x[M(x) \to D(x)]$	hypothesis 1
2.	$M(F) \to D(F)$	step 1 and universal instantiation
3.	$M(F)$	hypothesis 2
4.	$D(F)$	steps 2 and 3 and *modus ponens*

EXERCISE 1.7.1. *Determine whether the following argument is valid or invalid. Give a formal proof. Provide reasons.*

There is someone in this class who has taken Calculus III. Everyone who takes Calculus III also takes Physics (concurrently). Therefore, someone in this class has taken Physics.

1.8. Fallacies. The following are **not valid** argument forms.

Affirming the Consequent	$p \to q$ q $\therefore p$
Denying the Antecedent	$p \to q$ $\neg p$ $\therefore \neg q$
Begging the Question or Circular Reasoning	Use the truth of the consequent in the argument

Discussion

There are several common mistakes made in trying to create a proof. Here we list three of the most common *fallacies* or errors in logic. Since they are not valid arguments, obviously you should *not* use them in a proof. Just as important, you should be able to recognize one of them if you were to encounter it in someone else's argument.

The fallacy of affirming the consequent occurs when the converse of a premise is used to prove a statement. For example, here is an "argument" using the fallacy of affirming the consequent.

EXAMPLE 1.8.1. *If Jack lands the new account, then he will get a raise. Jack got a raise. Therefore, he landed the new account.*

Note that $[(p \to q) \wedge q] \to p]$ is *not* a tautology, so this is not a valid argument. The "if ..., then ..." statement is not equivalent to its converse. In the above example, just because Jack got a raise, you can't conclude from the hypothesis that he landed the new account.

The fallacy of denying the antecedent comes from the fact that an implication is not equivalent to its inverse. Here is an example of incorrect reasoning using the fallacy of denying the antecedent:

EXAMPLE 1.8.2. *If the cat is purring, then he ate the canary. The cat is not purring. Therefore, the cat didn't eat the canary.*

In this example, the hypothesis does not allow you to conclude anything if the cat is not purring, only if he *is* purring. The fallacy results from the fact that the propositional form $[(p \to q) \wedge \neg p] \to \neg q$ is not a tautology.

Begging the question, or circular reasoning, occurs when the conclusion itself is used in the proof. Here is an example of this type of fallacy:

EXAMPLE 1.8.3. *Prove: If xy is divisible by 5, then x is divisible by 5 or y is divisible by 5.*

> *Incorrect Proof: If xy is divisible by 5, then $xy = 5k$ for some k. Then $x = 5\ell$ for some ℓ, or $y = 5\ell$ for some ℓ. Hence, x is divisible by 5 or y is divisible by 5.*

This argument breaks down once we assert, without justification, that either $x = 5\ell$ for some ℓ, or $y = 5\ell$ for some ℓ. This, of course, is what we are trying to prove, and it doesn't follow directly from $xy = 5k$.

EXERCISE 1.8.1. *Give a careful proof of the statement: For all integers m and n, if m is odd and n is even, then $m + n$ is odd.*

EXAMPLE 1.8.4. *Prove: for all real x, $x < x + 1$.*

PROOF. First we fix an arbitrary real number: Let $x \in \mathbb{R}$. We wish to show $x < x+1$. This inequality is equivalent to $0 < (x+1)-x$. But by the commutative and associative properties of real numbers this inequality is equivalent to $0 < 1 + (x - x)$ or equivalently, $0 < 1$. We know the last inequality is true and so the equivalent expression $x < x + 1$ is also true.

□

In the previous example we took the expression we wished to show was true and rewrote it several times until we reached an expression that we knew to be true. This is a useful tool but one must be extremely cautious in using this technique. Notice we did not actually assume what we wished to prove. Instead, we used equivalences to rephrase what we needed to show.

EXAMPLE 1.8.5. *Now, here is an incorrect "proof" of the same statement in Exercise 1.8.4. This proof would be marked wrong.*

INCORRECT "PROOF" OF EXERCISE 1.8.4. Let $x \in \mathbb{R}$. Then

$$\begin{aligned} & x < x + 1 \\ \Rightarrow\ & 0 < (x + 1) - x \\ \Rightarrow\ & 0 < (x - x) + 1 \quad \text{by the associative and commutative} \\ & \qquad\qquad\ \ \text{properties of real numbers} \\ \Rightarrow\ & 0 < 1 \end{aligned}$$

We know $0 < 1$. □

EXERCISE 1.8.2. *Consider the following hypotheses: If the car does not start today, then I will not go to class. If I go to class today then I will take the quiz. If I do not take the quiz today then I will ask the teacher for an extra credit assignment. I asked the teacher for an extra credit assignment.*

Determine whether each of the following are valid or invalid conclusions of the above hypotheses. Why or why not?

(1) *I did not go to class today.*
(2) *Remove the hypothesis "I asked the teacher for an extra credit assignment" from the above assumptions. Can one now conclude "If the car does not start today, then I will ask the teacher for an extra credit assignment" for the remaining assumptions?*

EXERCISE 1.8.3. *Find the error in the proof of the following statement.*

Suppose x is a positive real number. Claim: the sum of x and its reciprocal is greater than or equal to 2.

INCORRECT "PROOF". Multiplying by x we get $x^2 + 1 \geq 2x$. By algebra, $x^2 - 2x + 1 \geq 0$. Thus $(x-1)^2 \geq 0$. Any real number squared is greater than or equal to 0, so $\frac{x^2+1}{x} \geq 2$ is true. □

EXERCISE 1.8.4. *Find the fallacy associated with the following:*

Problem: *Solve for x given the equation $\sqrt{x} + \sqrt{x-a} = 2$, where a is a real number.*

Incorrect "Solution": *The given equation also implies that*

$$\frac{1}{\sqrt{x} + \sqrt{x-a}} = \frac{1}{2},$$

so

$$\sqrt{x} - \sqrt{x-a} = \frac{a}{\sqrt{x} + \sqrt{x-a}} = \frac{a}{2}.$$

Adding the original equation with this one gives

$$2\sqrt{x} = 2 + (a/2)$$

and thus

$$x = (1 + \frac{a}{4})^2.$$

Notice, however, if $a = 8$ then $x = 9$ according to the solution, but this does not satisfy the original equation.