INTRODUCTION TO PROOF

Theorem : A statement that can be shown to be true

Axioms : Statements that we assume to be true

Lemma : A less important theorem that is helpful in the proof of other results

Corrolary: It is a theorem that can be established directly from a proven theorem.

Conjecture ; Conjecture is a statement that is proposed as true statement, usually on the basis of some partial evidence.

↓

A heuristic argument.

⊞ When a conjecture is proved, it becomes a theorem.

⊞ Role of thumb:

To prove a universal statement, it must be shown that it works for all cases

To disprove a universal statement, one counter example is enough.

MATHEMATICAL PROOFS ...

Direct Proof :

Direct proof is a mathematical argument that uses rules of inference to draw conclusion out of the premises.

Let's consider Disjunctive syllogism

$$\begin{array}{ll} p \vee q & \text{Premise 1} \\ \neg p & \text{Premise 2} \\ \hline \therefore q & \end{array}$$

We can use direct proof method, that is, a chain of inferences,

$$\begin{array}{ll} p \vee q & \text{Premise} \\ q \vee p & \text{Commutivity of } \vee \\ \neg(\neg q) \vee p & \text{Double negation Law} \\ \neg q \rightarrow p & A \rightarrow B \equiv \neg A \vee B \\ \neg p & \text{Premise 2} \\ \neg\neg q & \text{Modus Tollens} \\ \hline q & \text{Conclusion} \end{array}$$

Generally, when we want to prove a conditional statement $p \rightarrow q$, we assume "p" as true and follow implications to show that q is true as well.

$\downarrow$ Direct proof

We need to find the propositions that obtain q as the conclusion.

Prove: Given m is even and n is odd, their sum (m+n) is always odd.

By definition of odd and even:

If there's an integer j, then

odd "n" = $2j+1$
even "m" = $2K$

Their sum,

$$m+n = (2j+1) + 2K$$
$$= 2\underbrace{(j+K)}_{\text{an integer}} + 1$$

So, $(j+K)$ is an integer. Thus, m+n is odd by definition.

This is direct proof.

Comments on direct proofs:

In direct proofs –
- We start with hypothesis
- Continue with a sequence of ~~deductions~~

↓ end with

Conclusion

However, this may not be true always. We may reach to dead ends if direct methods are followed.

*n is an even integer, n^2 is even

say, $n = 2K$. Then,

$n^2 = 4K^2$

$\Rightarrow n^2 = 2.(2K^2)$

$= 2.$ integer

$\equiv$ even

Proved

We need indirect methods that do not start with hypothesis.

INDIRECT METHODS

Contrapositive:

" If it is $\overset{p}{\text{hartal}}$ today,
then I do $\underset{q}{\text{not}}$ go to class"

$\Big\downarrow$ Contrapositive

" If I $\overset{\neg q}{\text{go to class}}$, then
it is not $\underset{\neg p}{\text{hartal}}$ today "

Converse:

" If I do not go to class, then it is hartal today "

Not true; fallacy of the converse.

Given, 'n' is an integer and 3n+2 odd, then "n" is odd.

Direct Proof:

$$3n+2 = 2K+1$$

$$\Rightarrow 3n = 2K-1$$

what's next?

No direct way to proceed further

Indirect Method: Proof by contraposition

So, according to contraposition theorem

we assume n is even

$\Big\downarrow$ and we show

$3n+2$ is even

So, $n = 2K$, for some integer "K"

$$3n+2 = 3.2K+2 = 2\underbrace{(3K+1)}_{\text{this is another integer}}$$

$$\equiv \text{even}$$

Proof by contraposition continues ...

Because the negation of the conclusion is false and it implies that the hypothesis false, therefore the original conditional statement is true.

Another example

Assume $x \in \mathbb{Z}$. Prove that if $\underbrace{x^2 - 6x + 5 \text{ is even}}_{p}$, then $\underbrace{x \text{ is odd}}_{q}$.

Let's consider

$x = 2a$ for any integer "a"

↳ We start with $\neg q$; contraposition ↳ even.

So, we obtain,

$$
\begin{aligned}
x^2 - 6x + 5 &= (2a)^2 - 6 \cdot 2a + 5 \\
&= 4a^2 - 12a + 5 \\
&= 4a^2 - 12a + 4 + 1 \\
&= 2(2a^2 - 6a + 2) + 1 \\
&= 2k + 1 \\
&\equiv \text{odd}
\end{aligned}
$$

So, we started with $\neg q$ and we show that $x^2 - 6x + 5$ is odd; that is $\neg p$.

That's, we prove that $x^2 - 6x + 5$ is odd.

Proof by contradiction

In this proof method, we assume that the statement made is not true.

$\downarrow$ then

We derive a contradiction

Example

Prove that $\sqrt{2}$ is irrational.

we assume rational

Let's assume $\sqrt{2}$ is rational

$\downarrow$ implies, $\sqrt{2}$ can be written as

m/n, where m, n are integers

$\downarrow$

$m^2/n^2 = 2 \Rightarrow m^2 = 2n^2 \Rightarrow m^2$ is even

$\Rightarrow m$ is even

$\Rightarrow m = 2K$.

Now,

$(2K)^2 = 2n^2$

$\Rightarrow 2n^2 = 4K^2$

$\Rightarrow n^2 = 2K^2 \Rightarrow$ n is also even.

Thus,

- m and n are both even and they have a common factor 2.

- This contradicts the assumption that m/n was in lowest terms

  ↳ Not in lowest term

So, by contradiction, it can be concluded that $\sqrt{2}$ is irrational.

Proof by cases

$$
\begin{array}{lll}
 & p \rightarrow r & \text{Premise 1} \\
 & q \rightarrow r & \text{Premise 2} \\
 & p \vee q & \text{Premise 3} \\
\hline
\therefore & r & \text{conclusion}
\end{array}
$$

Example:

Given x is an integer
x^2+x is even

Set-up for proof-by-cases:

Let's assume p: x is even | r: x^2+x is even
q: x is odd |

Verify Premise 1: if x is even, $x = 2n$

$$
\begin{aligned}
x^2+x &= (2n)^2+2n \\
&= 4n^2+2n \\
&= (2n)2+2n
\end{aligned}
$$

↳ which is even

Verify Premise 2: if x is odd $x = 2n+1$

$$
\begin{aligned}
x^2+x &= (2n+1)^2+2n+1 \\
&= (4n^2+4n+1)+2n+1 \\
&= 4n^2+6n+2
\end{aligned}
$$

↳ even

Verify Premise 3: An arbitrary integer is either even or odd.

So, the conclusion is proved.

Mistakes in Proof

$\Rightarrow a = b$ Given

$\Rightarrow a^2 = ab$ Multiplied by a

$\Rightarrow a^2 - b^2 = ab - b^2$ subtract b^2

$\Rightarrow (a-b)(a+b) = b(a-b)$

$\Rightarrow (a-b)(a+b) = b(a-b)$ Mistake is here; divide by $(a-b)$

$\Rightarrow a + b = b$

$\Rightarrow 2b = b$ Replace a by b as $a = b$

$\Rightarrow 2 = 1$

Where's the mistake?

Proof by cases: another example

Let n be an integer. show that if n is not divisible by 3, then $n^2 = 3k+1$ for some integer k

Case 1: Assume $n = 3m+1$. So, $n^2 = (3m+1)^2 = 9m^2+6m+1 = 3(3m^2+2m)+1$

Not divisible by 3

$= \underbrace{3(3m^2+2m)}_{\text{integer}}+1 = 3k+1$

Case 2: $n = 3m+2$. So, $n^2 = (3m+2)^2 = 9m^2+12m+4$

$= 9m^2+12m+3+1$

$= 3\underbrace{(3m^2+4m+1)}_{\text{integer } k}+1$

$= 3k+1$, which is not divisible by 3

So, Case I and Case II reflect all possible possibilities. Thus, proved.

Proofs of Equivalence

To prove a theorem that is a biconditional statement, that is, statement of the form $p \leftrightarrow q$

we show that

$p \rightarrow q$ and $q \rightarrow p$ are true

This approach is based on :

$$(p \leftrightarrow q) \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$$

is the tautology.

For example: Given a theorem

If n is a positive integer, then n is odd if and only if n^2 is odd

To prove this, we must show that

$p \rightarrow q$, $q \rightarrow p$

where,

p: "n is odd"

q: "n^2 is odd"

NORMAL FORM

A product of the variables and their negations in a formula is called an elementary product.

$\neg p \wedge q$, $q \wedge r$ are example of elementary products.

A sum of variables and their negations is called an elementary sum.

$\neg p \vee q$, $q \vee p \vee s$ are examples of elementary sum

Elementary sum is the disjunction of literals.

Elementary product is the conjunction of literals.

Observation:

Necessary condition for an elementary product to be identically false is to have at least one pair of literals where one(p) is the negation ($\neg p$) to generate the others.

$$\underbrace{p \wedge \neg p}_{F} \wedge \dots \dots \wedge q \dots \equiv F$$

For elementary sum,

it becomes a tautology if one pair exists where one is the negation of other.

$$\underbrace{P \vee \neg P}_{T} \vee \ldots \quad \ldots \quad \ldots \equiv T$$

Disjunctive Normal Form:

It is the formula which is similar to, the original formula, But it consists of a sum of elementary product.

To translate any formula to disjunctive normal form — Replace $\rightarrow$ and $\leftrightarrow$ using $\wedge$, $\vee$, and $\neg$

Example: $(P \rightarrow q) \wedge \neg q$ obtain DNF

$$\equiv (\neg P \vee q) \wedge \neg q$$

$$\equiv (\neg P \wedge \neg q) \vee (q \wedge \neg q)$$

Conjunctive Normal Form:

A formula which is equivalent to a given formula and consists of a product of elementary sums is called conjunctive normal form. CNF

Example: $(P \rightarrow q) \wedge \neg q$

$$\equiv (\neg P \vee q) \wedge \neg q \equiv \text{CNF}$$

CNF continues...

- We can bring any formula to normal form
- Conjunctive normal form is unique.

Example of CNF

$$(p \to q) \leftrightarrow (p \to r)$$

$$\equiv \left[(p\to q) \to (p \to r)\right] \wedge \left[(p \to r) \to (p \to q)\right]$$

$$\equiv \left[\neg(p \to q) \vee (p \to r)\right] \wedge \left[\neg(p \to r) \vee (p \to q)\right]$$

$$\equiv \left[\neg(\neg p \vee q) \vee (\neg p \vee r)\right] \wedge \left[\neg(\neg p \vee r) \vee (\neg p \vee q)\right]$$

$$\equiv \left[(p \wedge \neg q) \vee (\neg p \vee r)\right] \wedge \left[(p \wedge \neg r) \vee (\neg p \vee q)\right]$$

$$\equiv \left[(p \wedge \neg q) \vee \neg p \vee r\right] \wedge \left[(p \wedge \neg r) \vee (\neg p) \vee q\right]$$

$$\equiv \left[(p \vee \neg p) \wedge (\neg q \vee \neg p) \vee r\right] \wedge \left[\left((p \vee \neg p) \wedge (\neg r \vee \neg p)\right) \vee q\right]$$

$$\equiv (\neg q \vee \neg p \vee r) \wedge (\neg r \vee \neg p \vee q)$$