Discrete Mathematics: Lecture 18

logically equivalent, rule of replacement, tautological implications

Xuming He
Associate Professor

School of Information Science and Technology
ShanghaiTech University

Spring Semester, 2022

Notes by Prof. Liangfeng Zhang

(continue from last lec)

Logically Equivalent

THEOREM: Let $A^{-1}(\mathbf{T})$ be the set of truth assignments such that A is true. Then $A \equiv B$ if and only if $A^{-1}(\mathbf{T}) = B^{-1}(\mathbf{T})$.

- $A \equiv B$ if and only if $A^{-1}(\mathbf{F}) = B^{-1}(\mathbf{F})$

Just a sign

A/B truch assign set equal

False

same space

(same var list)

Proving $A \equiv B$

EXAMPLE: $P \wedge Q \equiv Q \wedge P$ **//commutative law**

- <u>Idea: Show that $A^{-1}(\mathbf{T}) = B^{-1}(\mathbf{T})$.</u>
- $A = P \wedge Q; B = Q \wedge P$
  - $A = \mathbf{T}$ if and only if $(P, Q) = (\mathbf{T}, \mathbf{T})$
    - $A^{-1}(\mathbf{T}) = \{(\mathbf{T}, \mathbf{T})\}$
  - $B = \mathbf{T}$ if and only if $(Q, P) = (\mathbf{T}, \mathbf{T})$
    - $B^{-1}(\mathbf{T}) = \{(\mathbf{T}, \mathbf{T})\}$
- $A^{-1}(\mathbf{T}) = B^{-1}(\mathbf{T})$
- $A \equiv B$

REMARK: $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$ can be shown similarly.

- **Associative law**

Proving $A \equiv B$

EXAMPLE: $P \vee Q \equiv Q \vee P$ **//commutative law**

- Idea: Show that $A^{-1}(\mathbf{F}) = B^{-1}(\mathbf{F})$.
- $A = P \vee Q$; $B = Q \vee P$ prove with F better
  - $A = \mathbf{F}$ if and only if $(P, Q) = (\mathbf{F}, \mathbf{F})$
    - $A^{-1}(\mathbf{F}) = \{(\mathbf{F}, \mathbf{F})\}$
  - $B = \mathbf{F}$ if and only if $(Q, P) = (\mathbf{F}, \mathbf{F})$
    - $B^{-1}(\mathbf{F}) = \{(\mathbf{F}, \mathbf{F})\}$
- $A^{-1}(\mathbf{F}) = B^{-1}(\mathbf{F})$
- $A \equiv B$

REMARK: $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$ can be shown similarly.

- **Associative law**

Tautological Implications

DEFINITION: Let A and B be WFFs in propositional variables $p_1, \ldots, p_n$.

- A **tautologically implies** (重言蕴涵) B if every truth assignment that causes A to be true causes B to be true.
  - Notation: $A \Rightarrow B$, called a **tautological implication**
  - $A^{-1}(\mathbf{T}) \subseteq B^{-1}(\mathbf{T})$; $B^{-1}(\mathbf{F}) \subseteq A^{-1}(\mathbf{F})$

diff

$\Rightarrow$

$\rightarrow$

THEOREM: $A \Rightarrow B$ iff $A \rightarrow B$ is a tautology.

- $A \Rightarrow B$ iff $A^{-1}(\mathbf{T}) \subseteq B^{-1}(\mathbf{T})$ iff $A \rightarrow B$ is a tautology

T for all truth assign

THEOREM: $A \Rightarrow B$ iff $A \wedge \neg B$ is a contradiction.

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

Proving $A \Rightarrow B$: (1) $A^{-1}(\mathbf{T}) \subseteq B^{-1}(\mathbf{T})$; (2) $B^{-1}(\mathbf{F}) \subseteq A^{-1}(\mathbf{F})$;

(3) $A \rightarrow B$ is a tautology; (4) $A \wedge \neg B$ is a contradiction

{ tautologically imply
tautology.

Proving $A \Rightarrow B$

$B = q$

since no matter p.

EXAMPLE: Show the tautological implication "$p \wedge (p \to q) \Rightarrow q$".

- Let $A = p \wedge (p \to q)$; $B = q$. Need to show that "$A \Rightarrow B$"
- $A^{-1}(\mathbf{T}) = \{(\mathbf{T}, \mathbf{T})\}$; $B^{-1}(\mathbf{T}) = \{(\mathbf{T}, \mathbf{T}), (\mathbf{F}, \mathbf{T})\}$: $A^{-1}(\mathbf{T}) \subseteq B^{-1}(\mathbf{T})$.

p	q	$p \to q$	A	B
T	**T**	**T**	**T**	**T**
T	**F**	**F**	**F**	**F**
F	**T**	**T**	**F**	**T**
F	**F**	**T**	**F**	**F**

- $A \to B \equiv \neg\big(p \wedge (p \to q)\big) \vee q$
  $\equiv \big(\neg p \vee \neg(p \to q)\big) \vee q$
  $\equiv (\neg p \vee q) \vee \neg(p \to q)$
  $\equiv (p \to q) \vee \neg(p \to q)$
  $\equiv \mathbf{T}$

iff $A \to B$ is T

- $A \wedge \neg B \equiv \big(p \wedge (p \to q)\big) \wedge \neg q$
  $\equiv (\neg q \wedge p) \wedge (p \to q)$
  $\equiv \neg(p \to q) \wedge (p \to q)$
  $\equiv \mathbf{F}$

iff $A \wedge \neg B$ is F

① $A = \cdots$ $B = \cdots$

② $A \to B$ T / $A \wedge \neg B$ F / {t f}

Tauto rules

Tauto rules

Tautological Implications

Name	Tautological Implication	NO.
Conjunction(合取)	$(P) \wedge (Q) \Rightarrow P \wedge Q$	1
Simplification(化简)	$P \wedge Q \Rightarrow P$	2
Addition(附加)	$P \Rightarrow P \vee Q$	3
Modus ponens(假言推理)	$P \wedge (\overset{\neg P \vee Q}{P \to Q}) \Rightarrow Q$	4
Modus tollens(拒取)	$\neg Q \wedge (\overset{\neg P \vee Q}{P \to Q}) \Rightarrow \neg P$	5
Disjunctive syllogism(析取三段论)	$\neg P \wedge (P \vee Q) \Rightarrow Q$	6
Hypothetical syllogism(假言三段论)	$(\overset{\neg P \vee Q}{P \to Q}) \wedge (\overset{\neg Q \vee R}{Q \to R}) \Rightarrow (\overset{\neg P \vee R}{P \to R})$	7
Resolution (归结)	$(P \vee Q) \wedge (\neg P \vee R) \Rightarrow Q \vee R$	8

Proofs for 5 and 6

EXAMPLE: $\neg Q \wedge (P \to Q) \Rightarrow \neg P$

- $A = \neg Q \wedge (P \to Q), B = \neg P.$
- $A \to B \equiv \neg\big(\neg Q \wedge (P \to Q)\big) \vee \neg P$

$$\equiv \big(Q \vee \neg(P \to Q)\big) \vee \neg P$$

$$\equiv (\neg P \vee Q) \vee \underbrace{\neg(P \to Q)}_{\neg(\neg P \vee Q)}$$

$$\equiv \mathbf{T}$$

EXAMPLE: $\neg P \wedge (P \vee Q) \Rightarrow Q$

- $A = \neg P \wedge (P \vee Q), B = Q.$
- $A \to B \equiv \neg\big(\neg P \wedge (P \vee Q)\big) \vee Q$

$$\equiv \big(P \vee \neg(P \vee Q)\big) \vee Q$$

$$\equiv (\neg(P \vee Q) \vee P) \vee Q$$

$$\equiv \neg(P \vee Q) \vee (P \vee Q)$$

$$\equiv \mathbf{T}$$

Proofs for 7 and 8

EXAMPLE: $(P \to Q) \land (Q \to R) \Rightarrow P \to R$

- $A = (P \to Q) \land (Q \to R);\ B = (P \to R).$
- $A \land \neg B \equiv (\neg P \lor Q) \land (\neg Q \lor R) \land (P \land \neg R)$

$$\equiv \big((\neg P \lor Q) \land P\big) \land \big((\neg Q \lor R) \land \neg R\big)$$

$$\equiv \big((\neg P \land P) \lor (Q \land P)\big) \land \big((\neg Q \land \neg R) \lor (R \land \neg R)\big)$$

$$\equiv (Q \land P) \land (\neg Q \land \neg R)$$

$$\equiv \mathbf{F}$$

EXAMPLE: $(P \lor Q) \land (\neg P \lor R) \Rightarrow Q \lor R$

- $A = (P \lor Q) \land (\neg P \lor R); B = (Q \lor R).$
- $A \land \neg B \equiv (P \lor Q) \land (\neg P \lor R) \land (\neg Q \land \neg R)$

$$\equiv \big((P \lor Q) \land \neg Q\big) \land ((\neg P \lor R) \land \neg R)$$

$$\equiv (P \land \neg Q) \land (\neg P \land \neg R)$$

$$\equiv \mathbf{F}$$

More Examples

CNF

EXAMPLE: $(P \leftrightarrow Q) \wedge (Q \leftrightarrow R) \Rightarrow (P \leftrightarrow R)$

- $A = (P \leftrightarrow Q) \wedge (Q \leftrightarrow R)$; $B = (P \leftrightarrow R)$.
- $A = \mathbf{T}$ iff $(P \leftrightarrow Q) = \mathbf{T}$ and $(Q \leftrightarrow R) = \mathbf{T}$ iff $P = Q$ and $Q = R$
  - $A^{-1}(\mathbf{T}) = \{(\mathbf{T}, \mathbf{T}, \mathbf{T}), (\mathbf{F}, \mathbf{F}, \mathbf{F})\}$
- $B = \mathbf{T}$ iff $P = R$ T, F
  - $B^{-1}(\mathbf{T}) = \{(\mathbf{T}, \mathbf{T}, \mathbf{T}), (\mathbf{T}, \mathbf{F}, \mathbf{T}), (\mathbf{F}, \mathbf{T}, \mathbf{F}), (\mathbf{F}, \mathbf{F}, \mathbf{F})\}$
- $A^{-1}(\mathbf{T}) \subseteq B^{-1}(\mathbf{T})$

EXAMPLE: $(Q \rightarrow R) \Rightarrow ((P \vee Q) \rightarrow (P \vee R))$

- $A = Q \rightarrow R$; $B = ((P \vee Q) \rightarrow (P \vee R))$.
- $A = \mathbf{F}$ iff $(Q, R) = (\mathbf{T}, \mathbf{F})$
  - $A^{-1}(\mathbf{F}) = \{(\mathbf{T}, \mathbf{T}, \mathbf{F}), (\mathbf{F}, \mathbf{T}, \mathbf{F})\}$
- $B = \mathbf{F}$ iff $(P \vee Q, P \vee R) = (\mathbf{T}, \mathbf{F})$ iff $(P, Q) \neq (\mathbf{F}, \mathbf{F})$ and $(P, R) = (\mathbf{F}, \mathbf{F})$
  - $B^{-1}(\mathbf{F}) = \{(\mathbf{F}, \mathbf{T}, \mathbf{F})\}$
- $A^{-1}(\mathbf{F}) \supseteq B^{-1}(\mathbf{F})$

inverse!

More Examples

EXAMPLE: $(P \to R) \wedge (Q \to S) \wedge (P \vee Q) \Rightarrow R \vee S$

- $A = (P \to R) \wedge (Q \to S) \wedge (P \vee Q)$; $B = R \vee S$
- $A \wedge \neg B \equiv (P \to R) \wedge (Q \to S) \wedge (P \vee Q) \wedge \neg(R \vee S)$

$$\equiv (\neg P \vee R) \wedge (\neg Q \vee S) \wedge (P \vee Q) \wedge (\neg R \wedge \neg S)$$
$$\equiv ((\neg P \vee R) \wedge \neg R)) \wedge ((\neg Q \vee S) \wedge \neg S) \wedge (P \vee Q)$$
$$\equiv ((\neg P \wedge \neg R) \vee (R \wedge \neg R)) \wedge ((\neg Q \wedge \neg S) \vee (S \wedge \neg S)) \wedge (P \vee Q)$$
$$\equiv ((\neg P \wedge \neg R) \vee \mathbf{F}) \wedge ((\neg Q \wedge \neg S) \vee \mathbf{F}) \wedge (P \vee Q)$$
$$\equiv (\neg P \wedge \neg R) \wedge (\neg Q \wedge \neg S) \wedge (P \vee Q)$$
$$\equiv \neg R \wedge (\neg Q \wedge \neg S) \wedge (\neg P \wedge (P \vee Q))$$
$$\equiv \neg R \wedge (\neg Q \wedge \neg S) \wedge ((\neg P \wedge P) \vee (\neg P \wedge Q))$$
$$\equiv \neg R \wedge (\neg Q \wedge \neg S) \wedge (\mathbf{F} \vee (\neg P \wedge Q))$$
$$\equiv \neg R \wedge (\neg Q \wedge \neg S) \wedge (\neg P \wedge Q)$$
$$\equiv \neg R \wedge \neg S \wedge \neg P \wedge (\neg Q \wedge Q)$$
$$\equiv \neg R \wedge \neg S \wedge \neg P \wedge \mathbf{F}$$
$$\equiv \mathbf{F}$$