Section 1.7
Proof Methods and Strategy

Existence Proofs

We wish to establish the truth of

$$xP(x).$$

• ***Constructive*** existence proof:

- Establish P(c) is true for some c in the universe.

- Then $xP(x)$ is true by Existential Generalization (EG).

Example:

Theorem: *There exists an integer solution to the equation* $x^2 + y^2 = z^2$.

Proof:

Choose x = 3, y = 4, z = 5.

Example:

Theorem: *There exists a bijection from A= [0,1] to B= [0, 2].*

Proof:

We build two injections and conclude there must be a bijection without ever exhibiting the bijection.

Let f be the identity map from A to B.

Then f is an injection (and we conclude that $| A | \leq | B |$).

Define the function g from B to A as g(x) = x/4.

Then g is an injection.

Therefore, $| B | \leq | A |$.

We now apply a previous theorem which states that

$$\text{if } | A | \leq | B | \text{ and } | B | \leq | A | \text{ then } | A | = | B |.$$

Hence, there must be a bijection from A to B.

(Note that we could have chosen g(x) = x/2 and obtained a bijection directly).

Q. E. D.

- ***Nonconstructive*** existence proof.

  - Assume no c exists which makes P(c) true and derive a contradiction.

Example:

Theorem: *There exists an irrational number*.

Proof:

Assume there doesn't exist an irrational number.

Then all numbers must be rational.

Then the set of all numbers must be countable.

Then the real numbers in the interval [0, 1] is a countable set.

But we have already shown this set is not countable.

Hence, we have a contradiction (The set [0,1] is countable and not countable).

Therefore, there must exist an irrational number.

Q. E. D.

Note: we have not produced such a number!

• Disproof by ***Counterexample***:

Recall that $\; x\neg P(x) \leftrightarrow \neg \; xP(x)$.

To establish that $\neg \; xP(x)$ is true (or $\; xP(x)$ is false) construct a c such that $\neg P(c)$ is true or P(c) is false.

In this case c is called a *counterexample* to the assertion $\; xP(x)$

Nonexistence Proofs

We wish to establish the truth of

$\neg \; xP(x)$ (which is equivalent to $\; x\neg P(x)$)**.**

Use a proof by contradiction by assuming there is a c which makes P(c) true.

Universally Quantified Assertions

We wish to establish the truth of

$$xP(x).$$

We assume that x is an arbitrary member of the universe and show P(x) must be true. Using UG it follows that $xP(x)$.

Example:

Theorem: *For the universe of integers, x is even iff x^2 is even.*

Proof: The quantified assertion is

$$x[x \text{ is even } \leftrightarrow x^2 \text{ is even}]$$

We assume x is arbitrary.

Recall that $P \leftrightarrow Q$ is equivalent to $(P \rightarrow Q) \quad (Q \rightarrow P)$.

<u>Case 1.</u> We show if x is even then x^2 is even using a direct proof (the *only if* part or *necessity*).

If x is even then x = 2k for some integer k.

Hence, $x^2 = 4k^2 = 2(2k^2)$ which is even since it is an integer which is divisible by 2.

This completes the proof of case 1.

Case 2. We show that if x^2 is even then x must be even (the *if* part or *sufficiency*) .

We use an indirect proof:

Assume x is not even and show x^2 is not even.

If x is not even then it must be odd.

So, $x = 2k + 1$ for some k.

Then

$$x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

which is odd and hence not even.

This completes the proof of the second case.

Therefore we have shown x is even iff x^2 is even.

Since x was arbitrary, the result follows by UG.

Q.E.D.

Dear students: Learning how to construct proofs is probably one of the most difficult things you will face in life. Few of us are gifted enough to do it with ease. One only learns how to do it by practicing.

