Chapter 4

Proof Techniques

"Absence of proof is not proof of absence." M. Crichton

We now come to the last part of predicate logic, namely, we will see how to apply the logic rules we have seen to justify different proof techniques. We will discuss three proof technique: direct proof, induction, proof by contradiction.

Direct Proof. As the name suggests, these are proofs that are perfomed without particular techniques. Some claim has to be shown, and there is a specific way to do so in this particular context.

Example 42. Suppose we want to show that $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$, $\forall n \in \mathbb{N}$. Write down the following array:

$$\begin{array}{cccccc} 1 & 2 & 3 & \dots & n-1 & n \\ n & n-1 & n-2 & \dots & 2 & 1 \end{array}$$

If you sum up the entries of the first row, you get $\sum_{i=0}^{n} i$, and if you sum up the entries of the second row, you also get $\sum_{i=0}^{n} i$, Thus if you sum up all entries in this array, you get $2\sum_{i=0}^{n} i$. Now if we sum up the first column, we get $n+1$, if we sum up the second column we get $n+1$, ..., and for the nth column we also get $n+1$, so the total is $n+1$ times n columns.

Proof Techniques

A valid proof is a valid argument, i.e. the conclusion *follows* from the given assumptions.

Three techniques:
- Direct proof
- Proof by induction
- Proof by contradiction.

Proof by example:
The author gives only the case n = 2 and suggests that it contains most of the ideas of the general proof.

Proof by intimidation: 'Trivial.'

Proof by cumbersome notation: Best done with access to at least four alphabets and special symbols.

Proof by exhaustion: An issue or two of a journal devoted to your proof is useful.

Proof by omission: 'The reader may easily supply the details.' 'The other 253 cases are analogous.' '...'

Proof by obfuscation: A long plotless sequence of true and/or meaningless syntactically related statements.

Proof by wishful citation: The author cites the negation, converse, or generalization of a theorem from literature to support his claims.

© PROOF TECHNIQUES by A. H. Zemanian, The Physics Teacher, May 1994.

Proof Technique: Direct Proof

- Prove that $\forall n \in N, \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$
- Define $S = \sum_{i=0}^{n} i = \underbrace{0+1+2+\ldots+n-1+n}_{\text{n+1 terms}}$
  - Note: $S = \sum_{i=0}^{n} i = n+n-1+\ldots+2+1+0$
- Sum up: $2S = \overbrace{n+n+\ldots+n+n+n}^{\text{n+1 terms}}$

$$\Rightarrow 2S = (n+1)n$$

- Thus: $S = \frac{n(n+1)}{2}$

Leonhard Euler
(1707-1783)

3/11

If we sum up the elements horizontally, we got $2\sum_{i=0}^{n} i$, while if we sum up the elements vertically, we got $n(n+1)$. But the sum does not change when we count differently, thus:

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$$

The legend attributes this proof technique to young Euler, who apparently was punished for not behaving in the classroom. His teacher would have asked him to compute the sum of integers from 1 to 100, and Euler would have, or so the legend says, came up with this technique so as to have to compute all the additions!

Mathematical Induction. This is a proof technique to show statements of the form $\forall n,\ P(n)$. We first explain the technique, then give a proof of why this proof technique is valid, and finally provide an example. A proof by mathematical induction follows two steps:

1. Basis step: You need to show that $P(1)$ is true.
2. Inductive step: You assume that $P(k)$ is true, and have to prove that $P(k+1)$ is then true.

When both steps are complete, we have proved that $\forall n,\ P(n)$ is true. Why is that the case? From the inductive step, we have that

$$P(k) \to P(k+1)$$

for any k, therefore this is true for when we instantiate in $k = 1$, that is

$$P(1) \to P(2).$$

But from the basis step, we know that $P(1)$ is true, thus combining $(P(1) \to P(2)); P(1)$; we get that therefore $P(2)$ holds. We can repeat this process with $k = 2$ to deduce that $P(3)$ holds, and so on and so forth.

Mathematical Induction

- Prove propositions of the form: $\forall n\ P(n)$
- The proof consists of two steps:
  - Basis Step: The proposition P(1) is shown to be true
  - Inductive Step:
    - Assume P(k) is true (when n=k), then, prove P(k+1) is true (when n=k+1).
- When both steps are complete, we have proved that "$\forall n$ P(n)" is true

Why Does it Work?

- From step 2: $P(1) \rightarrow P(2)$ by Universal Instantiation.
- From step 1: $P(1)$
- Applying *modus ponen*: $P(2)$.
- Repeat the process to get P(3),P(4), P(5), etc. So, all P(k) are true! i.e., $\forall n\ P(n)$

Analogy with climbing Ladders.

Inductive step

$$[P(1) \wedge \forall k(P(k) \rightarrow P(k+1))] \rightarrow \forall n P(n)$$

Basis

Hypothesis

(valid argument)

Example 43. We want to prove

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2},\ \forall n\ \mathbb{N}$$

using mathematical induction. Then set

$$P(n) = \text{“}\sum_{i=0}^{n} i = \frac{n(n+1)}{2}\text{”},\ \forall n\ \mathbb{N}.$$

- Basis step: $P(1) = 1 = \frac{1(1+1)}{2}$.
- Inductive step: suppose that $P(k)$ is true, that is $\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$ is true for all k. Now we need to show that $P(k+1)$ holds.

$$\begin{aligned}\sum_{i=0}^{k+1} i &= \sum_{i=0}^{k} i + (k+1)\\ &= \frac{k(k+1)}{2} + (k+1)\\ &= \frac{k(k+1)+2(k+1)}{2} = \frac{(k+1)(k+2)}{2}.\end{aligned}$$

There $P(n)$ is true for all n.

Complete Induction. A proof by complete induction is a variation of mathematical induction. A proof by complete induction follows two steps:

1. Basis step: You need to show that $P(1)$ is true.
2. Inductive step: You assume that for $k > 1$, $P(m)$ is true for every $m < k$, and have to prove that $P(k)$ is then true.

When both steps are complete, we have proved that $\forall n,\ P(n)$ is true. Notice the difference with mathematical induction: for mathematical induction, we assume that $P(k)$ is true for an arbitrary k, and we prove $P(k+1)$, while for complete induction, we assume that $P(m)$ is true for every $m < k$, and then prove that $P(k)$ is true.

We give an example of complete induction which illustrates the difference between mathematical induction and complete induction.

Example: Mathematical Induction

- Prove that $\forall n \in N, \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$
- Let P(n) denote $\left[\sum_{i=0}^{n} i = \frac{n(n+1)}{2}\right]$

Basis step: P(1) is true

$$1 = \frac{1(1+1)}{2}$$

- Inductive step. Assume P(k) true, k>0: $\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$

  Prove P(k+1) true :

$$\sum_{i=0}^{k+1} i = \sum_{i=0}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1)$$
$$= \frac{(k+1)(k+2)}{2} = \frac{(k+1)[(k+1)+1]}{2}$$

So, *P*(*n*) is true for *n*=*k*+1 and thus true for all n: $\forall n$ P(*n*) is true

6/11

Complete Induction

- Prove propositions of the form: ∀n P(n)
- The proof consists of two steps:
  - Basis Step: The proposition P(1) is shown to be true
  - Inductive Step:
    - Assume, for k>1, P(m) is true **for every m < k**, then, prove P(k) is true.
- When both steps are complete, we have proved that "$\forall n$ P(*n*)" is true

Example 44. We want to prove that every natural number $n > 1$ is either a prime, or a product of primes. We define $P(n)$ to be "$(n = 1) \vee (n$ is prime$) \vee$ (n can be factored into primes)".

1. Basis step: You need to show that $P(1)$ is true, and indeed $P(1)$ is true.

2. Inductive step: You assume that for $k > 1$, $P(m)$ is true for every $m < k$, and have to prove that $P(k)$ is then true. So either k is a prime, or it is not. If k is a prime, then we are done because $P(k)$ is true. Otherwise, since $k > 1$, we can factor $k = pq$ with p, q natural numbers smaller than k. Now we can apply the induction on both p and q. Therefore both p and q are factored into primes, and so is k, which concludes the proof.

Note here that the usual mathematical induction does not work: when $k = pq$, p and q are not related to $k - 1$, they are typically smaller.

Proof by Contradiction. We want to prove that $P(n) \to Q(n)$ is true. In a proof by contradiction, we assume by contradiction that $P(n) \to Q(n)$ is false, that is, that $\neg(P(n) \to Q(n))$ is true. The only way this might happen, is if $P(n)$ is true and $Q(n)$ is false. Thus we start with $P(n)$ true and $Q(n)$ false. If from there we deduce a contradiction, that is a statement of the form $C \wedge \neg C$, which is always false, what we have proven is

$$\neg(P(n) \to Q(n)) \to C \wedge \neg C$$

is true. This is equivalent to $P(n) \to Q(n)$. To see that, set $S(n) =$ "$P(n) \to Q(n)$", and look at the truth table:

S	C	$\neg S$	$C \wedge \neg C$	$(\neg S) \to (C \wedge \neg C)$
T	T	F	F	T
T	F	F	F	T
F	T	T	F	F
F	F	T	F	F

Therefore, to prove $P(n) \to Q(n)$ (or any other statement), it suffices to instead prove the conditional statement $\neg(P(n) \to Q(n)) \to C \wedge \neg C$, which is done by direct proof, by assuming $\neg(P(n) \to Q(n))$ and deduce $C \wedge \neg C$. One difficulty is to figure out what is C given the proof to effectuate.

Example: Complete Induction

- Prove that every natural number n>1 is either a prime, or a product of primes.
- P(n)="(n=1) V (n is prime) V (n can be factored into primes)"
- Basis Step: P(1) is true because n=1
- Inductive Step: Suppose k>1, and P(m) is true for all m<k.

  We must show that P(k) is true.

  ✓ If k is prime, then P(k) is true.
  ✓ Otherwise, since k>1, we can factor k=pq, with p,q natural numbers <k.
  The factor p is either prime or factors into prime, by induction hypothesis.
  ✓ And the same is true for q.
  Therefore k factors into primes.

8/11

Proof by Contradiction

- We want to prove $P(n) \rightarrow Q(n)$
- Assume by contradiction that $\neg(P(n) \rightarrow Q(n))$
- This happens exactly if P(n) and $\neg Q(n)$.
- Suppose that P(n) and $\neg Q(n)$.
- Prove that this gives a contradiction, namely

  $\neg(P(n) \rightarrow Q(n)) \rightarrow C \wedge \neg C$

- This is equivalent to P(n) → Q(n) (truth table!)

Example 45. Suppose we want to prove that: if n^2 is even, then n is even, for n integer. Set $P(n)$="n^2 is even", and $Q(n)$="n is even". We want to prove that $P(n) \to Q(n)$, which is equivalent to $\neg(P(n) \to Q(n)) \to C \wedge \neg C$. Suppose $\neg(P(n) \to Q(n))$, that means $P(n)$ is true and $Q(n)$ is false: n^2 is even, and n is not even (equivalently n is odd). Now if n is odd, then $n = 2k + 1$, and $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, that is n^2 is odd. Thus $C =$ "n^2 is even", and we have just shown that n^2 is odd, that is $C \wedge \neg C$, a contradiction!

We may alternatively use that $P(n) \to Q(n)$ is equivalent to $\neg Q(n) \to \neg P(n)$. This would be a proof using contrapositive.

Example 46. Suppose we want to prove that: if n^2 is even, then n is even, for n integer. Set $P(n)$="n^2 is even", and $Q(n)$="n is even". We want to prove that $P(n) \to Q(n)$, which is equivalent to $\neg Q(n) \to \neg P(n)$. Suppose that $\neg Q(n)$, that is: n is not even, or n is odd. Now if n is odd, then $n = 2k + 1$, and $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, that is n^2 is odd, which is equivalent to $\neg P(n)$, which concludes the proof.

Proof by Contradiction: Example

- Prove that: If n^2 is even, then n is even, for n integer.
- Lets assume: n^2 is even but n is not even (P(n)="n^2 is even " and Q(n)="n is even ").
- n is not even $\Leftrightarrow$ n is odd, i.e., $n = 2k+1$, k integer.
  - Then $n^2 = (2k+1)^2$
    $= 4k^2 + 4k + 1$
    $= 2(2k^2 + 2k) + 1$ (odd)
- This is a contradiction (C="n^2 is even" , $C \wedge \neg C$)
- *This concludes the proof!*

10/11

Proof by Contrapositive

- We want to prove $P(n) \rightarrow Q(n)$
- This is equivalent to prove that $\neg Q(n) \rightarrow \neg P(n)$

Example: Prove that if n^2 is even, then n is even.

- P(n)="n^2 is even", Q(n)="n is even"
- n is not even $\Leftrightarrow$ n is odd, i.e., $n = 2k+1$, k integer.
  - Then $n^2 = (2k+1)^2$
    $= 4k^2 + 4k + 1$
    $= 2(2k^2 + 2k) + 1$ (odd)
- This shows that $\neg P(n)$, and concludes the proof!

Exercises for Chapter 4

Exercise 38. Let q be a positive real number. Prove or disprove the following statement: if q is irrational, then $\sqrt{q}$ is irrational.

Exercise 39. Prove using mathematical induction that the sum of the first n odd positive integers is n^2.

Exercise 40. Prove using mathematical induction that $n^3 - n$ is divisible by 3 whenever n is a positive integer.

Exercise 41. Prove by mathematical induction that

$$1^2 + 2^2 + \ldots + n^2 = \frac{1}{6}n(n+1)(2n+1).$$