Basic Proof Technique

Charles Aunkan Gomes
Lecturer, Dept. of CSE
United International University
charles@cse.uiu.ac.bd

Proof Terminology

- Theorem: statement that can be shown to be true
- Proof: A valid argument that establishes the truth of a theorem
- Axioms: Statements we assume to be true
- Lemma: A less important theorem that is helpful in the proof of other results
- Corollary: Theorem that can be established directly from a theorem that has been proved
- Conjecture: Statement that is being proposed to be a true statement

Standard forms of different numbers

Type	Standard Form
Even number	$2k$, where k is an integer
Odd number	$2k + 1$ or $2k - 1$, where k is an integer
Multiple of k	kn, where n is an integer
Division by k gives remainder r	$kn + r$, where n is an integer
Perfect square	k^2, where k is an integer
Rational number	$\frac{p}{q}$, where p, q are integers and $q \neq 0$ (Sometimes also assume p, q do not have any common factors other than 1)
Irrational number	NO STANDARD FORM

Vacuous Proof

If we prove a conditional statement by disproving its hypothesis, then the proof technique is called vacuous proof

Example: Prove that P(0) true, where, $P(n) \equiv (n>1) \rightarrow (n^2>n)$

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Trivial Proof

If we prove a conditional statement by proving its conclusion, then the proof technique is called trivial proof.

Example: Prove that P(0) true, where $P(n) \equiv \forall a \forall b((a \geq b) \rightarrow (a^n \geq b^n))$

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Proof Techniques

Three basic techniques:

- Direct proof
- Proof by contradiction
- Proof by contraposition

Direct Proof

A direct proof is a logical argument where you start with the given assumptions (or premises) and apply a series of deductive steps to arrive at the conclusion.

- First step is a premise
- Subsequent steps use rules of inference or other premises
- Last step proves the conclusion

Direct Proof

A direct proof of a conditional statement $p \rightarrow q$

First assumes that p is true, and uses axioms, definitions, previously proved theorems, with rules of inference, to show that q is also true. The above targets to show that the case where p is true and q is false never occurs

Thus, $p \rightarrow q$ is always true.

Direct Proof (Example)

- Give a direct proof of the theorem "If n is an even integer, then n^2 is even."

Assume that n is an even integer. This implies that there is some integer k such that, $n = 2k$

Then,

$n^2 = (2k)^2$

$= 4k^2$

$= 2(2k^2)$

Since n^2 can be written as 2 times of an integer which is even, it follows that n^2 is even. [proved]

Direct Proof (Example)

- Give a direct proof that if *m* and *n* are both perfect squares, then *mn* is also a perfect square.(A perfect square is the square of an integer*)*

Assume that m and n are both squares. This implies that there are integers u and v such that,

$$m = u^2 \text{ and } n = v^2.$$

Then,

$mn = u^2 v^2$

$= (uv)^2$

Notice that $(uv)^2$ is the square of the integer $u \cdot v$.

Thus, mn is a perfect square.$_{\text{[proved]}}$

Direct Proof (Example)

- Prove that the product of two rational numbers is rational

Note: A real number r is rational if there exist integers p and q with $q \neq 0$ such that $r = p / q$ .A real number that is not rational is called irrational.

Prove that the product of two rational numbers is rational

Assume a and b are rational numbers. By definition of rational numbers, there exist integers p,q,r,s with $q \neq 0$and $s \neq 0$ such that:

Then, $\frac{p}{q}$ and $\frac{r}{s}$

$$ab = \frac{p}{q} \cdot \frac{r}{s}$$

$$= \frac{p.\ r}{q.\ s}$$

Notice that p . r and q. s are both integers because the product of integers is an integer.

Also, $q \,.\, s \neq 0$ because neither q nor s is zero.

Therefore, (p,r)/(q.s) is in the form

integer/ nonzero integer , which is the definition of a rational number.

Thus, the product of two rational numbers is rational$_{\text{[proved]}}$

Proof by Contraposition

- To prove $p \rightarrow q$, we first assume that $\neg q$ is true, and hence prove that $\neg p$ is true

- We actually prove the contrapositive of the actual sentence, i.e. $\neg q \rightarrow \neg p$

- Why? Sometimes, it may be easier to directly prove $\neg q \rightarrow \neg p$ than $p \rightarrow q$

Proof by Contraposition(example)

- Prove that if n is an integer and n^2 is odd, then n is odd.

P: n^2 is odd

Q:n is odd

¬P: n^2 is even

¬Q: n is even

Prove by contraposition that if n is an integer and n^2 is odd, then n is odd

We have to proof is if n^2 is odd, then n is odd.

Suppose,

p= n^2 is odd and q= n is odd

n^2 is odd → n is odd

∴ $p \rightarrow q$

Contapositive of the original statement is, $\neg q \rightarrow \neg p$

≡ ¬(n is odd) → ¬(n^2 is odd)

≡ n is even → n^2 is even

If n is even, we can say n=2k

Then,

$n^2 = (2k)^2$

$= 4k^2$

$= 2(2k^2)$

Since n^2 can be written as 2 times an integeris even, it follows that n^2 is even.

Since the contrapositive is true, the original statement is also true. Thus, we have proved that **if n is an integer and n^2 is odd, then n is odd**$_{\text{[proved]}}$

Proof by contraposition(Example)

If $3n + 2$ is an odd integer, then n is odd.

Suppose,

p= $3n + 2$ is odd and q= n is odd

$3n + 2$ is odd → n is odd

∴ $p \to q$

Contapositive of the original statement is, $\neg q \to \neg p$

≡ ¬(n is odd) → ¬($3n + 2$ is odd)

≡ n is even → $3n + 2$ is even

If n is even, we can say $n=2k$

Then,

$3n + 2 = 3(2k) + 2$

$= 6k+2$

$= 2(3k+1)$

Since $3n + 2$ can be written as 2 times an integeris even, it follows that $3n + 2$ is even.

Since the contrapositive is true, the original statement is also true. Thus, we have proved that **if $3n + 2$ is an odd integer, then n is odd**[proved]

Proof by Contradiction

Proof by contradiction is a logical method used to prove a statement by assuming the opposite (negation) of the statement is true and then demonstrating that this assumption leads to a contradiction. Since a contradiction indicates that the assumption must be false, the original statement is therefore proven to be true.

For statements of the form "if (p), then (q)":

- Assume p is true and q is false ($\neg q$).
- Show that assuming $\neg q$ leads to a situation where p cannot be true.
- This creates a contradiction since we started by assuming p is true.
- Therefore, our assumption that p is true and q is false must be incorrect.
- Consequently, when p is true, q must also be true.

Proof by contradiction that if 3n + 2 is even, then *n* is even

Give a proof by contradiction of the theorem "If 3n + 2 is even, then n is even."

Given, (3n+2) is even. We assume that n is not even, that is n is odd. If n is odd, there is some integer k such that, n=2k+1.

Then, 3n+2 = (3(2k+1)+2)=6k+3+2 = 6k+5

Since 6k is obviously even (because 6 is even and any integer multiplied by an even number is even), adding 5 (an odd number) to an even number results in an odd number.

Thus 3n+2 turned out to be odd. This contradicts our assumption that 3n+2 is even.

Since assuming that n is odd leads to a contradiction, our initial assumption must be incorrect.

Therefore,n must be even when 3n+2 is even.[proved]

Prove by contradiction that √2 is irrational

Assume that √2 is irrational is false. That means, assume that √2 is rational. So √2 can be expressed as $\frac{p}{q}$, where p, q are integers and $q \neq 0$

(Sometimes also assume p, q do not have any common factors other than 1)

$\sqrt{2} = \frac{p}{q}$

$\equiv 2 = \frac{p^2}{q^2}$

$\equiv p^2 = 2q^2$

$2q^2$ is even, which means p^2 is even, so p must be even.

Hence, p=2k

$\equiv p^2 = (2k)^2 = 4k^2$

$\equiv 2q^2 = 4k^2$

$\equiv q^2 = 2k^2$

$2k^2$ is even, which means q^2 is even, so q must be even.

We have now concluded that both p and q are even, so they have a common factor of 2. Since our assumption that √2 is rational leads to a contradiction, we must conclude that √2 is irrational.[proved]


THANK YOU