Section 2.1: Proof Techniques

September 10, 2007

Abstract

Sometimes we see patterns in nature and wonder if they hold in general: in such situations we are demonstrating inductive reasoning to propose a **theorem**, which we can attempt to prove via deductive reasoning. From our work in Chapter 1, we conceive of a theorem as an argument of the form $P \rightarrow Q$, whose validity we seek to demonstrate.

This section outlines a variety of proof techniques, including direct proofs, proofs by contraposition, proofs by contradiction, proofs by exhaustion, and proofs by dumb luck or genius! You have already seen each of these in chapter 1 (with the exception of "dumb luck or genius", perhaps!).

1 Theorems and Informal Proofs

The theorem-forming process is one in which we

- make observations about nature, about a system under study, etc.;
- discover patterns which appear to hold in general;
- state the rule; and then
- attempt to prove it (or disprove it!).

This process is formalized in the following definitions:

- **inductive reasoning** - drawing a conclusion based on experience, which one might state as a conjecture, hypothesis, or theorem.
- **deductive reasoning** - application of a logic system to investigate a proposed conclusion based on hypotheses (hence proving, disproving, or, failing either, holding in limbo the conclusion).
- **counterexample** - an example which violates a proposed rule (or theorem), proving that the rule doesn't work in the particular interpretation.

Before attempting to prove a theorem, we should be convinced of its correctness; if we doubt it, then we should pursue the line of our doubt, and attempt to find a counterexample.

1.1 Exhaustive Proof

Example: The Four-color problem

- Description (see p. 369/432).
- This theorem is partly famous because it provided the first example of a computer-aided proof of a major result. The reason the computer became useful was that the proof came down to testing a rather large number of special cases (proof by exhaustion).

When there are only a few things (in particular, a finite number) to test, we can use proof by exhaustion.

Example: Prolog

Prolog stands for "PROgramming in LOGic", and is built on a finite database of "facts", "rules" relating facts and rules, and then the inference and deduction rules of logic. For example, we might find in our data base that

$$\begin{array}{l} animal(raccoon) \\ animal(bear) \\ animal(fish) \\ plant(algae) \\ eats(fish, algae) \\ eats(bear, fish) \end{array}$$

From these facts and rules, we can then create new wffs using the standard connectives, such as

Rule	*Definition*
$prey(x)$	$eat(y,x) \wedge animal(x) \rightarrow prey(x)$
$inFoodChain(y,x)$	$eats(y,x) \vee (\exists z)(eats(y,z) \wedge inFoodChain(z,x)) \rightarrow inFoodChain(y,x)$

Note that the definition of *inFoodChain* is recursive (more on that later!).

We are then able to test conjections, or theorems, such as

$$\begin{array}{l} (\exists x) animal(x) \text{ or} \\ inFoodChain(bear, algae) \end{array}$$

by simply doing a proof by exhaustion: it checks all cases, and eventually finds that

- There is an animal (e.g. bear), and that
- algae is indeed in the bear's food chain, via fish.

Example: My young friend Sam

Kids are wonderful at developing conjectures, and sometimes even applying deductive logic as illustrated by my friend Sam's Story. Sam made an amazing application of proof by exhaustion.

Practice 1, p. 85/90 illustrates the kinds of conjectures kids will make (e.g. "All animals living in the ocean are fish."), and parents, sibling, friend, and teachers all have the priviledge and pleasure of coming up with counterexamples.

1.2 Direct Proof

The most obvious, and perhaps common technique, is the direct proof: you start with your hypotheses P_i, and proceed toward your conclusion Q:

$$P_1 \land P_2 \land \cdots \land P_n \to Q$$

Example: Exercise 9/12, p. 92/98

Prove directly that the sum of even integers is even

x even $\land$ y even $\to$ $x+y$ even

1. x even — hyp
2. y even — hyp
3. $(\exists m)(x = 2m)$ — defn of evenness
4. $(\exists n)(y = 2n)$ — "
5. $x = 2m$ — ei, 3
6. $y = 2n$ — ei, 4
7. $x + y = 2m + 2n$ — defn. of add
8. $x + y = 2(m+n)$ — dist.
9. $m + n \in \mathbb{Z}$ — closure!
10. $(\exists\, m+n)(x + y = 2(m+n))$ — eg.
11. $x + y$ even — defn

1.3 Contraposition

If $P \to Q$ isn't getting you anywhere, you can use your logic systems to rewrite it as $Q' \to P'$ (the contrapositive). This is called "proof by contraposition".

Example: Practice 4 and 5, p. 89/94

The statements from chapter 1.1 are:

1. If the rain continues, then the river will flood.
2. A sufficient condition for network failure is that the central switch goes down.
3. The avocados are ripe only if they are dark and soft.
4. A good diet is a necessary condition for a healthy cat.

Example: Exercise 17/21, p. 93/99 If x is positive, so is $x+1$.

(Proof by contraposition)

If $x+1$ not positive, then x is not positive.

1. $x+1$ not positive hyp
2. $x+1 \leq 0$ defn.
3. $x \leq -1$ law of inequalities
4. $-1 \leq 0$
5. $x \leq -1 \leq 0$
6. $x \leq 0$
7. x is not positive

1.4 Contradiction

Contradiction represents some interesting logic: again, we want to prove $P \to Q$, but rather than proceed directly, we seek to demonstrate that $P \wedge Q' \to 0$: that is, that P and Q' leads to a contradiction. Then we cannot have both P true, and Q false - which would lead to $P \to Q$ false, of course.

Example: Exercise 22/26, p. 93/99 $(\forall x)[x \text{ prime} \wedge x \text{ even} \to x = 2]$

If x is an even prime number, then $x = 2$.

Proof by contradiction: suppose not

$(\exists x)[x \text{ even prime} \wedge x \neq 2] \to 0$

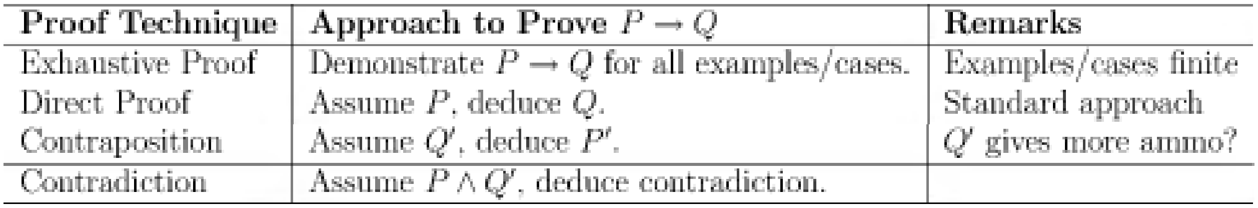
H. $(\exists x)[x \text{ even prime} \wedge x \neq 2]$

0. x even prime $\wedge\ x \neq 2$

1. x even prime 0, simp
2. $x \neq 2$ 0, simp
3. $(\exists m)(x = 2m)$ defn. of evenness
4. $x = 2m$ 3, ei
5. $2 \mid x$ defn. of divisibility
6. $x = 2$ x is prime, only divisible by 1 & itself

contradiction!

Table 1: Summary of useful proof techniques, from Gersting, p. 91/96.



Proof Technique	**Approach to Prove $P \to Q$**	**Remarks**
Exhaustive Proof	Demonstrate $P \to Q$ for all examples/cases.	Examples/cases finite
Direct Proof	Assume P, deduce Q.	Standard approach
Contraposition	Assume Q', deduce P'.	Q' gives more ammo?
Contradiction	Assume $P \wedge Q'$, deduce contradiction.	

1.5 Serendipity

Mathematicians often spend a great deal of time finding the most "elegant" proof of a theorem, or the shortest proof, or the most intuitive proof. We may stumble across a beautiful proof quite by accident ("serendipitously"), and those are perhaps the most pleasant proofs of all. There is a wonderful story associated with Exercise 55/69, p. 94/100.