Discrete Mathematics
Proof Methods and Strategy

Exhaustive Proof

Some theorems can be proven by examining a relatively small number of examples. Such proofs are called exhaustive proofs (we just exhaust all the possibilities).

Example: Prove that there are NO positive perfect cubes less than 1000 that are the sum of the cubes of two positive integers.

$1^3 = 1$ $\quad 6^3 = 216$ $\quad \_\_ \neq \_\_^3 + \_\_^3$

$2^3 = 8$ $\quad 7^3 = 343$

$3^3 = 27$ $\quad 8^3 = 512$

$4^3 = 64$ $\quad 9^3 = 729$

$5^3 = 125$

$9 + 8 + \dots + 1 = 45$ possibilities

Peoples can carry out exhaustive proofs only when it is necessary to check only a relatively small number of instances of a statement. Computers do better, but still there are limitations.

Proof by Cases

A proof by cases must cover all possible cases that arise in a theorem.

Example: Use a proof by cases to show that $min(a, min(b, c)) = min(min(a, b), c)$, whenever a, b, and c are real numbers.

$a = 3 \quad b = \pi \quad c = 7$

$min(3, min(\pi, 7)) = min(min(3, \pi), 7)$

$3 = 3$

Proof:

Case 1: a is the smallest or tied for the smallest

$a \leq min(b, c)$

$LHS = a \quad RHS = a$

Case 2: b is the smallest or tied for the smallest

$LHS = b \quad RHS = b$

Case 3: c is the smallest or tied for the smallest

$c \leq min(a, b)$

$LHS = c \quad RHS = c$

QED.

Common errors with exhaustive proofs and proofs by cases

We must consider all possible cases. No matter how many examples are considered, a theorem is NOT proved unless every possible example is covered.

Example: Conjecture: "If x is a real number, then x^2 is a positive real number."

Proof by cases (???):

Case 1: Let x be a positive real number. Then x^2 is positive since positive times positive is positive.

Case 2: Let x be a negative real number. Then x^2 is positive since negative times negative is positive.

Mistake: $x = 0$ has not been considered!

$0^2 = 0$ not positive!

Existence Proofs

Definition: A proof of a proposition of the form $\exists x P(x)$ is called an existence proof.

There are two types of existence proofs.

1. **Constructive**
   The proof is given by finding an element such that $P(a)$ is true.

2. **Nonconstructive**
   Someone shows that an element a such that $P(a)$ is true must exist but does not tell us what that element is.
   One method that could be used here is a proof by contradiction. We show that the negation of an existence quantifier implies a contradiction.

Example: Prove that there is a positive integer that can be written as the sum of squares of positive integers in two different ways.

Constructive proof:

$$50 = 5^2 + 5^2$$
$$50 = 1^2 + 7^2$$

QED.

Example: Theorem: Let $1, 2, \dots, n$ be natural numbers and k be their arithmetic mean (average), $k = \frac{1+2+\dots+n}{n}$. There exists a number m (among $1, 2, \dots n$) such that $m \geq k$.

Nonconstructive existence proof by contradiction:

Assume that the statement is not true.

Then all numbers $1, 2, 3, \dots, n$ are strictly less than k.

$$\underbrace{1+2+3+\dots+n} < k \cdot n = \frac{1+2+\dots+n}{\cancel{n}} \cdot \cancel{n}$$

$$= \underbrace{1+2+\dots+n}$$

Contradiction!

QED

Uniqueness Proofs

Some theorems assert the existence of a unique element with a particular property. In other words, these theorems assert there is exactly one element with this property.

To prove a statement of this type we need to show that an element with this property exists and no other element has this property.

The two parts of a uniqueness proof are:

1. ***Existence:*** We show that an element with a desired property exists.
2. ***Uniqueness:*** We show that if x and y both have the desired property, then $x = y$.

Example: Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Proof:

1. ***Existence***

Note $r = -\frac{b}{a}$

Since $a \neq 0$, r must exist.

2. ***Uniqueness***

Suppose s is a real number such that $as + b = 0$.

Then $ar + b = as + b$

$ar = as$

$r = s$

This establishes the uniqueness part.

QED.