11.01.16

January 11, 2016 12:58 PM

Logic

It started with Greeks (father of logic: Aristotle, 384-322 BC).
Sophisticated analysis on logic; propositional and quantificational and model logic.
The fragment of logic most useful in Engineering and Computer Science is called propositional logic (by Stoics, 250 BC).
In propositional logic, everything is True or False (i.e. declarative sentence, their value is either T or F).

Let p be a proposition.
By $\neg p$ we mean "not p", it's not the case that p.

Let p, q be propositions, we can form formulas or compound formulas as follows:
$(p \wedge q)$ means "p and q", "p conjunction q"
Values: $(p \wedge q)$ is True when both p and q are True and $(p \wedge q)$ is False otherwise.

Truth table for $p \wedge q$ and $\neg p$:

p	q	$p \wedge q$	$\neg p$
T	T	T	F
T	F	F	F
F	T	F	T
F	F	F	T

Inclusive **or** (the one used by mathematicians); it means and / or.
$(p \vee q)$ is True when one or the other (or both) is True.

The usual linguistic expression (p or q) but not both is $p \dot{\vee} q$.

Truth table for $p \vee q$ and $p \dot{\vee} q$:

p	q	$p \vee q$	$p \dot{\vee} q$
T	T	T	F
T	F	T	T
F	T	T	T
F	F	F	F

There is also implication:
p implies q $(p \to q)$
Other notation: $p \supset q, p \Rightarrow q$

p is the hypothesis (a given) and q is the conclusion

Truth table for $p \to q$:

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

$1 + 1 = 3 \to 2 + 5 = 6$
False False
Therefore the statement is True.

Logical equivalence:
$p \leftrightarrow q$ means "p if and only if q", "p iff q", "p is equivalent to q"
It is True if p and q have the same value, and it is False otherwise.

Truth table for $p \leftrightarrow q$:

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

$(p \vee p) \leftrightarrow p$ is always True:

p	$p \vee p$	$p \leftrightarrow p$
T	T	T
F	F	T

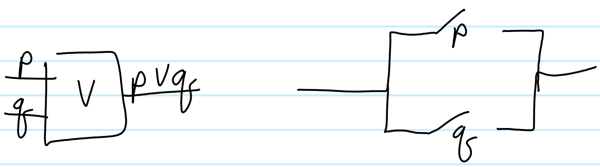
$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$ is always True

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$	$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$
T	T	T	T	T	T	T	T	T
T	T	F	T	T	T	T	F	T
T	F	T	T	T	F	T	T	T
T	F	F	F	F	F	F	F	T
F	T	T	T	F	F	F	F	T
F	T	F	T	F	F	F	F	T
F	F	T	T	F	F	F	F	T
F	F	F	F	F	F	F	F	T

A formula in propositional logic whose truth table value (in each row) is True is called a tautology.
The algebraic laws of tautologies are called Boolean Algebra Laws.

Leibniz was interested in logical machines and formalizing arguments (never accomplished).
George Boole: mathematical investigation of the laws of thought.
Claude Shannon: circuit analysis

$p \wedge q$ corresponds exactly to a
switching circuit where electricity
flows iff p, q are both ON, else NOT



electricity flows iff p or q is True

$\neg p$ is True when p is False and vice-versa

p_1	...	p_n
T		T
T		F
T		T
...		...
F		T
F		F
F		T

Translation

$\neg p$ is "not p", "it is not the case that p"
$p \wedge q$ is "p and q", "p but q"
$p \vee q$ (always the inclusive or) is "p or q", "p and/or q", "p or q or both", "p unless q"
$p \rightarrow q$ is "p implies q", "if p then q", "p is sufficient for q", q follows from p", "q whenever p", "q is a necessary condition for p", "q unless not p", "q or else not p".
$p \leftrightarrow q$ is "p iff q", "p is necessary and sufficient for q", "if p then q and conversely if q then p"

Exercice: Check $p \leftrightarrow q$ is equivalent to $p \rightarrow q \wedge q \rightarrow p$.

13.01.16

January 13, 2016 11:28 AM

Propositional Calculus

Formulas are built from atoms $p_1, p_2, p_3, \ldots$

Using a recursive definition

① Atoms are formulas (of propositions)

② If A, B are formulas, so are $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$

③ That's the definition

Meaning of formulas : all formulas are valued in {T, F}

		not ...	... and ...	... or ...	... implies ...	... iff ...
P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \rightarrow Q$	$P \leftrightarrow Q$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

In $P \rightarrow Q$, P is the hypothesis or premise and Q is the conclusion.

The exclusive or is definable :

$P \dot{\vee} Q$ or $P \oplus Q \overset{\text{def}}{=} (P \vee Q) \wedge \neg(P \wedge Q)$

Check:

P	Q	$P \oplus Q$
T	T	F
T	F	T
F	T	T
F	F	F

Translation (Rosen 1.1)

$\neg p$	not p	it is not the case that p		
$P \wedge Q$	P and Q	both P and Q	P but Q	P together with Q

The sky is not blue but the sun is shining.

Let P be "The sky is blue" and Q be "The sun is shining".

"The sky is not blue but the sun is shining" becomes $\neg P \wedge Q$

$P \vee Q$	P or Q	either P or Q	P or else Q	P unless Q

"The sky is blue unless the sun is not shining" becomes $P \vee \neg Q$

$P \rightarrow Q$	P implies Q	if P then Q	P only if Q	Q, if P	P is sufficient	Q is necessary
	Q follows	Provided that	Q, provided			

In order for the sun to be shining, it suffices that the sky is blue.
i.e. the sky is blue is sufficient for the sun to be shining
$P \to Q$
i.e. the sun shining is necessary for the sky to be blue.

Logical argument

H_1
H_2
$\vdots$
H_n

$\therefore C$

(Hypothesis 1 ∧ Hypothesis 2 ∧ ... ∧ Hypothesis n) → Conclusion C

$A =$ Sam is an engineer
$A \to B =$ If Sam is an engineer then Sam is brilliant
∴ Sam is brilliant

$Z =$ I like blue cheese
$W =$ Blue cheese is strong
$X =$ Blue cheese is medium
$Y =$ Blue cheese is hard

- I like blue cheese only if it is either not strong or medium.
- Blue cheese is strong unless it is medium
- Blue cheese being medium is sufficient for it to be hard
  ∴ if I like blue cheese, it will be hard

$Z \to (\neg W \vee X)$
$W \vee X$
$\underline{X \to Y}$
$\therefore Z \to Y$

A tautology is a formula whose value (in each row of the truth table) is True.
Example: $p \vee \neg p$

Truth table for $p \vee \neg p$:

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

$(P \to Q) \leftrightarrow (\neg Q \to \neg P)$

Hempel's paradox

The contrapositive of $P \to Q$ is $\neg Q \to \neg P$

P	Q	$P \to Q$	$\neg Q$	$\neg P$	$\neg Q \to \neg P$	$(P \to Q) \leftrightarrow (\neg Q \to \neg P)$
T	T	T	F	F	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

Logical equivalences

$A \equiv B \stackrel{\text{def}}{=} A \leftrightarrow B$ is a tautology.
$P \rightarrow Q \equiv \neg Q \rightarrow \neg P$
$P \equiv P \vee P$
$P \equiv P \wedge P$

P	$P \vee P$	$P \wedge P$	$(P \vee P) \leftrightarrow P$	$(P \wedge P) \leftrightarrow P$
T	T	T	T	T
F	F	F	T	T

The equations of logical equivalence are the laws of Boolean Algebra.

$A \vee \neg A \equiv$ T
$A \wedge \neg A \equiv$ F
F $\vee A \equiv A$
T $\wedge A \equiv A$

T	A	T $\wedge A$	$A \leftrightarrow (T \wedge A)$
T	T	T	T
T	F	F	T

$A \vee A \equiv A$
$A \wedge A \equiv A$
$\neg\neg A \equiv A$
$A \vee B \equiv B \vee A$
$A \wedge B \equiv B \wedge A$

A	B	$A \wedge B$	$B \wedge A$	$(A \wedge B) \leftrightarrow (B \wedge A)$
T	T	T	T	T
T	F	F	F	T
F	T	F	F	T
F	F	F	F	T

$(A \vee B) \vee C \equiv A \vee (B \vee C)$
$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$
$\neg(A \wedge B) \equiv \neg A \vee \neg B$
$\neg(A \vee B) \equiv \neg A \wedge \neg B$

Read notes on consistency

A says "if $1 + 1 = 2$ then $1 + 2 = 3$"

See Rosen 1.2

A says "I am a knave but B is not".

Case 1:
A is a knight
If so, A speaks True
But he says "I am a knave" $\Rightarrow$ contradiction

Case 2:
A is a knave
If so, A speaks False
A says "A is a knave $\wedge$ B is a knight"
But "A knave $\wedge$ B knight" must be False since A says True and A knave
$\therefore$ A knave is True
$\therefore$ B is a knight is False
$\therefore$ A, B both knaves

Example 2:
A says
① I love Linda
② If I love Linda then I love Kathy

Case 1: A is a knight
A loves Linda
By part 2, A also loves Kathy

Case 2: A is a knave
A does not love Linda (from ①)
② is also False
A does love Linda
<u>Contradiction</u>

18.01.16

January 18, 2016 12:53 PM

Review:
Knights always speak True and knaves always speak False

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$
T	T	T	T	T
T	F	F	T	F
F	T	F	T	T
F	F	F	F	T

De Morgan's Laws:
$\neg(p \vee q) \equiv \neg p \wedge \neg q$
$\neg(p \wedge q) \equiv \neg p \vee \neg q$

Example 2:

There are two individuals A and B on the island.
A says "I am a knave but B isn't"
Can we conclude anything?

A: "(A is a knave) $\wedge$ (B is not a knave)"

Case 1: A is a knight
So A speaks True
But A says a conjunction so each statement is True
Therefore "A is a knave" is True $\Rightarrow$ contradiction

Case 2: A is a knave
So A speaks False
De Morgan's law:
$\neg$ ((A is a knave) $\wedge$ (B is not a knave)) $\equiv \neg$ (A is a knave) $\vee$ $\neg$ (B is not a knave)
Either A is not a knave or B is a knave
But we know that A is a knave
Therefore B is a knave
There are no contradictions if A and B are knaves!

Example 3:

A, B, C are three inhabitants of the island.
A says "B is a knave"
B says "A and C are of the same type"

What is C?

Let's do cases on A since A's statement is simpler.

Case 1: A is a knight
$\therefore$ A speaks True
$\therefore$ B is a knave
$\therefore$ B lies
$\therefore$ A and C are not the same type
$\therefore$ C must be a knave

Case 2: A is a knave
∴ B is a knight
∴ B speaks True
∴ A and C are the same type
∴ C is a knave

Example 4:

You ask A: "Is there gold on the island?".
A says "There is gold if and only if I am knight." *

Answer: analyze the two cases

Case 1: A is a knight
∴ A speaks True
∴ * is True
A says "There is gold $\leftrightarrow$ I am a knight"
Since the RHS (right-hand side) is True, and * is True
And if A says no, there is no gold

Case 2: A is a knave
If A says yes, then the statement is False
But the RHS, so * is False
Therefore there is gold since one of two statements has to be True
And if A says no, the statement * is True
But the RHS of * is True
∴ the LHS is False
∴ there is no gold

Fundamental theorem of knights and knaves

Example 5:

A says "If $1 + 1 = 2$, then I am a knight"
B says "I am a knight only if $1 + 1 = 2$"

Case 1: A is a knight
Consistent since we get $\text{T} \rightarrow \text{T} = \text{T}$

Case 2: A is a knave
Also consistent since $\text{T} \rightarrow \text{F} = \text{F}$

Anyone can say what A said

Case 1: B is a knight
B is a knight $\rightarrow 1 + 1 = 2$ is always True
∴ B is a knight

A set of formulas $\{A_1, A_2, \dots, A_n\}$ is consistent if their conjuction is True in some row.

We say that A is a tautology if the value of A is True in every row.

$A \equiv B$ means $A \leftrightarrow B$ is a tautology.
i.e. the value colums of A and B in the truth table are equal.

$A \rightarrow B \equiv \neg A \vee B$
$\neg(A \rightarrow B) \equiv A \wedge \neg B$

The Laws of Boolean Algebra

$A \vee \neg A \equiv T$	$A \wedge \neg A \equiv F$	Negation Laws
F $\vee A \equiv A$	$T \wedge A \equiv A$	Unit Laws
$A \vee A \equiv A$	$A \wedge A \equiv A$	Idempotent Laws
$\neg\neg A \equiv A$	$\neg\neg A \equiv A$	Double Negative Law
$A \vee B \equiv B \vee A$	$A \wedge B \equiv B \wedge A$	Commutative Laws
$(A \vee B) \vee C \equiv A \vee (B \vee C)$	$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$	Associativity Laws
$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$	$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$	Distributive Laws
$\neg(A \wedge B) \equiv \neg A \vee \neg B$	$\neg(A \vee B) \equiv \neg A \wedge \neg B$	De Morgan's Laws

Read proof of $A \vee A \equiv A$ (from other equations)
e.g. $(A \to B) \wedge C \equiv (\neg A \vee B) \wedge C \equiv C \wedge (\neg A \vee B) \equiv (C \wedge \neg A) \vee (C \wedge B)$
(since $A \to B \equiv \neg A \vee B$)
The last one is called a disjunctive normal form (DNF), e.g. $(A \to B) \wedge C$

An argument

$$\left.\begin{matrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{matrix}\right\} \text{hypotheses}$$

$\therefore B$ (conclusion)

is True if $(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \to B$ is a tautology.

20.01.16

January 20, 2016 11:34 AM

Disjunctive Normal Forms (DNF)
(dual CNF, conjunctive normal forms)

Notation:
By associativity, $A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$ and $A \vee (B \vee C) \equiv (A \vee B) \vee C$.
We simply write $(A \vee B \vee C)$ disjunction of A, B, C.

We'll describe DNF's in three ways

- Truth tables
- Boolean algebra manipulation
- Truth-trees (or semantic tableaux)

A DNF is a formula of the form $C_1 \vee \cdots \vee C_k$ where $C_i = \ell_1 \wedge \cdots \wedge \ell_v$, where ℓ_r are literals.
A literal is an atom or the negation of an atom.

Examples:
$p_1 \wedge (p_2 \rightarrow p_3)$ is not a DNF
$p_1 \wedge (p_2 \vee p_3)$ is not a DNF
But $p_1 \wedge (p_2 \vee p_3) \equiv (p_1 \wedge p_2) \vee (p_1 \wedge p_3)$, and $(p_1 \wedge p_2) \vee (p_1 \wedge p_3)$ is a DNF.

Fact: every formula of propositional calculus is equivalent to a DNF.

Special case of a DNF: $k = 1$
Therefore the DNF is $C_1 = \ell_1 \wedge \cdots \wedge \ell_v$
Therefore $p_1 \wedge \neg p_3 \wedge p_4$ is a degenerate DNF.
However $p_1 \wedge \neg(p_2 \wedge p_3) \wedge p_4$ is not a DNF because the second element is not an atom or the negation of an atom.

Truth table algorithm for DNF of a formula ϕ.

- Draw the truth table of ϕ

p_1	…	p_{r-1}	p_r	ϕ	
T		T	T	T	C_1
⋮		T	F	T	C_2
⋮		F	T	F	C_3
T		F	F	F	
F		T	T	F	
⋮		⋮	⋮	⋮	
⋮		⋮	⋮	⋮	
F		F	F	F	

- Note the rows with value T
- Associate a conjunction C to a row (with value T) as follows:

$$C = \ell_1 \wedge \cdots \wedge \ell_v, \text{ where } \ell_i = \begin{cases} p_i, & \text{if } p_i = T \\ \neg p_i, & \text{if } p_i = F \end{cases}$$

$\phi \equiv C_1 \vee C_2 \vee C_3$

Example 1:

p	q	r	ϕ	
T	T	T	T	C_1
T	T	F	T	C_2
T	F	T	F	
T	F	F	T	C_3
F	T	T	F	
F	T	F	T	C_4
F	F	T	F	
F	F	F	T	C_5

$\phi = C_1 \vee C_2 \vee C_3 \vee C_4 \vee C_5$

$C_1 = p \wedge q \wedge r$
$C_2 = p \wedge q \wedge \neg r$
$C_3 = p \wedge \neg q \wedge \neg r$
$C_4 = \neg p \wedge q \wedge \neg r$
$C_5 = \neg p \wedge \neg q \wedge \neg r$

Notice that $C_1 \vee C_2 \vee C_3 \vee C_4 \vee C_5$ is True when ϕ is True and it is False when ϕ is False.

Example 2:

p	q	ϕ	
T	T	T	C_1
T	F	F	
F	T	T	C_2
F	F	T	C_3

DNF: $C_1 \vee C_2 \vee C_3$

$C_1 = p \wedge q$
$C_2 = \neg p \wedge q$
$C_3 = \neg p \wedge \neg q$

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

Now let's talk about Boolean algebra

$(A \rightarrow B) \equiv (\neg A \vee B)$
$(A \leftrightarrow B) \equiv (A \rightarrow B) \wedge (B \rightarrow A) \equiv (\neg A \vee B) \wedge (\neg B \vee A)$

Suppose A, B are atoms.
Find a DNF of $\neg(A \leftrightarrow B)$ by Boolean Algebra.

$\neg(A \leftrightarrow B) \equiv \neg\big((\neg A \vee B) \wedge (\neg B \vee A)\big)$
By De Morgan's laws ($\neg(p \wedge q) \equiv \neg p \vee \neg q$):
$\neg(A \leftrightarrow B) \equiv \neg(\neg A \vee B) \vee \neg(\neg B \vee A)$
By De Morgan's laws ($\neg(p \vee q) \equiv \neg p \wedge \neg q$):
$\neg(A \leftrightarrow B) \equiv (\neg\neg A \wedge \neg B) \vee (\neg\neg B \wedge \neg A)$
$\neg(A \leftrightarrow B) \equiv (A \wedge \neg B) \vee (B \wedge \neg A)$, which is a DNF.

Suppose A, B, C are atoms.

$\psi = \neg(A \leftrightarrow B) \wedge C$. Find a DNF.

$\neg(A \leftrightarrow B) \wedge C \equiv \big((A \wedge \neg B) \vee (B \wedge \neg A)\big) \wedge C$
Distributive law ($(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r)$):
$\neg(A \leftrightarrow B) \wedge C \equiv (A \wedge \neg B \wedge C) \vee (B \wedge \neg A \wedge C)$, which is a DNF of ψ.

Boolean algebra DNF's can often be simplified.

e.g. if $C_1 \vee C_2 \vee \cdots \vee C_k \vee T \equiv T$ (since $A \vee T \equiv T$, the unit law)
Also, if $C_i = \ell_1 \wedge \ell_2 \wedge \cdots \wedge \ell_v \wedge F \equiv F$.

This leads to another test for finding tautologies. If you show $A \equiv T$, then A is a tautology.

Find a DNF for $p \to (q \to p)$ (by Boolean algebra).

$p \to (q \to p) \stackrel{\text{def}}{=} \neg p \vee (q \to p)$
$p \to (q \to p) \stackrel{\text{def}}{=} \neg p \vee (\neg q \vee p)$
$p \to (q \to p) \equiv \neg p \vee (p \vee \neg q)$
By associativity:
$p \to (q \to p) \equiv (\neg p \vee p) \vee \neg q$
$p \to (q \to p) \equiv \mathrm{T} \vee \neg q$
$p \to (q \to p) \equiv \mathrm{T}$

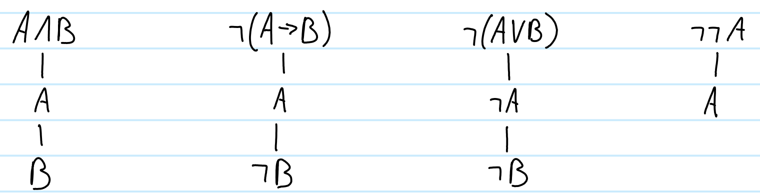
Hence $p \to (q \to p)$ is a tautology.

We can check:

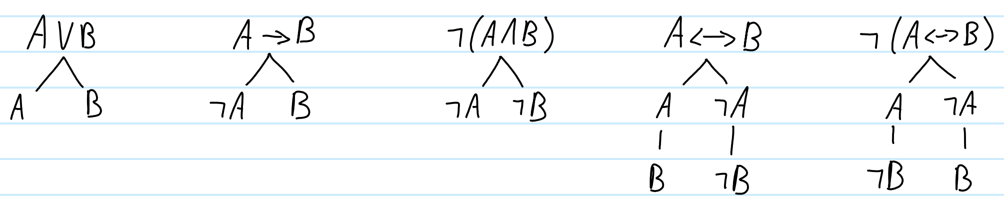
p	q	$q \to p$	$p \to (q \to p)$
T	T	T	T
T	F	T	T
F	T	F	T
F	F	T	T

You're not allowed to use Boolean methods with truth trees.
Formulas are considered as syntactic objects and no simplifications (except for tree rules).

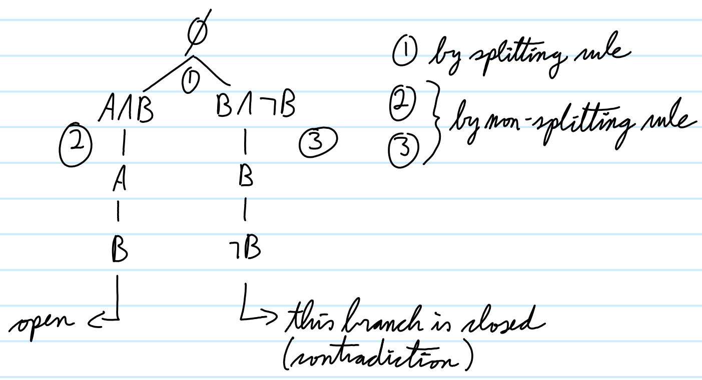
Non-splitting:



Splitting:



$\phi = (A \wedge B) \vee (B \wedge \neg B)$
Draw the truth tree for ϕ.



Break formulas down to literals.
If a branch is open, everything on that branch (including the root) is True.
Therefore we can assign a truth value (valuation) do ϕ. $V(A) = V(B) = T$

A	B	ϕ
T	T	T

25.01.16

January 25, 2016 1:07 PM

Supplemental questions

1.

p	q	P_3	P_4
T	T	T	F
T	F	F	T
F	T	T	F
F	F	T	T

What are P_3 and P_4 in DNF?

P_3: $(p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)$
P_4: $(p \wedge \neg q) \vee (\neg p \wedge \neg q)$

These are called perfect DNFs; each clause has every atom or its negation

Now we can simplify

$P_3 = (p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)$
Distributive law:
$P_3 \equiv (p \wedge q) \vee \left(\neg p \wedge (q \vee \neg q)\right)$
Negation law:
$P_3 \equiv (p \wedge q) \vee (\neg p \wedge \mathrm{T})$
Unit law:
$P_3 \equiv (p \wedge q) \vee \neg p$
$P_3 \equiv (p \vee \neg p) \vee (q \vee \neg p)$
$P_3 \equiv \mathrm{T} \wedge (q \vee \neg p)$
$P_3 \equiv q \vee \neg p$

Now let's do P_4

By observation of the table: $P_4 \equiv \neg q$

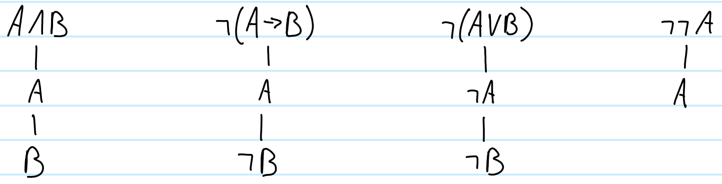
Proof:
Distributive law:
$P_4 \equiv (p \vee \neg p) \wedge \neg q$
Negation law:
$P_4 \equiv \mathrm{T} \wedge \neg q$
$P_4 \equiv \neg q$

In Boolean algebra, associativity of $\wedge$ and $\vee$ hold
$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$
$A \vee (B \vee C) \equiv (A \vee B) \vee C$

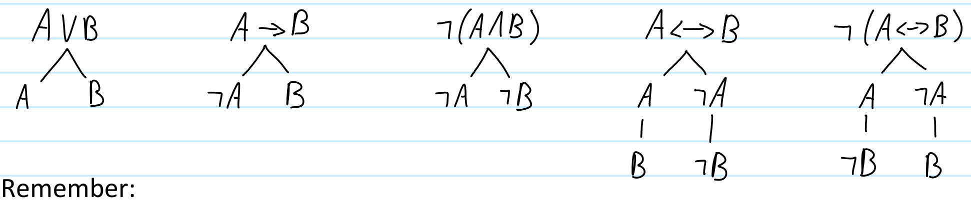
In Boolean algebra, we can write $(A \vee B \vee C)$ without ambiguity

Truth Trees (NO BOOLEAN OPERATIONS ALLOWED)

α-rules (non-splitters)
Formula is equivalent to a conjunction



β-rules (splitters)
Formula is equivalent to a disjunction



Remember:
$A \leftrightarrow B \equiv (A \to B) \wedge (B \to A)$
$A \leftrightarrow B \equiv (\neg A \vee B) \wedge (\neg B \vee A)$
and
$\neg(A \leftrightarrow B) \equiv \neg\big((A \to B) \wedge (B \to A)\big)$
$\neg(A \leftrightarrow B) \equiv \neg\big((\neg A \vee B) \wedge (\neg B \vee A)\big)$

But why is $A \leftrightarrow B$ itself a β-formula?

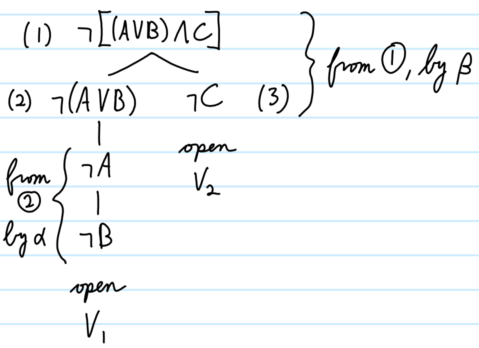
We can use truth trees (also called semantic tableaux or analytic tableaux).

① Check if a formula is a tautology
② Check if the arguments are valid
③ Find DNF
④ Check for consistency of sets of formulas of propositions

Truth trees form a refutation based theorem proving system
To check if a formula ϕ is a tautology or not, suppose it's false (look for $\neg\phi$) and look for a contradiction (in every branch). If every branch (of the tree for $\neg\phi$) has a contradiction, the formula at the root $\neg\phi$ is never true, so ϕ is always true, hence a tautology. If some branch of the tree for $\neg\phi$ is not contradictory (open), then $\neg\phi$ is true on that branch, so ϕ is false. The open branch corresponds to one row of the truth table for ϕ, in which ϕ has value F.

$\phi \equiv (A \vee B) \vee C$

To check if it's a tautology, form the tree for $\neg\phi$



Each open branch corresponds to a valuation V_1, V_2.

$V_1(A) = F, \quad V_1(B) = F, \quad V_1(C)$ arbitrary

$$= \begin{cases} V_{1a}(A) = F, & V_{1a}(B) = F, & V_{1a}(C) = T \\ V_{1b}(A) = F, & V_{1b}(B) = F, & V_{1b}(C) = F \end{cases}$$

V_1 gives us 2 valuations : V_{1a} & V_{1b}

first branch

	A	B	C	ϕ
V_{1a}	F	F	T	F
V_{1b}	F	F	F	F

$V_2(C) = F$

$V_2(A) = V_2(B) =$ arbitrary

Here we get 4 valuations : V_{2a}, V_{2b}, V_{2c} & V_{2d}

second branch

	A	B	C	ϕ
V_{2a}	T	T	F	F
V_{2b}	T	F	F	F
V_{2c}	F	T	F	F
V_{2d}	F	F	F	F

$$\phi = \Big(\big((C \to (M \vee \neg A)) \wedge (\neg A \to P) \wedge (P \to M)\big) \to (C \to M)\Big)$$

Show that ϕ is a tautology

① $\neg\phi$

② $C \to (M \vee \neg A)$

③ $(\neg A \to P)$

④ $(P \to M)$

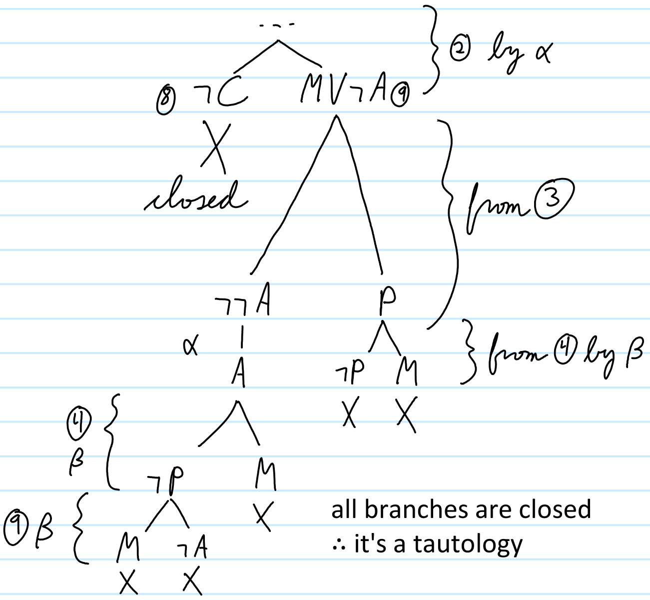
⑤ $\neg(C \to M)$

(② – ⑤: from ①, by α-rule)

⑥ C

⑦ $\neg M$

(⑥ – ⑦: from ⑤ by α-rule)



all branches are closed

∴ it's a tautology

Notation for truth trees

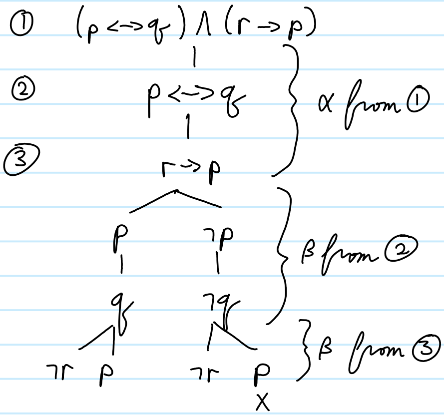
$(A \vee B \vee C)$ will mean associativity to left; $((A \vee B) \vee C)$

② Finding DNFs for ϕ

Draw tree for ϕ

$$\bigvee_{\text{open branches}} \bigwedge_{\text{literals on open branches}} = DNF_\phi$$

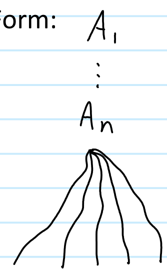
$\phi = (p \leftrightarrow q) \wedge (r \rightarrow p)$
Find DNF$_\phi$



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

branch 1 — branch 2 — branch 3

Consistency of $\{A_1, \ldots, A_n\}$
Form:



We look for open branches

27.01.16

January 27, 2016 11:32 AM

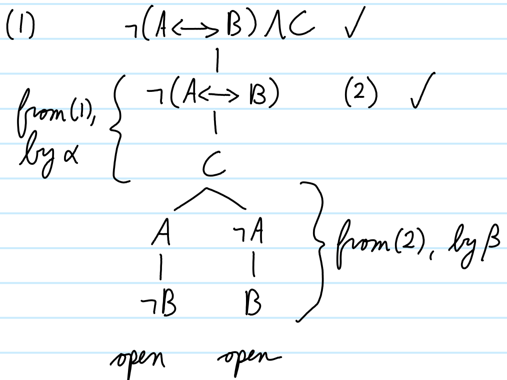
Truth trees can be used for

- finding tautologies (including validity of arguments)
- finding DNFs
- consistency of sets of formulas

Example:

Find a DNF of $\phi = \neg(A \leftrightarrow B) \wedge C$

① Put ϕ at the top of the tree (NOT $\neg\phi$, which is only for checking tautologies)
② Draw the complete truth tree
③ Ignore closed branches, conjunct the literals on each open branch to get a clause and disjunct all clauses (from open branches)

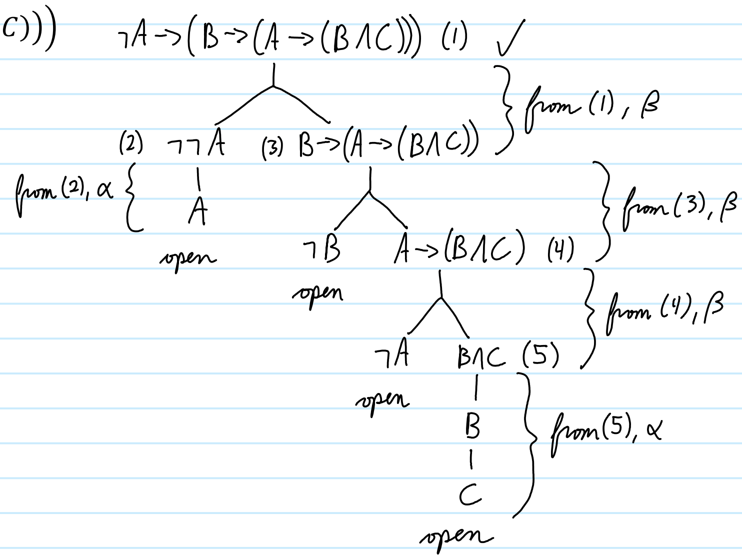


clause 2 : $((B \wedge \neg A) \wedge C)$

clause 1 : $(\neg B \wedge A) \wedge C$

DNF : clause 1 ∨ clause 2
$((\neg B \wedge A) \wedge C) \vee ((B \wedge \neg A) \wedge C)$

Find DNF of $\phi = \neg A \rightarrow \big(B \rightarrow (A \rightarrow (B \wedge C))\big)$



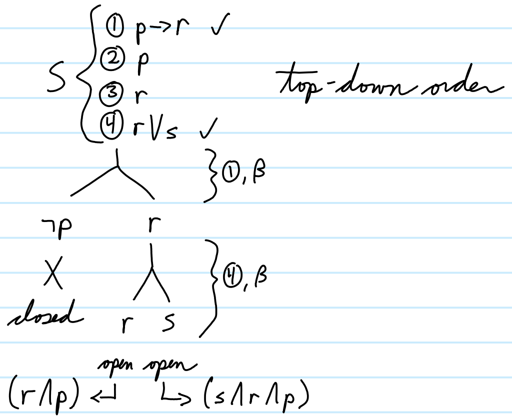
DNF : $((A \vee \neg B) \vee \neg A) \vee (B \wedge C)$
$\equiv (A \vee \neg B \vee \neg A) \vee (B \wedge C)$
$\equiv (T \vee \neg B) \vee (B \wedge C)$
$\equiv T \vee (B \wedge C)$
$\equiv T$

Consistency: $S = \{A_1, \dots, A_n\}$ is consistent if and only if $A_1 \wedge \cdots \wedge A_n$ is satisfiable
i.e. on some row of the truth table, the value $V(A_1 \wedge \cdots \wedge A_n) = \text{T}$ if and only if there's some valuation V so that $V(A_1) = V(A_2) = \cdots = V(A_n) = \text{T}$.

To check if S is consistent, $S = \{A_1, \dots, A_n\}$:

- Put S at the top of the tree and draw the complete truth tree
- We search for at least one open branch
- If there is at least one open branch, S is consistent on that branch

Example: $S = \{p \to r, p, r, r \vee s\}$



DNF: $(r \wedge p) \vee (s \wedge r \wedge p)$

Valuation making S true:
V_1 = clause 1: $V_1(r) = \text{T}$, $V_1(p) = \text{T}$, $V_1(s)$ = arbitrary
V_2 = clause 2: $V_2(p) = V_2(r) = V_2(s) = T$

$$V_{1a} = \begin{Bmatrix} p = \text{T} \\ r = \text{T} \\ s = \text{T} \end{Bmatrix} = V_2$$

$$V_{1b} = \begin{cases} p = \text{T} \\ r = \text{T} \\ s = \text{F} \end{cases}$$

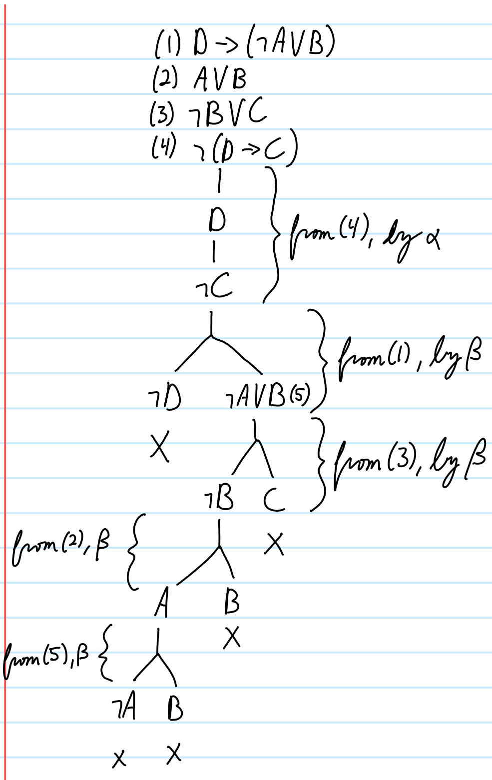
To check if ϕ is a tautology by truth trees, draw complete truth tree for $\neg\phi$.
① If every branch is closed, ϕ is a tautology
② If there are open branches, ϕ is not a tautology and the open branches to valuations V where $V(\neg\phi) = \text{T}$ i.e. $V(\phi) = \text{F}$.

$$\left.\begin{array}{l} H_1 \\ H_2 \\ \vdots \\ \underline{H_n} \\ \therefore C \end{array}\right\}$$ This argument is valid if $(H_1 \wedge H_2 \wedge \cdots \wedge H_n) \to C$ is a tautology

$$\neg\big((H_1 \wedge H_2 \wedge \cdots \wedge H_n) \to C\big) \equiv H_1 \wedge \cdots \wedge H_n \wedge \neg C$$

Method: Draw the tree for $\begin{array}{l} H_1 \\ H_2 \\ \vdots \\ \underline{H_n} \\ \therefore C \end{array}$

$$\left.\begin{array}{r} D \to \neg A \vee B \\ A \vee B \\ \underline{\neg B \vee C} \\ \therefore D \to C \end{array}\right]$$ – is this valid?



The argument is valid: every branch is closed (①∧②∧③ → ④ is a tautology)

<u>Formal proofs</u> (à la Rosen)

A formal proof is a list of formulas ($A_1, A_2, \ldots, A_k$) where each formula is either a **hypothesis** or follows from previous formulas by a **rule**.

A_1 (hypothesis)
A_2 (hypothesis or rule from previous lines)
A_3
$\vdots$
$A_\ell =$ conclusion of theorem (rule)

A proof is
A_1 justification
A_2 justification
$\vdots$
A_ℓ justification

Rule (Modus Ponens):
p (hypothesis)
$\underline{p \rightarrow q}$ (hypothesis)
$\therefore q$ (conclusion)

1. p (hypothesis)
2. $p \rightarrow q$ (hypothesis)
3. q (Modus Ponens, from line 1 and 2)

Rosen also allows Boolean equivalences

Logical argument	Tautology	Name
p $\underline{p \to q}$ $\therefore q$	$(p \land (p \to q)) \to q$	Modus Ponens
$p \to q$ $\underline{\neg q}$ $\therefore \neg p$	$((p \to q) \land \neg q) \to \neg p$	Rule of contraposition OR Modus Tollens
$p \to q$ $\underline{q \to r}$ $\therefore p \to r$	$(p \to q) \land (q \to r) \to (p \to r)$	Hypothetical syllogism OR transitivity of implication
$p \lor q$ $\underline{\neg p}$ $\therefore q$	$((p \lor q) \land \neg p) \to q$	Disjunctive syllogism
$\underline{p \land q}$ $\therefore p$	$(p \land q) \to p$	$\land -$ elimination

Prove

$\underline{p \land q}$

$\therefore q$

1. $p \land q$ (hypothesis)
2. $q \land p$ (Boolean equivalence, line 1)
3. q ($\land -$ elimination, line 2)

— Rosen-style proof

01.02.16

February 1, 2016 12:59 PM

Logical argument	Tautology	Name
p $\underline{q}$ $\therefore p \wedge q$	$(p \wedge q) \to (p \wedge q)$ or $p \to (q \to (p \wedge q))$	$\wedge -$ introduction
$p \vee q$ $\underline{\neg p \vee r}$ $\therefore q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \to q \vee r$	Resolution (or cut) rule

Heuristic: we can only prove valid arguments by Rosen Rules.

So, to prove an argument (using Rosen's Rules) is formally valid, it is a good idea to check that it is a valid argument before starting.

Where

$$\left.\begin{matrix} H_1 \\ H_2 \\ \vdots \\ \underline{H_n} \\ \therefore C \end{matrix}\right\}$$ is valid means $(H_1 \wedge H_2 \wedge \cdots \wedge H_n) \to C$ is a tautology.

$\underline{\neg(p \vee q)}$
$\therefore p \to q$

1. $\neg(p \vee q)$ hypothesis
2. $\neg p \wedge \neg q$ De Morgan's Law, from line 1
3. $\neg p$ $\wedge -$ elimination, from line 2
4. $\neg p \vee q$ $\vee -$ introduction, from line 3
5. $p \to q$ Boolean equivalence, from line 4

Now let's try to prove it using words.

Is $\neg(p \vee q) \to (p \to q)$ a tautology? Suppose it's false.
Since it's an implication, $\neg(p \vee q)$ must be True and $(p \to q)$ must be False.
Hence the value $V(p \to q) =$ F, which means that $V(p) =$ T and $V(q) =$ F.
$\therefore V(p \vee q) =$ T $\vee$ F $=$ T
$\therefore V(\neg(p \vee q)) =$ F. But we assumed $\neg(p \vee q) =$ T $\Rightarrow$ contradiction.

<u>Styles of math proofs</u>

<u>Direct proof</u>: starts with hypotheses and definitions and directly proves the conclusion.

Definitions:
$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ integers
$\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ positive integers
$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ naturals numbers
$\mathbb{Q} = \left\{\frac{m}{n} \middle| m, n \in \mathbb{Z}, n \neq 0\right\}$ rational numbers

$m \in \mathbb{Z}$ is even if $m = 2k$, for some $k \in \mathbb{Z}$
$m \in \mathbb{Z}$ is odd if $m = 2k + 1$, for some $k \in \mathbb{Z}$

Directly prove the fact "if m is odd, then $m+1$ is even".
Proof: suppose m is odd: $\therefore m = 2k+1$ for some $k \epsilon \mathbb{Z}$
$\therefore m+1 = (2k+1)+1 = 2k+2 = 2(k+1)$
$\therefore m+1$ is even

Proposition: n is odd $\Rightarrow n^2$ is odd, $n \epsilon \mathbb{Z}$
Proof: suppose n is odd, so by definition $n = 2k+1$, for some $k \epsilon \mathbb{Z}$
$\therefore n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$
$\therefore n^2$ is odd

2 other methods for proof:

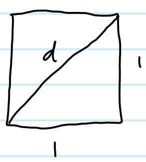
- Method of contradiction:
  To prove p, suppose $\neg p$ as a hypothesis and get a contradiction.
  $\therefore p$ is True
  (that is equivalent to saying $(\neg p \to \mathrm{F}) \equiv p$
- Method of contrapositive
  To prove $p \to q$, just prove $\neg q \to \neg p$ since $p \to q \equiv \neg q \to \neg p$.

Theorem: If n^2 is even, then n is even.
Proof: we prove the contrapositive
$\neg(n$ is even$) \to \neg(n^2$ is even$)$
i.e. we must proof that if n is odd, n^2 is odd
see previous example

Method of contradiction (small variation of method of contrapositive)
To prove $p \to q$, suppose p and $\neg q$ are true.
Get a contradiction, $\therefore$ it must be that $p \to q$

Theorem: if n^2 is even, then n is even
Proof by contradiction: suppose n^2 is even but $\neg(n$ is even$)$.
$\therefore n$ is odd, $\therefore n = 2k+1$ for some k, $\therefore n^2 = (2k+1)^2 = 2(2k^2+2k)+1$ is odd (contradiction)

Styles of math proofs



$d = \sqrt{2}$
Theorem: $\sqrt{2} \notin \mathbb{Q}$

A fraction is in lowest form if you factor out any common divisor of numerator and denominator, i.e. $\frac{6}{8} = \frac{3}{4}$.
Proof (by contradiction):
Suppose $\sqrt{2} = \frac{m}{n}$, where $\frac{m}{n}$ is in lowest terms.
Square both sides: $2 = \frac{m^2}{n^2}$, $\therefore m^2 = 2n^2$, $\therefore m^2$ is even.
So by the theorem, m is even, $\therefore m = 2k$ for some k
$m^2 = 4k^2 \Rightarrow 2n^2 = 4k^2 \Rightarrow n^2 = 2k^2$, $\therefore n^2$ is even.
So again by the theorem, n is even; 2 is a common factor $\Rightarrow$ contradiction

Proof by cases:
Based on logical principle
$\big((A \lor B) \to C\big) \equiv \big((A \to C) \land (B \to C)\big)$

If $A \lor B$ is exclusive and covers all cases, then from $A \to C$ and $B \to C$ and the truth of $A \lor B$ we can prove C.
For example, if $A \lor B$ says "either A is a knight or A is a knave".

Three people A, B and C on the island of knights and knaves.
Suppose A says "all of us are knaves" and B says "exactly one of us is a knave".
Prove: C must be a knight

Proof: by cases

Case 1: A is a knight
∴ he speaks True
∴ they are all knaves ⇒ contradiction

Case 2: A is a knave
Subcase 2.1: B is a knight: ∴ B speaks True,
∴ there's only one knave and it must be A, therefore C is a knight

Subcase 2.2: B is a knave: A, B both lie, B's statement is consistent but A lies
∴ not all of them are knaves
∴ C must be the knight

In conclusion: C is a knight

Exercise: redo the above using the cases:

Case 1: B is a knight
Case 2: B is a knave

Again prove: (Case 1 ∨ Case 2) → C is a knight by proving:
(Case 1 → C is a knight) ∧ (Case 2 → C is a knight) and notice that (Case 1 ∨ Case 2) is always True.

03.02.16

February 3, 2016 11:30 AM

Methods of proof: direct proofs, indirect proofs (= contraposition), contradiction, proof by cases and a mixture of these (all proofs in words, written mathematics but using the logical forms we've already seen)

c.f. Rosen §1.7 and 1.8

Direct proof

Proposition: if q, q' are rational, then $q \cdot q'$ is rational.

Proof:
q rational means $q = \frac{m}{n}$ for some $m, n \in \mathbb{Z}, n \neq 0$ and
q' rational means $q' = \frac{m'}{n'}$ for some $m', n' \in \mathbb{Z}, n' \neq 0$, then
$q \cdot q' = \left(\frac{m}{n}\right) \cdot \left(\frac{m'}{n'}\right) = \frac{mm'}{nn'} \in \mathbb{Q}$
Note: $nn' \neq 0$ (why?)

Recall: $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$
To prove $p \leftrightarrow q$, you must prove $p \to q$ and $q \to p$.
Let $m, n \in \mathbb{Z}^+$, we say m (evenly) divides n if $n = km$ for some $k \in \mathbb{Z}^+$.
m divides n if n is a multiple of m.

$5 \mid 10$ is 5 divides 10
$2 \mid 6$ is 2 divides 6
$3 \mid 6$ is 3 divides 6

$10 \nmid 13$ is 10 does not divide 13
$7 \nmid 15$ is 7 does not divide 15

Standard notation: $m \mid n$ means m divide n (NOT $\frac{n}{m}$)

Theorem: Let $m, n \in \mathbb{Z}^+$, then $m = n$ (this will be the LHS) iff $m \mid n$ **and** $n \mid m$ (this will be the RHS).

Proof (⇒): Suppose LHS
Then $m = n$; we must prove $m \mid m$ and $n \mid n$.
Clearly $m = 1 \cdot m$
$\therefore$ there is a $k \in \mathbb{Z}^+$ (namely $k = 1$) such that $m = k \cdot m$
Summary: LHS true means we reduce the RHS to the problem of asking if $x \mid x$ for any x (which is trivially True)

Proof (⇐): Suppose RHS
$\therefore m \mid n$ and $n \mid m$
If $m \mid n$, then for some $k \in \mathbb{Z}^+$, $n = km$, and
if $n \mid m$, then for some $k' \in \mathbb{Z}^+$, $m = k'n$.
$\therefore n = km = kk'n$. In $\mathbb{Z}^+$, kk' must equal 1.
But in $\mathbb{Z}^+$, if $kk' = 1$, then $k = k' = 1$.
$\therefore n = m$

$$\left.\begin{array}{l} H_1 \\ H_2 \\ \vdots \\ \underline{H_n} \\ \therefore C \end{array}\right\} \text{is valid if } (H_1 \wedge H_2 \wedge \cdots H_n) \to C \text{ is a tautology.}$$

→ here, any kind of tautology if OK; the argument is still valid

Theorem:
If $0 > 1$, then $\sqrt{2}$ is rational.
This is valid because $0 > 1$ is false.
So $(0 > 1) \rightarrow (\sqrt{2} \epsilon \mathbb{Q})$ is a tautology.

Theorem:
Let $p(x) = x^2 + x + 1$ be a polynomial.
Then $p(x)$ has no positive rational roots.

Reminder:
A root of $p(x)$ is a number r where $p(r) = 0$.

Proof (by contradiction and by cases):

Reminder:
A proof of
H_1
H_2
$\vdots$
$\underline{H_n}$
$\therefore C$
by contradiction says: suppose the hypotheses are all True and C is false; look for a contradiction. If you get a contradiction $\Rightarrow \therefore (H_1 \wedge H_2 \wedge \cdots \wedge H_n) \rightarrow C$ is always True.

An indirect proof is a proof by contrapositive. To prove $H \rightarrow C$ instead prove $\neg C \rightarrow \neg H$ (contrapositive).

Proof:
Suppose $p(r) = 0$ and suppose $r \epsilon \mathbb{Q}^+$. Get a contradiction.
Say $r = \frac{m}{n} > 0$ (in lowest terms), so $p\left(\frac{m}{n}\right) = 0$. Get a contradiction.

Case 1: $m > 0, n > 0, r = \frac{m}{n}$
$p(r) = 0$
$\therefore r^2 + r + 1 = 0$
$\therefore \left(\frac{m}{n}\right)^2 + \frac{m}{n} + 1 = 0$
$\therefore \frac{m^2}{n^2} + \frac{m}{n} + 1 = 0$
Multiply each side by n^2:
$m^2 + mn + n^2 = 0$
But $m^2 > 0, n^2 > 0$ and $mn > 0$
$\therefore$ the sum is not equal to 0 $\Rightarrow$ contradiction

Case 2: $m < 0, n < 0, r = \frac{m}{n}$
$\therefore$ we proceed as in case 1, we get $m^2 + mn + n^2 = 0$
$m^2 > 0, n^2 > 0$ and $mn > 0$ since it's the product of two non-zero negative integers $\Rightarrow$ same contradiction

Logical form of above
Let P be $p(r) = 0$ for some positive rational $\frac{m}{n}$

Case 1: $m, n > 0$: we proved case 1 $\rightarrow$ False
Case 2: $m, n < 0$: we proved case 2 $\rightarrow$ False

Notice (Case 1 $\vee$ Case 2) is True. Hence, overall, we conclude False (i.e. a contradiction)

i.e. we suppose there is a positive rational root and get a contradiction

Case 1 ∨ Case 2
Case 1 → F
Case 2 → F
∴ F

$$\big((A \vee B) \to C\big) \equiv \big((A \to C) \wedge (B \to C)\big)$$

$A \vee B$
$A \to C$
$B \to C$
$\therefore C$

Prove by contradiction: if x is irrational, then $\frac{1}{x}$ is irrational

Proof:
Suppose x is irrational and $\frac{1}{x}$ is rational
Find a contradiction
If $\frac{1}{x}$ is rational, then $\frac{1}{x} = \frac{m}{n}$ for some $m, n \in \mathbb{Z}, n \neq 0$
$\therefore x = \frac{1}{m/n} = \frac{n}{m} \in \mathbb{Q}$ (since $m \neq 0$, why?) (since $\frac{1}{0}$ is not defined, just like $\frac{1}{1/0}$)
Contradiction!

Exercise: give an indirect proof

Set theory:
Sets are the collections of "elements" or "individuals" — foundation of modern mathematics.

Several classes of sets:
① Finite set: $\{x_1, x_2, \ldots, x_n\} \Rightarrow$ the set consists of distinct elements $x_1, x_2, \ldots, x_n$.
More examples: {■,★, !}, {🍌, 1, ☐}

Empty set (or null set): it's a finite set with 0 elements denoted by $\emptyset$. Do not write { } (too confusing).

$\{1, 1, 5\}$ is the same set as $\{1, 5\}$.
But they are different lists or different multisets.

$A = B$ (two sets) if they have the same elements.