- Using truth table to show an argument is valid is not always feasible.

  e.g. if the argument ~~has~~ form has 10 different propositional variables, truth table requires 2^{10} rows.

- Instead, we use rules of inference which are some relatively simple argument forms.

  provides a systematic way of showing statements are equivalent to each other.

- We first establish validity of these rules of inference ~~rules~~ which can be used as building blocks to construct more complicated valid argument form

Rules of Inference	Tautology	Name
1. p, $p \to q$, $\therefore q$	$[p \land (p \to q)] \to q$	Modus Ponens
2. $\neg q$, $p \to q$, $\therefore \neg p$	$[\neg q \land (p \to q)] \to \neg p$	Modus Tollens
3. $p \to q$, $q \to r$, $\therefore p \to r$	$[(p \to q) \land (q \to r)] \to (p \to r)$	Hypothetical Syllogism
4. $p \lor q$, $\neg p$, $\therefore q$	$[(p \lor q) \land \neg p] \to q$	Disjunctive syllogism.
5. p, $\therefore p \lor q$	$p \to (p \lor q)$	Addition.

Rules of Inference	Tautology	Name
6. $\dfrac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification
7. $\dfrac{\begin{array}{c} p \\ q \end{array}}{\therefore p \wedge q}$	$[(p) \wedge (q)] \rightarrow p \wedge q$	Conjunction
8. $\dfrac{\begin{array}{c} p \vee q \\ \neg p \vee r \end{array}}{\therefore q \vee r}$	$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	Resoluti

proof using truth table
proof using identity.

---

① **Modus Ponens** (latin for "mode that affirms") or "the way that affirms by affirming

$$\begin{array}{ll} p \rightarrow q & \text{Major premise} \\ p & \text{Minor premise} \\ \hline \therefore q & \text{Conclusion.} \end{array}$$

Example: Given the major premise
"If $\underbrace{\text{I step in poison ivy}}_{p}$, then $\underbrace{\text{I will have a rash.}}_{q}$"

and the minor premise
" $\underbrace{\text{I step in poison ivy.}}_{p}$ "

What is the conclusion by modus ponens.

Soln Rewrite this argument in symbolic form

$$\begin{array}{c} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

So the conclusion by modus ponens is "I will have a rash".

Theorem Modus ponens

$[(p \to q) \wedge p] \to q$ ~~$\Leftrightarrow T$~~ is a tautology.

prof-1

p	q	$p \to q$	$(p \to q) \wedge p$	$[(p \to q) \wedge p] \to q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

prof-2

$p \to q \Leftrightarrow \neg p \vee q$

$[(p \to q) \wedge p] \to q$

$\Leftrightarrow [(\neg p \vee q) \wedge p] \to q$ (Implication law)

$\Leftrightarrow [p \wedge (\neg p \vee q)] \to q$ (Commutative law)

$\Leftrightarrow (p \wedge \neg p) \vee (p \wedge q) \to q$ (Distributive law)

$\Leftrightarrow F \vee (p \wedge q) \to q$ (contradiction)

$\Leftrightarrow p \wedge q \to q$ (identity)

$\Leftrightarrow \neg(p \wedge q) \vee q$ (Implication)

$\Leftrightarrow (\neg p \vee \neg q) \vee q$ (De Morgan)

~~$\Leftrightarrow q \vee (\neg p \vee \neg q)$~~

$\Leftrightarrow \neg p \vee (\neg q \vee q)$ (Associativity)

$\Leftrightarrow \neg p \vee T$ (Excluded Middle)

$\Leftrightarrow T$ (Domination).

$\neg[(\neg p \vee q) \wedge p] \vee q$

$= (p \wedge \neg q) \vee \neg p \vee q$

$= [(p \vee \neg p) \wedge (\neg q \vee \neg p)] \vee q$

$= [(p \vee \neg p) \wedge (\neg q \vee \neg p)] \vee q$

$= [T \wedge (\neg q \vee \neg p)] \vee q$

$= \neg q \vee \neg p \vee q$

$= T \vee \neg p$

$= T$

Implication versus Inference

Cory and Richard are taking about their mobile phones, when Richard makes the following (absurd) assertions:

If it ain't broke, don't fix it.
If a person updates their phone, they're stupid.

Cory had updated his phone recently without Richard's knowledge. Cory thinks quickly:

If I update my phone, then I'm stupid.
I have updated my phone

Therefore, I'm stupid.

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$$

Cory exclaims, "I have updated my phone! Are you infering I'm stupid?"

Richard corrects him, "No, no, no, I implied it. You inferred it"

- Implication is to state a logical consequence.
- Inference is a conclusion that is reached based on implications.

Modus Tollens (Latin for "mode that denies" or "the way that denies by denying")

$$\begin{array}{ll} p \to q & \text{Major premise} \\ \neg q & \text{Minor premise} \\ \hline \therefore \neg p & \text{Conclusion.} \end{array}$$

Example: Given the major premise

"If $\underbrace{\text{I step in poison ivy}}_{p}$, then $\underbrace{\text{I will have a rash}}_{q}$".

& the minor premise

"I don't have a rash".

What is the conclusion by modus tollens?

Sol^n. Symbolic form

$$\begin{array}{l} p \to q \\ \neg q \\ \hline \therefore \neg p \end{array}$$

So the conclusion is "I did not step on poison ivy."

Theorem Modus tollens

$[(p \to q) \wedge (\neg q)] \to \neg p$ is a tautology.

proof-I

p	q	$p \to q$	$\neg p$	$\neg q$	$[(p\to q)\wedge \neg q]$	$[(p\to q)\wedge \neg q] \to \neg p$
T	T	T	F	F	F	T
T	F	F	F	T	F	T
F	T	T	T	F	F	T
F	F	T	T	T	T	T

proof - II Using elementary rules of inference.

$$((p \to q) \land \neg q) \to \neg p.$$

$\Leftrightarrow [(\neg p \lor q) \land (\neg q)] \to \neg p.$ (Implication)

$\Leftrightarrow [(\neg q) \land (\neg p \lor q)] \to \neg p$ (Commutation)

$\Leftrightarrow [(\neg q \land \neg p) \lor (\neg q \land q)] \to \neg p$ (distributive)

$\Leftrightarrow \neg(q \lor p) \lor F \to \neg p$ (De Morgan, contradiction)

$\Leftrightarrow \neg(q \lor p) \to \neg p$ (Identity)

$\cancel{\Leftrightarrow \neg(\neg p) \Leftarrow}$

$\Leftrightarrow \neg(\neg(q \lor p)) \lor (\neg p)$ (Implication)

$\Leftrightarrow q \lor p \lor (\neg p).$ (Double negation)

$\Leftrightarrow q \lor (p \lor \neg p)$ (Associative)

$\Leftrightarrow q \lor T$ (Excluded middle)

$\Leftrightarrow T$ (Domination)

$\neg[(\neg p \lor q) \land \neg q] \lor (\neg p)$

$\Leftrightarrow (p \land \neg q) \lor q \lor (\neg p)$

$\Leftrightarrow (p \lor q) \land \underbrace{(\neg q \lor q)}_{T} \lor (\neg p)$

$\Leftrightarrow (p \lor q) \lor \neg p.$

$\Leftrightarrow T \lor q$

$\Leftrightarrow T.$

F^{p} p^{T}

think Table

Fas

$T \lor p \Leftrightarrow T$

$F \lor p \Leftrightarrow p$

$T \land p \Leftrightarrow p$

$F \land p \Leftrightarrow F$

<u>Example:</u> Determine whether the following argument is valid:

$$\begin{array}{l} p \vee (\neg q) \\ q \\ \hline \therefore \neg p \end{array}$$

Major premise

Minor premise

Conclusion.

$p \to q \Leftrightarrow \neg p \vee q$

$p \vee (\neg q) \Leftrightarrow (\neg q) \vee p$
$\Leftrightarrow q \to p.$

$$\begin{array}{l} q \to p \\ q \\ \hline \therefore \neg p \end{array}$$

but by modus ponens, conclusion should be p
So the argument is invalid.

<u>Example:</u>

"If $\sqrt{2} > \frac{3}{2}$, then $(\sqrt{2})^2 > \left(\frac{3}{2}\right)^2$. We know $\sqrt{2} > \frac{3}{2}$.
Consequently, $(\sqrt{2})^2 = 2 > \left(\frac{3}{2}\right)^2 = \frac{9}{4}$".

Determine whether the above argument is valid & determine whether its conclusion must be true because of the validity of the argument.

<u>Soln.</u> Let p be "$\sqrt{2} > \frac{3}{2}$", q be "$(\sqrt{2})^2 > \left(\frac{3}{2}\right)^2$"

Then symbolic form ~~of this~~ is:

$2 > \frac{9}{4} = 2.25$

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$$

Major premise

Minor premise

Conclusion

Therefore, valid argument.
but the minor premise p is false
So we cannot conclude ~~that~~ anything about the conclusion ~~is true~~.
however the conclusion is false as $2 \not> \frac{9}{\ldots}$

Syllogism (3 propositions)

1) Hypothetical Syllogism

$$\begin{array}{ll} p \to q & \text{major premise} \\ q \to r & \text{minor premise} \\ \hline \therefore p \to r & \text{Conclusion.} \end{array}$$

Example: Given the premises

"Socrates is a man",

and "All men are mortal",

What is the conclusion by the hypothetical syllogism?

$p(x)$ = x is a man
$M(x) = x$ is mortal.

$$\begin{array}{l} \forall x(p(x) \to M(x)) \\ p(\text{Socrates}) \\ \hline M(\text{Socretes}). \end{array}$$

Sol^n. Argument form

$$\begin{array}{ll} p \to q & \text{Socrates is a man} \\ q \to r & \text{All mean are mortal} \\ \hline \therefore p \to r & \text{Therefore, Socreates is mortal.} \end{array}$$

~~Example: If Mohan is a lawyear~~

Theorem Hypothetical Syllogism

$$[(p \to q) \wedge (q \to r)] \to (p \to r). \Leftrightarrow T.$$

proof

p	q	r	$p \to q$	$q \to r$	$(p\to q)\wedge(q\to r)$	$(p \to r)$	$(p\to q)\wedge(q\to r) \to (p\to r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

Exercise prove the above using only elementary rules ~~for~~ of inference.

Example: "If $\overbrace{\text{you send me an e-mail message}}^{p}$, then $\underbrace{\text{I will finish writing program}}_{q}$"

"If you not send me e-mail message, then $\underbrace{\text{I will go to sleep early}}_{r}$"

"If I go to sleep early, then $\underbrace{\text{I will wake up feeling refreshed}}_{s}$."

"If I do not finish writing the program then I will wake up feeling refreshed"

Show that the above argument is valid.

Soln: Symbolic form

$$\begin{array}{l} p \to q \\ \neg p \to r \\ r \to s \\ \hline \therefore \neg q \to s \end{array}$$

$$\begin{array}{l} \neg q \to \neg p \quad \text{(contraposition)} \\ \neg p \to r \\ \hline \therefore \neg q \to r \quad \text{(Hypothetical syllogism)} \end{array}$$

$$\begin{array}{l} \neg q \to r \\ r \to s \\ \hline \therefore \neg q \to s \quad \text{(desired conclusion)} \quad \text{(Hypothetical syllogism)} \end{array}$$

Hence the argument is valid.

2. Disjunctive Syllogism

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$

Takes a single disjunction & negation of one of the propositions & conclude that the alternate proposition in the disjunction must be true.

Example;

" Socrates is either living (p) or dead (q)"
Socrates is not living"

Therefore, Socrates is dead.

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$

Theorem: Disjunctive syllogism is a tautology

i.e. $[(p \vee q) \wedge (\neg p)] \longrightarrow q \Leftrightarrow T$

proof:- Exercise.

Resolution principle (Another way of proving that an argument is correct).

- literal → a variable or negation of a variable.
- disjunction of literals → sum
- conjunction of literals → product
- clause → disjunction of literals i.e. sum

- let C_1, C_2 be two clauses.
- L_1 in C_1 is a literal
- L_2 in C_2 is a literal & $L_2 = \neg L_1$

delete L_1 and L_2 from C_1 & C_2 respectively & construct the disjunction of the remaining clauses.

→ the ~~resullting~~ resulting clause is a resolvent of C_1 & C_2.

Example:
$$C_1 = P \vee Q \vee R$$
$$C_2 = \neg P \vee \neg S \vee T$$

The resolvent of C_1, C_2 is $Q \vee R \vee \neg S \vee T$

Theorem: Given two clauses, a resolvent C of C_1, C_2 is a logical consequence of C_1 & C_2.
(i.e. if C_1, C_2 true, then C is true)

Example: Modus ponens
$$\begin{array}{c} P \to Q \\ P \\ \hline \therefore Q \end{array}$$

$C_1 : P \to Q \Leftrightarrow \neg P \vee Q$

$C_2 : P$

The resolvent of C_1, C_2 is Q which is a logical consequence of C_1 & C_2.

Example: Modus tollens
$$\begin{array}{c} P \to Q \quad \text{i.e. } \neg P \vee Q \\ \neg Q \\ \hline \neg P \end{array}$$

$C_1 : \neg P \vee Q$

$C_2 : \neg Q$

The resolvent of C_1, C_2 is $\neg P$ which is a logical consequence of C_1 & C_2.

Proof of the Theorem

let $C_1 = L \vee C_1'$, $C_2 = \neg L \vee C_2'$.

Then $C = C_1' \vee C_2'$ is the resolvent of C_1, C_2.

Claim: C is a logical consequence of C_1, C_2
i.e. if C_1, C_2 true, then C is true.

proof of claim

$C_1 = C_1' \vee L$
$C_2 = C_2' \vee \neg L$
$C = C_1' \vee C_2'$

Assume C_1, C_2 true

Either L is true or L is false

- if L true, then $\neg L$ false
  in order that C_2 true, C_2' must be true, so C is true
- if L is false, then in order that C_1 is true, we must
  have C_1' true & hence C is true.

Thus, whenever C_1, C_2 true, C is true

$\Rightarrow$ C is a logical consequence of C_1 & C_2.

The resolution principle

- Given a set S of clauses, a (resolution) deduction of C from S is a finite sequence $C_1, C_2, \ldots, C_k$ of clauses such that each C_i either is a clause in S or a resolvent of clauses preceding C & $C_k = C$.

$$S \xrightarrow{\text{deduction of}} C$$

- A deduction of $\square$ (empty clause) is called a refutation or a proof of S.

Validity check of an argument using resolution principle

- let $P_1, P_2, \ldots, P_n$ be premises & C be the conclusion of an argument.
- put $P_1, P_2, \ldots, P_n$ in clause form & add to it $\neg C$ form
- from this sequence, if $\square$ can be derived, the argum

Example: Modus ponens

$$\begin{array}{l} P \to Q \quad \text{i.e. } \neg P \vee Q. \\ P \\ \hline \therefore Q \end{array}$$

Sequence of Clauses

$C_1 : \neg P \vee Q$

$C_2 : P$

$C_3 : \neg Q$

$C_4 : Q$ (resolution of C_1, C_2).

$C_5 : \square$ (resolution of C_3, C_4).

Hence the argument Modus ponens is correct.

Example: Show that the following argument is correct.

If today is Tuesday, I have a test in Mathematics or Economics, If my Economics Professor is sick, I will not have a test in Economics. Today is Tuesday and my Economics professor is sick. Therefore, I have a test in Mathematics.

Sol^n. Converting to logical notation

denotes
$t \to$ Today is Tuesday
$m \to$ I have a test in Mathematics
$e \to$ I have a test in Economics.
$s \to$ My Economics professor is sick

premises are

$$\begin{array}{l} t \to m \vee e \\ s \to \neg e \\ t \wedge s \\ \hline \end{array}$$

conclusion is $\therefore m$

Putting in clause form

$C_1 : (\neg t) \vee (m \vee e)$

$C_2 : (\neg s) \vee (\neg e)$

$C_3 : t$

$C_4 : s$

$C_5 : \neg m$ (negation of conclusion).

$C_6 : (\neg t) \vee m \vee (\neg s)$ (resolution of C_1, C_2)

$C_7 : m \vee (\neg s)$ (resolution of C_6, C_3)

(resolution of C_7, C_4)

Hence the argument is correct.

Rules of Inference for Quantified Statements

Rules of Inference	Name
1. $\dfrac{\forall x P(x)}{\therefore P(c)}$	Universal instantiation
2. $\dfrac{P(c) \text{ for an arbitrary } c}{\forall x P(x)}$	Universal generalization
3. $\dfrac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$	Existential instantiation
4. $\dfrac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$	Existential generalization

Example: "Everyone in this discrete mathematics class has taken a course in computer science"
"Marla is a Student in this class"

Therefore, Marla has taken a course in Computer Science

Symbolic form

$D(x) \rightarrow x$ has taken DM
$C(x) \rightarrow x$ has taken C

$$\forall x (D(x) \rightarrow C(x))$$
$$D(\text{Marla})$$
$$\overline{\therefore C(\text{Marla})}$$

validity check.

$\forall x (D(x) \rightarrow C(x))$ by Universal Instant

Modus ponens
$D(\text{Marla}) \rightarrow C(\text{Marla})$
$D(\text{Marla})$

Examples Given the premises

"Socrates is a man",

& "All men are mortal",

What is the conclusion? ~~by the~~

Sol^n. **Symbolic form**

$P(x)$ denotes x is a man,

$M(x)$ denotes x is mortal,

domain of discourse consists of all men.

$$\begin{array}{l} P(\text{Socrates}) \\ \forall x\,(P(x) \to M(x)) \\ \hline M(\text{Socrates}). \end{array}$$

i.e. Socrates is ~~a man~~ mortal.

as $\forall x(P(x) \to M(x))$ means $P(\text{Socrates}) \to M(\text{Socrates})$ by Universal instantiation.

$$\begin{array}{l} \forall x\, P(x) \\ \hline P(c) \end{array}$$

Also $P(\text{Socrates})$ by Hypothesis

$\therefore M(\text{Socrates})$ by Modus ponens

i.e. the conclusion of the argument is 'Socrates is mortal'.

Hamming Bird Example:

$\forall x\,(P(x) \to S(x))$

$\neg\, \exists x\,(Q(x) \wedge R(x)) \Leftrightarrow \forall x\,(\neg Q(x) \vee \neg R(x))$

$\forall x\,(\neg R(x) \to \neg S(x))$

$\therefore\ \forall x\,(P(x) \to \neg Q(x))$

negation of conclusion:

$\neg\, \forall x\,(P(x) \to \neg Q(x)) \Leftrightarrow \exists x\, \neg\,(P(x) \to \neg Q$

$\Leftrightarrow \exists x\, \neg\,(\neg P(x) \vee \neg Q($

$\Leftrightarrow \exists x\,(P(x) \wedge Q$

C_1: $\forall x\,(P(x) \to S(x))$

C_2: $\forall x\,(\neg Q(x) \vee \neg R(x))$

C_3: $\forall x\,(\neg R(x) \to \neg S(x))$

C_4: $\exists x\,(P(x) \wedge Q(x))$ (negation of conclusion)

C_5: $P(a) \wedge Q(a)$ for some element a in the domain (Existential instantiation from C_4)

C_6: $P(a)$ } simplification from C_5.)

C_7: $Q(a)$ }

C_8: $S(a)$ (Modus ponens from C_1 & C_6)

C_9: $\neg\neg R(a)$ i.e. $R(a)$ (Modus tollens from C_8 & C_3)

C_{10}: $\neg Q(a) \vee \neg R(a)$ (Universal Instantiation from C_2).

C_{11}: $\neg Q(a)$ (Resolution of C_9, C_{10})

C_{12}: $\square$ (Resolution of C_7, C_{11})

Hamming bird example:

$$\forall x\ (P(x) \rightarrow S(x))$$
$$\neg \exists x\ (Q(x) \wedge R(x))$$
$$\forall x\ (\neg R(x) \rightarrow \neg S(x))$$
$$\therefore \forall x\ (P(x) \rightarrow \neg Q(x))$$

C_1: $\forall x\ (P(x) \rightarrow S(x))$ premise

C_2: $P(c) \rightarrow S(c)$ Rule of inference, Universal instantiation

C_3: $\boxed{\neg P(c) \vee S(c)}$ Rule of inference for implication

C_4: $\neg \exists x (Q(x) \wedge R(x))$ premise

C_5: $\forall x\ (\neg Q(x) \vee \neg R(x))$ (negating quantified expression)

C_6: $\boxed{\neg Q(c) \vee \neg R(c)}$ Universal instantiation.

C_7: $\forall x\ (\neg R(x) \rightarrow \neg S(x))$ premise

C_8: $\boxed{\neg R(c) \rightarrow \neg S(c)}$ Universal instantiation.
$R(c) \vee \neg S(c)$

C_9: $\neg \forall x (P(x) \rightarrow \neg Q(x))$ negation of conclusion.

C_{10}: $\exists x\ \neg (P(x) \rightarrow \neg Q(x))$ (negating quantified expression

C_{11}: $\exists x\ \neg(\neg P(x) \vee \neg Q(x))$ DeMorgan

C_{12}: $\exists x\ (P(x) \wedge Q(x))$

C_{13}: $P(c) \wedge Q(c)$

C_{14}: $\boxed{P(c)}$

C_{15}: $\boxed{Q(c)}$

C_{16}: $\boxed{S(c)}$ Resolution of C_3 & C_{14}

C_{17}: $\neg R(c)$ Resolution of C_6 & C_{15}.

C_{18}: $\neg R(c)$ Resolution of C_8 & C_{16}

C_{19}: $\square$ Resolution of C_{17} & C_{18}.

Resolution

$p \vee q$

$\neg p \vee r$

$\therefore\ q \vee r$

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

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

$$\Leftrightarrow [(\neg p \wedge \neg q) \vee q] \vee [(p \wedge \neg r) \vee r]$$

$$\Leftrightarrow [(\neg p \vee q) \wedge \underbrace{(\neg q \vee q)}_{T}] \vee [(p \vee r) \wedge \underbrace{(\neg r \vee r)}_{T}]$$

$$\Leftrightarrow (\neg p \vee q) \vee (p \vee r)$$

$$\Leftrightarrow \underbrace{(\neg p \vee p)}_{T} \vee q \vee r$$

$$\Leftrightarrow \cancel{q \vee r}\ T$$

p T

$T \wedge p = p$

$T \vee p = T$

p	q	r	$p \vee q$	$\neg p$	$\neg p \vee r$	$\overbrace{q \vee r}^{Q}$	$\overbrace{(p \vee q) \wedge (\neg p \vee r)}^{P}$	$P \rightarrow Q$
T	T	T	T	F	T	T	T	T
T	T	F	T	F	F	T	F	T
T	F	T	T	F	T	T	T	T
T	F	F	T	F	F	F	F	T
F	T	T	T	T	T	T	T	T
F	T	F	T	T	T	T	T	T
F	F	T	F	T	T	T	F	T
F	F	F	F	T	T	F	F	T

$\therefore\ (p \vee q) \wedge (\neg p \vee r) \rightarrow q \vee r$ is a tautology.

$$\Leftrightarrow [(\neg p \vee p) \wedge (\neg p \vee \neg r) \wedge (\neg q \vee p) \wedge (\neg q \vee \neg r)] \vee (q \vee r)$$

$$\Leftrightarrow (\underbrace{\neg p \vee p}_{T} \vee q \vee r) \wedge (\neg p \vee \underbrace{\neg r \vee r}_{T} \vee q) \wedge (\underbrace{\neg q \vee q}_{T} \vee p \vee r) \wedge (\underbrace{\neg q \vee q}_{T} \vee \neg r \vee r)$$

$$\Leftrightarrow T \wedge T \wedge T \wedge T \Leftrightarrow T$$

Combining rules of Inference for propositions & quantified Statements.

- Universal modus ponens :

$$\forall x\,(P(x) \rightarrow Q(x))$$
$P(a)$, where a is a particular element in the domain
$$\therefore Q(a).$$

- Universal modus tollens :

$$\forall x\,(P(x) \rightarrow Q(x))$$
$\neg Q(a)$, where a is a particular element in the domain
$$\therefore \neg P(a).$$

Example: Assume that

"For all positive integers n, if n is greater than 4, then n^2 is less than 2^n."

is true. Use universal modus ponens to show that $100^2 < 2^{100}$.

Soln. Let $P(n)$ denotes "$n > 4$"

$Q(n)$ denotes "$n^2 < 2^n$"

$\forall n\,(P(n) \rightarrow Q(n))$, domain consists of all +ve integers.

$\forall n\,(P(n) \rightarrow Q(n))$, $P(100)$ are both true

Therefore, by modus ponens, $Q(100)$ must be true

Hence $100^2 < 2^{100}$.

Falacy: A fallacy is an argument that has an inherent flaw in the structure of the argument itself which renders the argument invalid.

Types of falacies (3 non sequiturs → latin for "it does not follow").

(i) Affirming the Disjunction →

$$\begin{array}{ll} p \vee q & \text{major premise} \\ p & \text{minor premise} \\ \hline \therefore \neg q & \text{Conclusion} \end{array}$$

(ii) Affirming the Consequent →

$$\begin{array}{ll} p \to q & \text{major premise} \\ q & \text{minor premise} \\ \hline \therefore p & \text{Conclusion.} \end{array}$$

(iii) Denying the Antecedent →

$$\begin{array}{ll} p \to q & \text{major premise} \\ \neg p & \text{minor premise} \\ \hline \therefore \neg q & \text{Conclusion.} \end{array}$$

Theorem.
None of the above arguments are valid.

proof (Exercise).

Example: (Affirming the disjunction)

I'm either going to listen to music or read a book.
I'll listen to music.

Therefore, I cannot read my book.

logical notation

$m \to$ listen to music
$b \to$ read a book

$$\begin{array}{l} m \vee b \\ m \\ \hline \neg b \end{array}$$

~~afirming~~ afirming disjunction ← m

m	b	$\neg b$	$m \vee b$	$(m \vee b) \wedge m$	$(m \vee b) \wedge m \to \neg b$
T	T	F	T	T	F
T	F	T	T	T	T
F	T	F	T	F	T
F	F	T	F	F	T

The argument is invalid, as it is possible to listen to music & read a book at the same time.

~~So you ... listen to music, but it does not preclude that~~

So you can read a book & it does not preclude the possibility of listening to music.

Example: (Affirming the consequent).
/fallacy of the converse

(Politician's syllogism)

If things are to improve, then things must change.
We are changing things.

Therefore, we are improving things.

Symbolic form

$i \to$ things are improving
$c \to$ things change.

$$\begin{array}{c} i \to c \\ c \\ \hline i \end{array}$$

i	c	$i \to c$	$(i \to c) \wedge c$	$((i \to c) \wedge c) \to i$
T	T	T	T	T
T	F	F	F	T
F	T	T	T	F
F	F	T	F	T

Thus the argument is affirming the consequent, hence invalid.

Example (Denying the antecedent).
(We cannot be Machines, Turing)

If each man had a definite set of rules of conduct by which ~~to~~ he regulated his life, ~~then~~ he would be no better than a machine.

But there are no such rules, so men cannot be machines.

Symbolically, this can be represented as follows:

$r \to$ each man has a definite set of rules of conduct by which he regulated his life.

$m \to$ man is machine.

$r \to m$		Major premise
$\neg r$		Minor premise
$\therefore \neg m$		Conclusion.

r	m	$\neg m$	$r \to m$	$\neg r$	$(r \to m) \wedge \neg r$	$[(r \to m) \wedge \neg r] \to \neg m$
T	T	F	T	F	F	T
T	F	T	F	F	F	T
F	T	F	T	T	T	F
F	F	T	T	T	T	T

Argument invalid by denying the antecedent.

i.e. A man ~~can~~ could still be a machine, while does not follow a definite set of rules.

<u>Example</u> (Other type of fallacy).

Convert the following argument into symbolic form, and determine if the following argument is valid or a fallacy:

Coffee is energy. Premise

Kerosene is energy. Premise.

Therefore, Kerosene is coffee. Conclusion.

$c_1: \neg c \vee e$

$c_2: \neg k \vee e$

$c_3: \neg(\neg k \vee c)$

$\therefore k \wedge \neg c$

$c_4: k$

$c_6: e$

$c_7: e$

Soln <u>Symbolic form</u>

$c \to e$

$k \to e$

$\overline{k \to c}$

c denotes coffee

e denotes energy

k denotes kerosene

c	e	k	$k\to c$	$c\to e$	$k\to e$	$(c\to e)\wedge(k\to e)$	$[(c\to e)\wedge(k\to e)]\to(k\to c$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	T	T
T	F	T	T	F	F	F	T
T	F	F	T	F	T	F	T
F	T	T	F	T	T	T	F
F	T	F	T	T	T	T	T
F	F	T	F	T	F	F	T
F	F	F	T	T	T	T	T

Since the last column is not a tautology, the argument is fallacy.

More complex argument

Dilemma: Dilemma is an argument in which both the hypothetical syllogism and disjunctive syllogism are combined together.

Example: Consider the following argument

$\neg(p \vee q)$ premise

$\neg r \vee q$ premise

$\neg s \to r$ premise

$\therefore s$ Conclusion.

Truth table would have $2^4 = 16$ rows.

One can ~~very~~ verify the ~~that~~ above argument is valid using truth table. (Exercise)

Note Once we start to have, say six propositions, then the truth table would have 64 rows & this is beyond the attention span of most people

Example: (The paradox of the court)

→ The most celebrated example of an argument from the Ancient Greeks.

→ The famous teacher Protagoras agreed to train a student named Euathlus in the art of logic.

→ The condition being only half the fee is required at the time of instruction & the remaining fee due when Euathlus won his first case in court.

→ Should Euathlus fail, then the fee would be forfeited.

→ When Euathlus' training was completed, he delayed to undertake any case.

→ Eventually, Protagoras could no longer wait for payment, and decided to expedite the process.

→ Protagoras decided to sue Euathlus.

Protagoras argued

1. If this case is decided in my favor, Euathlus must pay me by order of the court.
2. If it is decided in Euathlus's favor, Euathlus must pay me under the terms of the agreement.
3. But, it must be decided either in my favor, or Euathlus' favor

---

Therefore, Euathlus' is bound to pay me in any case.

Protagora's argument (Symbolic)

$p \rightarrow q$

$\neg p \rightarrow r$

$p \vee \neg p$

$\therefore q \vee r$

valid argument.

p : case is decided in my favor

q : Euathlus must pay me by the order of the court.

$\neg p$: case is not decided in my favor

r : Euathlus must pay me ~~by the~~ under the terms of the agreement

Euathlus cleverly rebutted with the following, using the same argument as his teacher

1. If the case is decided in favor of Protagoras, I am free by the terms of the argument.
2. If it is decided in my favor, I'm free by order of the court.
3. But, it must either be decided in Protagora's' favor or my favor

Therefore, I am discharged of my debt in any case.

$C_1: \neg p \vee q$

$C_2: p \vee r$

$C_3: p \vee \neg p$

$C_4: q \vee r$

$C_5: \neg q \wedge \neg r$ (negation of conclusion)

$C_6: \neg q$

$C_7: \neg r$

$C_8: r$

$C_9: \Box$

$q \vee \neg p$

$q \vee r$

Symbolically

$p \rightarrow q$

$\neg p \rightarrow r$

$p \vee \neg p$

$q \vee r$

C_1, C_3 : $q \vee \neg p$. (C_7)

C_2, C_7 : $q \vee r$ (C_8)

$\neg q$

$\neg r$

$\Box$

$C_1: \neg p \vee q$

$C_2: p \vee r$

$C_3: p \vee \neg p$

$C_4: \neg q \wedge \neg r$

$C_5: \neg q$

$C_6: \neg r$

$C_7: \neg p$ (C_1, C_5)

$C_8: r$ (C_2, C_7)

$C_9: p$ (C_3, C_7)

$C_{10}: \Box$

$\boxed{\text{Garbage in, Garbage out}}$ – Valid arguments with false propositions.
– Invalid deductions from true statements.

Valid argument

Snail is not an animal argument

(a false premise) If a snail is an animal (s), it has a voice (v) $\quad s \to v$

A snail does not have a voice. $\quad \neg v$

(false conclusion) Therefore, a snail is not an animal $\quad \therefore \neg s$

by modus tollens

We know that
a snail is an animal

· ~~This argument~~ is valid, but the ~~derived conclusion is false~~.

⇒ Derived conclusion is false; nonetheless, it has been derived from a valid argument.

⇒ · $\boxed{\text{Your inferences are only as good as your premises.}}$

Def^n (Truth & falsity): Truth & falsity are attributes of propositions.

Def^n (Validity & invalidity): Validity & invalidity are attributes of arguments.

Invalid arguments

	True Conclusion	False Conclusion
True premises	✓	✓
False Premises	✓	✓

Valid arguments

	True Conclusion	False Conclusions
True premises	✓	X
False premises	✓	✓

Example:

(~~false~~ true) All cats (c) have four legs (l) $c \to l$

(~~false~~ true) All dogs (d) have four legs (l) $d \to l$

(false) Therefore, all dogs (d) are cats (c) $\therefore d \to c$

Argument ~~is~~ invalid.

Example:

(false) All cats (c) understand French (f) $c \to f$

(false) All dogs (d) are cats (c) $d \to c$

(false) Therefore, all dogs understand french $\therefore d \to f$

Argument valid.

Sound argument When an argument is valid, and all of its premises are true, we call the argument sound.

Example: Is the following argument valid or invalid? Is it sound or unsound?

Time (t) is money (m). $t \to m$ false

All money (m) is paper (p). $m \to p$

Therefore, all time is paper. $\therefore t \to p$ by Hypothetical syllogism

Argument valid, but not sound as 'time is money' is not true; hence conclusion may be true or false.

Summary

- The rules of inference in logic provides a systematic way of showing statements are equivalent to each other.
- An argument consists of a set of propositions $p_1, p_2, \cdots, p_n$, called the premises, and a proposition q called the conclusion. An argument is valid iff the conclusion is true whenever the premises are all true.
- A fallacy is an argument that has an inherent flaw in the structure of the argument itself which renders the argument invalid.
- A syllogism consists of three propositions, the last of which, called the conclusion, is a logical consequence of the two former called the major and minor premise. The two types of syllogism are the hypothetical syllogism and the disjunctive syllogism.
- The dilemma is an argument in which both the hypothetical syllogism & disjunctive syllogism are combined together.
- Truth and falsity are attributes of individual propositions.
- Validity and invalidity are attributes of arguments.
- When an argument is valid, and all its premises are true, we call it a sound argument.

four main types of rules of inference

Modus Ponens

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$$

Modus Tollens

$$\begin{array}{l} p \to q \\ \neg q \\ \hline \therefore \neg p \end{array}$$

Hypothetical Syllogism

$$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array}$$

Disjunctive Syllogism

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$

fallacies (non sequiturs)

Affirming a Disjunction

$$\begin{array}{l} p \vee q \\ p \\ \hline \therefore \neg q \end{array}$$

Affirming the consequent

$$\begin{array}{l} p \to q \\ q \\ \hline \therefore p \end{array}$$

Denying the Antecedent

$$\begin{array}{l} p \to q \\ \neg p \\ \hline \therefore \neg q \end{array}$$

Three types of dilemmas (All valid)

Simple Constructive

$$\begin{array}{l} p \to r \\ q \to r \\ p \vee q \\ \hline \therefore r \end{array}$$

Complex Constructive

$$\begin{array}{l} p \to r \\ q \to s \\ p \vee q \\ \hline \therefore r \vee s \end{array}$$

Disjunctive

$$\begin{array}{l} p \to r \\ q \to s \\ \neg r \vee \neg s \\ \hline \therefore \neg p \vee \neg q \end{array}$$

$C_1: \neg p \vee r$
$C_2: \neg q \vee s$
$C_3: \neg r \vee \neg s$
$C_4: p \wedge q$
$C_5: p$
$C_6: q$
$C_7: r$
$C_8: s$
$C_9: \square$

$C_1: \neg p \vee r$
$C_2: \neg q \vee r$
$C_3: p \vee q$
$C_4: \neg r$
$C_5: r \vee q$
$C_6: r$
$C_7: \square$

$C_1: \neg p \vee r$
$C_2: \neg q \vee s$
$C_3: p \vee q$
$C_4: \neg(r \vee s)$ i.e. $\neg r \wedge \neg s$
$C_5: \neg r$
$C_6: \neg s$
$C_7: \neg p$
$C_8: q$
$C_9: \neg q$
$C_{10}: \square$

Proofs is a valid argument that establishes the truth of a mathematical statement.

- can use the hypotheses of the theorem, axioms assumed to be true & previously proven theorems along with rules of inference to establish the truth of the statement being proved.

proof.

formal proofs

- (all steps supplied, the rules for each step in the argument were given)
- (formal proofs extremely long, hard to follow)
- (used in computer for automated reasoning systems)

informal proofs.

- (designed for human consumption)
- (more than one rule ~~may~~ of inference may be used in each step, steps may be skipped, axioms ~~used~~ assumed and rules of inference used are not explicitly stated)

- Applications to prove mathematical theorems.
- Applications in Computer Science
  - verifying that computer programs are correct
  - establishing that operating systems are secure
  - making inferences in artificial intelligence
  - showing that system specifications are consistent.
  - so on.

Terminologies

~~Some inform~~ of ~~Some~~.

- Theorem → Statement that can be shown to be true
  (/fact/result)
  (important statement)

- proposition → less important theorems.

- axioms/postulates → Statements we assumed to be true.

- lemma → less important theorem that is helpful in the proof of other results.
  → Complicated proofs are easier to understand when they are proved using a series of lemmas.

- Corollary → a theorem that can be established directly from a theorem that has been proved.

- Conjecture → a statement being proposed to be true statement, usually on the basis of some partial evidence, a heuristic argument, or the intution of an expert.
  → becomes a theorem when a proof of a conjecture is found.
  → Many times conjectures are shown to be false, so they are not theorems.

Types of proofs for $p \to q$.

- Direct proof.
- Indirect proof.
  - contrapositive
  - proof by contradiction.
- Vacuous proof.
- Trivial proof.

Trivial proof:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

$p \to q$ is true when q is true

Example: let $P(n)$ be

"If $a \geq b$ then $a^n \geq b^n$."

Domain: all integers

p: $(a \geq b)$

q: $a^n \geq b^n$

$P(n)$: $p \to q$ true when q is true

Q> $\boxed{\text{Show that } P(0) \text{ is true}}$

As $a^0 = 1 = b^0$, we get $a^0 \geq b^0$ i.e. q true. Hence $P(0)$ (i.e. $p \to q$) is true

Vacuous proof:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

$p \to q$ is true when p is false.

Example:

let $P(n)$: "If $n > 1$, then $n^2 > n$."

Domain: all integers.

$p = (n > 1)$

$q = (n^2 > n)$.

$P(n)$: $p \to q$. true when p is false.

Q> $\boxed{\text{Show that } P(0) \text{ is true}}$.

As $0 > 1$ is false, $P(0)$ is true i.e. $p \to q$ is true

- Vacuous proofs are often used to establish special cases of theorems that state that a conditional statement is true for all positive integers.
- Trivial proofs are often important when special cases of theorems are proved of mathematical induction.

Example: Prove that if n is an integer & n^2 is odd, then n is odd.

Attempt a derect proof.

Suppose n is an integer & n^2 is odd.

Let $n^2 = 2k+1$, k is any integer.

$n = \pm\sqrt{2k+1}$ which does not help to conclude n is odd.

Use contraposition

p: n is an integer & n^2 odd

q: n odd

$p \to q$.

contraposition

$\neg q \to \neg p$.

Let n be not odd.

$\therefore$ n is even

$\therefore$ $n = 2k$ for some integer k.

Then $n^2 = 4k^2 = 2(2k^2) = 2t$, $t = 2k^2$

$\Rightarrow$ n^2 is even

i.e. n^2 not odd

Thus $\neg q \to \neg p$

So $p \to q$.

Use contradiction

Let p be true & $\neg q$ holds

i.e. n^2 odd for an integer n, but n is not odd

$\therefore$ n is even $\Rightarrow n = 2k$ for some integer k

$\Rightarrow n^2 = 4k^2 = 2(2k^2) = 2t$ for some integer t

$\Rightarrow n^2$ is even

$\Rightarrow n^2$ not odd $\Rightarrow$ $\neg p$ is true

Since p & $\neg p$ both true, we get a contradiction

Proof of equivalence

- $(p \leftrightarrow q) \Leftrightarrow [(p \to q) \wedge (q \to p)]$ is a tautology.

Example: Prove the theorem

"If n is a +ve integer, then n is odd iff n^2 is odd"

$\underbrace{n \text{ is a +ve integer}}_{p}$, then $\underbrace{n \text{ is odd iff } n^2 \text{ is odd}}_{q}$

To prove, $p \to q$ — $q \to p$ already proved above.

A Direct proof works here

n odd $\Rightarrow n = 2k+1$ for some integer k.

$n^2 = 4k^2 + 4k + 1 = 2k(k+1) + 1$. which is odd.

Both $p \to q$ & $q \to p$ true

Hence the theorem is true

- $p_1, p_2, \ldots, p_n$ are propositions which are equivalent

i.e. $p_1 \Leftrightarrow p_2 \Leftrightarrow \ldots \Leftrightarrow p_n$

$[p_1 \Leftrightarrow p_2 \Leftrightarrow \ldots \Leftrightarrow p_n] \Leftrightarrow [(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \ldots \wedge (p_n \to p_1)]$

i.e. $p_1, p_2, \ldots, p_n$ are equivalent if we can show

$p_1 \to p_2,\ p_2 \to p_3, \ldots, p_n \to p_1$

This is much more efficient than proving $p_i \to p_j$ for all $i \neq j$ with $1 \le i \le n$ & $1 \le j \le n$.

Counterexample: To show a statement of the form $\forall x P(x)$ false, we need only to find a counterexample.

Example: Show that the statement

"Every positive integer is the sum of squares of two integers"

$\forall c, \exists a, b \; (a^2+b^2=c)$

is false.

$a^2+b^2=c$

a, b, c are integers

Counterexample → $c=3$ cannot be written as a sum of two sqs.

proof techniques

- mathematical induction
- Combinatorial proofs.

Example: Show that 29 is a prime no.

~~proof.~~ Sol^n (by contradiction).

Let 29 is not a prime no.

$\therefore 29 = rs$, r & s are not 1 & 29.

Smaller of r & s, ~~must~~ say s, must be < 6

o.w. if r & s both are at least 6, ~~then~~ we should have $rs \geq 36$

So $s < 6$

i.e. $s = 2, 3, 4, 5$ ~~none of which is a multiple of 29~~

Thus $s = 2, 3, 4$ or 5 is a multiple of 29.

But we know none of $2, 3, 4, 5$ is a multiple of 29.

Therefore, our assumption must be false

Hence 29 is a prime no.

Theorem (Euler)

There is no greatest prime no.

proof. (by contradiction)

Let there is a greatest prime no., say X.

Make a complete list of primes in increasing order: $L = \{2, 3, 5, \dots, X\}$.

Consider the no. $Y = 2.3.5\dots X + 1$

$Y > X$, so Y is not a prime, thereby Y has a prime factor p from the list $L = \{2, 3, 5, \dots, X\}$.

$p \mid Y$, $p \mid 2.3.5\dots X \Rightarrow p \mid Y - 2.3.5\dots X \Rightarrow p \mid 1$ ($\rightarrow\leftarrow$)

Hence our assumption must be wrong. Hence no greatest prime no.

Example: The number 3 is a prime, and $3+1=4$ is a perfect square. Show that there are no other prime numbers n such that $n+1$ is a perfect square.

Sol^n: Domain of disclosure ~~is~~ consists of all natural nos. $n \geq 1$.

To prove

- n is prime $\rightarrow$ $n+1$ is not a perfect square.

Contraposition

- $n+1$ is a perfect square $\rightarrow$ n is not a prime.

$\rightarrow$ proof is straight forward.

if $n+1 = m^2$, then $n = m^2 - 1 = (m+1)(m-1)$ which is ~~not prime unless~~ product of two nos, $m-1$ & $m+1$, & is not prime, unless $m-1=1$ i.e. $m=2$ i.e. $n=3$.

$n=3$ is the only possibility as claimed.

- $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$.
- Sometimes it is easier to construct proof of the contrapositive.

- **proof by contradiction**

1) Given a statement s that we wish to prove true
2) assume the opposite, $\neg s$, and
3) deduce a statement r that is known to be false.

- r is often of the form $q \wedge (\neg q)$, an obvious contradiction.

Example: Decide whether the following statement is true or false.

" $2^{67}-1$ is a prime".

- $2^{67}-1$ has 20 digits
- Trial & error method ~~~~ does not help.
- Use Modern ~~~~ computer algebra system, such as Maple which has ~~~~ sophisticated programs for factorizing large numbers, & they quickly give the factorization:

difficult to establish

$$\underbrace{2^{67}-1}_{M_{67}} = (193{,}707{,}721) \times (761{,}838{,}257{,}287)$$

M_{67} (Mersenne number).

- Frank Nelson Cole (1903) factored M_{67} long before electronic calculators & computers were invented, using only pencil & paper calculations.

- It ~~took~~ him 20 years of Sunday afternoons to find the factors of M_{67}.

Example:

proof

- M_n to be prime, n must be prime.
- n prime does not always imply M_n is prime.

Claim

$k = \cancel{\ }$ is prim

if k not prim

$k = rs$

$a^k-1 = (a^r)^s-1$

$= (a^r-1)(a^{r(s-1)}+\dots+a^r+1)$

≥ 0

violating primality of a^k-1

a^k-1

$= (a-1)\underbrace{(a^{k-1}+a^{k-2}+\dots+a+1)}_{\geq a+1 > 1 \text{ for } a>0}$

nontrivial factor

a^k-1 prime $\Rightarrow a-1=1$

$\Rightarrow a=2$

- if ~~~~ a^k-1 is prime ~~iff a=2~~ then $a=2$ & k is prime

$(a>0,\ k\geq 2)$

Example: Prove the Theorem: $2^{66}-1$ is not a prime no.

$$2^{66}-1 = (2^{33})^2-1 = (2^{33}-1)(2^{33}+1)$$

easy to establish

(Existential Statements)

Example: ~~Prove~~ Decide whether the following statements are true or false.

1) There is a number n such that $n^2=441$.

2) There are numbers a, b, c, d s.t. $a^4+b^4+c^4=d^4$.

Domain of disclosure consists of all natural nos.

Soln: $\boxed{\text{find an example.}}$

1) $(21)^2 = 441$. So true example for the statement is $n=21$ $[(-21)^2=441$, but -21 is not within the domain of disclosure

2) Example for the statement

Not always easy

× $4,567,381^4 + 16,123,542^4 + 15,381,567^4 = 23,645,789$

✓ $2,682,440^4 + 15,365,639^4 + 18,796,760^4 = 20,615,673^4$

~~$a^4+b^4+c^4=d^4$~~

- For hundreds of years, many people doubted whether an example existed.
- During that time the statement was not proved to be either true or false.

→ Conjecture.

- (1988) example found, so it has now the status of a Theorem.

Example (Universal statements).

1) n^2+n is an even no. ($n(n+1)$ two consecutive nos, so even)
2) $4n-1$ is a prime no. (Counter example, $n=4$)
3) if n is a multiple of 6, then n is a multiple of 3 (true)
4) if n is a multiple of 3, then n is a multiple of 6. (false, Counter example $n=9$)

Domain $\to$ all natural nos.

- ~~To show a universal statement is false, we have to find a counter example.~~
- A universal statement is false if it is false for just one value of n.
- The value of n for which the statement is false is referred as a counter example.

$\downarrow$

Not always easy

Example: Let $X = \{n \in \mathbb{N} \mid 1 \le n \le 100\}$.

Show that the statement $\forall x \in X$, $\boxed{x^2+x+41}$ is a prime is false.

Euler's polynomial

$x=40$ also works

Soln A counter example is required.

Try with $x = 1, 2, \ldots$

$x^2+x+41 = 43, 47, \ldots$

our strategy

Take $x=41 \to 41^2+41+41 = 41\,(43)$.

counter example.

Assign a value to x so that all three term $x^2, x, 41$ have a common factor. $x=41$ more

- $f(n) = n^2+n+41$ widely believed to assumed only prime values.
- Euler (1772) shown this was false.

→ ~~produce~~ form for $n = 0, 1, 2, \cdots, 39$.

- This provocative conjecture is shattered in the cases $n = 40$ & $n = 41$.
- ~~Again~~ $f(42) = 1847$ turns out to be prime once again
- For first 100 integer values of n, the Euler's poly represents 86 primes.
- It has been shown that no polynomial of the form n^2+n+q, with q prime, can do better than Euler's polynomial in giving primes for successive values of n.

40

- $h(n) = 103n^2 - 3945n + 34381$ → (1988), produces more than 43 distinct primes for $n = 0, 1, \cdots 42$.
- Current record holder

$k(n) = 36n^2 - 810n + 2753$ → string of 45 prime value

Fermat's last Theorem

The Diophantine equ^n.

$$x^n + y^n = z^n$$

has no solution in integers x, y & z with $xyz \neq 0$

Whenever n is an integer with $n > 2$

- $\underline{n=2}$ $\quad x^2+y^2=z^2$ has infinitely many sol^{ns}. in integers $x, y,$ & z → Pythagorean triples
- $n=3$ (Euler)
- $n=4$ (Fermat)
- several failed attempts led to development of algebraic number theory.
- too 300 years to get a correct proof
- 1990, Andrew Wiles → using theory of elliptic curves → a sophisticated area of number theory.
  (10 years)

The $3x+1$ conjecture

- T → a transformation that sends an even integer x to $x/2$ and an odd integer x to $3x+1$.
- The $3x+1$ conjecture states that for all positive integers x, when we repeatedly apply the transformation T, we will eventually reach the integer 1.

Example: $\quad x = 13$

$T(13) = 3.13 + 1 = 40$

$T(40) = 40/2 = 20$

$T(20) = 10$

$T(10) = 5$

$T(5) = 16$

$T(16) = 8$

$T(8) = 4$

$T(4) = 2$

$T(2) = 1$.

Dilemmas

Example 1

$p \to q$

$\neg p \to r$

$p \vee \neg p$

$\checkmark \neg q$

$\checkmark \neg r$

$\checkmark \neg p \vee q$ $\quad \checkmark \neg p . \vee q$ $\quad r \vee q$ $\square$

$p \vee r$ $\quad \cancel{p \vee r}$

$x = 40$

$x^2 + x + 41$

$= 40^2 + 40 + 41$

$= 40 \cdot 41 + 41 = 41 \cdot 42$

$= \cancel{42^2 + 2 \cdot 42}$

$= \cancel{42 \cdot 43} + 41$

$2 \cdot 42^2 + 41.$

Example 2

$\neg(p \vee q)$

$\neg r \vee q$

$\neg s \to r$

$\neg s$

$\checkmark \neg p \wedge \neg q$

$\neg r \vee q$

$s \vee \neg r$

$\neg s$

$\cancel{\neg p}$

$\cancel{\neg q}$ $\checkmark q$

$\checkmark \neg r \vee q$

$\checkmark s \vee \neg r$

$\checkmark \neg s$

$\checkmark \neg r$ $\quad \checkmark s$ $\quad \square$

- attracted attention of mathematics since 1950s.
- goes by many other names –
  Collatz problem, Hasse's algm, Ulam's problem, the Syracuse problem, & Kakutani problem.
- many mathematicians have been diverted from their work to spend time attacking this conjecture.

Godel's Incompleteness Theorem

a formula involving propositional variables using connectives $\neg, \wedge, \vee, \to, \leftrightarrow$ in a proper manner

- A formal system is consistent if both an assertion A & its negation $\neg A$ cannot be proved in that.
- A formal system is complete if every true assertion can be proved in the system.

" There does not exist a consistent & complete system for integer arithmetic."

Idea of Godel numbering

- The Godel no. of the finite seq. of +ve integers $i_1, i_2, \ldots, i_n$ is $2^{i_1} * 3^{i_2} * \cdots * (\text{prime}(n-1))^{i_n}$ taking 2 as prime(0.)

Example: 3, 2, 1, 1

$\downarrow$

Godel no is

$2^3 * 3^2 * 5^1 * 7^1 = \boxed{2520}$

Example: Gode no. $= 300 = 2^2 \cdot 3^1 \cdot 5^2$

$\downarrow$

the cor. seq. is 2, 1, 2

$300/2 = 150/2 = 75/3$
75 $= 25/5$
$= 5/5$
$= 1$

English alphabet a $\to$ 1
b $\to$ 2
⋮

A sentence can get a Godel numbering.

Statement 1: $\boxed{\text{The statement whose Godel numbering is } x \text{, is not a theorem.}}$

(x was specified).

- The Godel no. of this Statement 1 was calculated

It was found to be x.

- If there exists an axiomatic complete & consistent system, every true statement must be a theorem there.

- Suppose there exists such a system. Then if Statement 1 is derived from the axioms using the rules of inference, it is a theorem.

- But Statement 1 says it is not a theorem.
- Hence we arrive at a contradiction.

- On the other hand, if Statement 1 ~~is~~ cannot be derived from the axioms using rules of inference, it is not a theorem and statement 1 is true statement which cannot be proved in the axiomatic system.

- Hence the system is not complete.
- Thus Godel stated that for any sound logical axiometic system that is sufficiently rich to contain the theory of numbers, there must be statements that can neither be proved nor disproved.