Section 2.1: Proof Techniques

February 1, 2022

Abstract

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

Example: A student was doing a proof and suddenly speculated "Couldn't we just say $(A \to (B \to C)) \wedge B \to (A \to C)$?" Can she? It's a theorem – either we prove it, or we provide a counterexample.

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).

We can prove it:

1. $A \to (B \to C)$ hyp
2. B hyp
3. A ded. method
4. $B \to C$ 1, 3, mp
5. C 2, 4, mp

✓

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;
- propose a rule, or "law"; and then
- attempt to prove it (or else **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 or theorem; but almost always as If (hypotheses) then (conclusion).

- **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), thus 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. 507).
  - This theorem is partly famous because it provided the first example of a computer-aided proof of a major mathematical 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). "They ... constructed an unavoidable set with around 1500 configurations.... Appel and Haken used 1200 hours of computer time to work through the details of the final proof."

  When there are only a few things (in particular, a finite number of cases) to test, we can use proof by exhaustion. (It may still take 1200 hours of computer time!:)
- **Example: Sherlock Holmes says "Once you eliminate the impossible, whatever remains, no matter how improbable, must be the truth." But only if you have a finite number of impossibilities may you use exhaustion to arrive at a conclusion!**
- **Example:** My young friend Sam made a very mature application of proof by exhaustion.

  Kids are wonderful at developing conjectures, and sometimes even applying deductive logic, as illustrated by Sam. Kids will also make all sorts of false conjectures (e.g. "All animals living in the ocean are fish," or "all meat-eaters are animals"), and parents, siblings, friends, and teachers all have the privilege and pleasure of coming up with counterexamples.

1.2 Direct Proof

there exist → ∃ integers m and n such that

The most obvious and common technique is the direct proof: you start with your hypotheses $\{P_i\}$, and proceed as directly as possible toward your conclusion Q:

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

Example: Exercise 13, p. 108 Prove directly that the sum of even integers is even.

two ∧

Given two even integers x + y,

$x = 2m$, $y = 2n$ | defn

Consider the sum

$x + y = 2m + 2n$

$= 2(m+n)$

1.3 Contraposition

hypothesis

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. 104, asks us to distinguish the converse ($Q \to P$) from the contrapositive ($Q' \to P'$): The statements from chapter 1.1 are:

(a) If the rain continues, then the river will flood.

- Rewritten as: $R \to F$
- Contrapositive: $F' \to R'$
- Converse: $F \to R$

(b) A sufficient condition for network failure is that the central switch goes down.

- Rewritten as: $CS \to NF$
- Contrapositive: $NF' \to CS'$
- Converse: $NF \to CS$

(c) The avocados are ripe only if they are dark and soft.

- Rewritten as: $R \to (D \wedge S)$
- Contrapositive: $(D \wedge S)' \to R'$
- Converse: $(D \wedge S) \to R$

(d) A good diet is a necessary condition for a healthy cat.

- Rewritten as: $H \to GD$
- Contrapositive: $GD' \to H'$
- Converse: $GD \to H$

Since integers are closed under addition, m+n is an integer.

∴ therefore

∴ x + y is even, since it can be written as the product of two and an integer.

Example: Exercise 23, p. 108 . Prove: If a number x is positive, so is $x + 1$ (do a proof by contraposition).

hypothesis

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

Does this sound familiar? It's **exactly** the strategy of TautologyTest.

Example: Exercise 29, p. 109 Prove (by contradiction): If x is an even prime number, then $x = 2$.

Table 1: Summary of useful proof techniques, from Gersting, p. 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.	e.g. TautologyTest

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 76, p. 110.

Prove: the sum of the integers from 1 to 100 is 5050.

At the end of a proof the mathematician likes to let everyone know that it's all over, frequently writing "QED" – shorthand for *quod erat demonstrandum* – roughly, "that which was to be shown." I'll just say "QED!"

To move toward section 2.2 (mathematical induction), how would we prove this theorem:

Prove: the sum of the positive integers from 1 to n is $\frac{n(n+1)}{2}$.

These sums are the so-called "triangular numbers", also found in Pascal's (Yanghui's) triangle.