Discrete Mathematics: Lecture 16

Part III. Mathematical Logic

truth table, tautology, contradiction, contingency,

satisfiable, rule of substitution, logically equivalent, rule of replacement

Xuming He
Associate Professor

School of Information Science and Technology
ShanghaiTech University

Spring Semester, 2025

Notes by Prof. Liangfeng Zhang and Xuming He

Review

Proposition: a declarative sentence that is either true or false.

- simple, compound, propositional constant/variable

Logical Connectives: $\neg$ (unary), $\wedge, \vee, \rightarrow, \leftrightarrow$ (binary)

- Truth table

Well-Formed Formulas (WFFs): formulas

- propositional constants (T, F) and propositional variables are WFFs
- $\neg A, (A \wedge B), (A \vee B), (A \leftarrow B), (A \leftrightarrow B)$
- Finite

Review: From Natural Language to WFFs

The Method of Translation:

- Introduce symbols p, q, r … to represent simple propositions
- Connect the symbols with logical connectives to obtain WFFs

EXAMPLE:

- "小明去过苏州或者杭州."
  - p:"小明去过苏州."; q:"小明去过杭州." Translation: $p \vee q$
- "虽然天气很冷, 可人们情绪很高."
  - p:"天气很冷."; q:"人们情绪很高." Translation: $p \wedge q$
- "只要小红努力学习, 她就会取得好成绩."
  - p:"小红努力学习"; q:"小红取得好成绩" Translation: $p \rightarrow q$
- "只有小红努力学习, 她才能取得好成绩."
  - p:"小红努力学习"; q:"小红取得好成绩" Translation: $q \rightarrow p$

Q1

Scenario:

Three students (P, Q, R) are deciding whether to join a study group. Which formula correctly translates the following conditions?

Conditions:

1. P joins **if and only if** Q does not join.
2. **If** R joins, **then** both P and Q must join.
3. **Either** P joins **or** R joins, **but not both**.

Variables:

- p: "P joins the study group."
- q: "Q joins the study group."
- r: "R joins the study group."

Options:

A. $(p \leftrightarrow \neg q) \wedge (r \rightarrow (p \wedge q)) \wedge ((p \vee r) \wedge \neg(p \wedge r))$

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

C. $(p \leftrightarrow \neg q) \wedge (r \rightarrow (p \vee q)) \wedge (p \oplus r)$

D. $(p \leftrightarrow \neg q) \vee (r \rightarrow (p \wedge q)) \vee \neg(p \wedge r)$

Q2

Question: According to the definition of Well-Formed Formulas (WFFs), is the expression **¬(p ∨ ¬q)** a valid WFF?

Options:

- ✅ Yes
- ❌ No

Truth Table

DEFINITION: Let F be a WFF of $p_1, \dots, p_n$, n propositional variables

- A **truth assignment** (真值指派) for F is a map $\alpha: \{p_1, \dots, p_n\} \to \{\mathbf{T}, \mathbf{F}\}$.
  - There are 2^n different truth assignments.

p_1	p_2	$\cdots$	p_n	F
T	**T**	$\cdots$	**T**	$\cdot$
T	**T**	$\cdots$	**F**	$\cdot$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
F	**F**	$\cdots$	**F**	$\cdot$

EXAMPLE: Truth tables of $A = p \vee \neg p, B = p \wedge \neg p, C = p \to \neg p$

p	$\neg p$	A
T	**F**	
F	**T**	

p	$\neg p$	B
T	**F**	
F	**T**	

p	$\neg p$	C
T	**F**	
F	**T**	

Truth Table

DEFINITION: Let F be a WFF of $p_1, \dots, p_n$, n propositional variables

- A **truth assignment** (真值指派) for F is a map $\alpha: \{p_1, \dots, p_n\} \to \{\mathbf{T}, \mathbf{F}\}$.
  - There are 2^n different truth assignments.

p_1	p_2	$\cdots$	p_n	F
T	**T**	$\cdots$	**T**	$\cdot$
T	**T**	$\cdots$	**F**	$\cdot$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
F	**F**	$\cdots$	**F**	$\cdot$

EXAMPLE: Truth tables of $A = p \vee \neg p, B = p \wedge \neg p, C = p \to \neg p$

p	$\neg p$	A
T	**F**	**T**
F	**T**	**T**

p	$\neg p$	B
T	**F**	**F**
F	**T**	**F**

p	$\neg p$	C
T	**F**	**F**
F	**T**	**T**

Truth Table

EXAMPLE: Truth table of $F = (p \rightarrow q) \wedge (q \rightarrow r) \leftrightarrow (p \rightarrow r)$

- $A = p \rightarrow q; B = q \rightarrow r;\ C = p \rightarrow r$
- $F = A \wedge B \leftrightarrow C$

p	q	r	A	B	C	$A \wedge B$	F
T	**T**	**T**					
T	**T**	**F**					
T	**F**	**T**					
T	**F**	**F**					
F	**T**	**T**					
F	**T**	**F**					
F	**F**	**T**					
F	**F**	**F**					

Truth Table

EXAMPLE: Truth table of $F = (p \to q) \wedge (q \to r) \leftrightarrow (p \to r)$

- $A = p \to q$; $B = q \to r$; $C = p \to r$
- $F = A \wedge B \leftrightarrow C$

p	q	r	A	B	C	$A \wedge B$	F
T	**T**	**T**	**T**	**T**	**T**		
T	**T**	**F**	**T**	**F**	**F**		
T	**F**	**T**	**F**	**T**	**T**		
T	**F**	**F**	**F**	**T**	**F**		
F	**T**	**T**	**T**	**T**	**T**		
F	**T**	**F**	**T**	**F**	**T**		
F	**F**	**T**	**T**	**T**	**T**		
F	**F**	**F**	**T**	**T**	**T**		

Truth Table

EXAMPLE: Truth table of $F = (p \to q) \land (q \to r) \leftrightarrow (p \to r)$

- $A = p \to q; B = q \to r;\ C = p \to r$
- $F = A \land B \leftrightarrow C$

p	q	r	A	B	C	$A \land B$	F
T	**T**	**T**	**T**	**T**	**T**	**T**	
T	**T**	**F**	**T**	**F**	**F**	**F**	
T	**F**	**T**	**F**	**T**	**T**	**F**	
T	**F**	**F**	**F**	**T**	**F**	**F**	
F	**T**	**T**	**T**	**T**	**T**	**T**	
F	**T**	**F**	**T**	**F**	**T**	**F**	
F	**F**	**T**	**T**	**T**	**T**	**T**	
F	**F**	**F**	**T**	**T**	**T**	**T**	

Truth Table

EXAMPLE: Truth table of $F = (p \to q) \land (q \to r) \leftrightarrow (p \to r)$

- $A = p \to q$; $B = q \to r$; $C = p \to r$
- $F = A \land B \leftrightarrow C$

p	q	r	A	B	C	$A \land B$	F
T	**T**	**T**	**T**	**T**	**T**	**T**	**T**
T	**T**	**F**	**T**	**F**	**F**	**F**	**T**
T	**F**	**T**	**F**	**T**	**T**	**F**	**F**
T	**F**	**F**	**F**	**T**	**F**	**F**	**T**
F	**T**	**T**	**T**	**T**	**T**	**T**	**T**
F	**T**	**F**	**T**	**F**	**T**	**F**	**F**
F	**F**	**T**	**T**	**T**	**T**	**T**	**T**
F	**F**	**F**	**T**	**T**	**T**	**T**	**T**

Example

- **System Specifications**: Determine if there is a system that satisfies all of the following requirements.
  1. The diagnostic message is stored in the buffer or it is retransmitted.
  2. The diagnostic message is not stored in the buffer.
  3. If the diagnostic message is stored in the buffer, then it's retransmitted.
  4. The diagnostic message is not retransmitted
     - $s \vee r; \neg s; s \rightarrow r; \neg r$

s	r	$s \vee r$	$\neg s$	$s \rightarrow r$	$\neg r$
T	**T**				
T	**F**				
F	**T**				
F	**F**				

Example

- **System Specifications**: Determine if there is a system that satisfies all of the following requirements.
  1. The diagnostic message is stored in the buffer or it is retransmitted.
  2. The diagnostic message is not stored in the buffer.
  3. If the diagnostic message is stored in the buffer, then it’s retransmitted.
  4. The diagnostic message is not retransmitted
     - $s \vee r$; $\neg s$; $s \rightarrow r$; $\neg r$
       - There is no system that satisfies 1, 2, 3 and 4.

s	r	$s \vee r$	$\neg s$	$s \rightarrow r$	$\neg r$
T	**T**	**T**	**F**	**T**	**F**
T	**F**	**T**	**F**	**F**	**T**
F	**T**	**T**	**T**	**T**	**F**
F	**F**	**F**	**T**	**T**	**T**

Example

Solving Logic Puzzle: An island has two kinds of inhabitants, knights, who always tell the truth, and knaves, who always lie. You go to the island and meet A and B. A says "B is a knight". B says "The two of us are of opposite types." What are A and B?

- p: A is a knight; q: B is a knight

Possibilities		A says "B is a knight."		B says "The two of us are of opposite types."	
p	q	p	q	p	q
T	**T**	**T**			**T**
T	**F**	**T**			**F**
F	**T**	**F**			**T**
F	**F**	**F**			**F**

Example

Solving Logic Puzzle: An island has two kinds of inhabitants, knights, who always tell the truth, and knaves, who always lie. You go to the island and meet A and B. A says "B is a knight". B says "The two of us are of opposite types." What are A and B?

- p: A is a knight; q: B is a knight

Possibilities		A says "B is a knight."		B says "The two of us are of opposite types."	
p	q	p	q	p	q
T	**T**	**T**	**T**	**F**	**T**
T	**F**	**T**	**T**	**X**	**F**
F	**T**	**F**	**F**	**X**	**T**
F	**F**	**F**	**F**	**F**	**F**

Types of WFFs

Tautology(重言式)**:** a WFF whose truth value is **T** for all truth assignment

- $p \vee \neg p$ is a tautology

Contradiction(矛盾式)**:** a WFF whose truth value is **F** for all truth assignment

- $p \wedge \neg p$ is a contradiction

Contingency(可能式)**:** neither tautology nor contradiction

- $p \rightarrow \neg p$ is a contingency

Satisfiable(可满足的):a WFF is satisfiable if it is true for at least one truth assignment

<u>**Rule of Substitution**: </u>(代入规则) Let B be a formula obtained from a tautology A by substituting a propositional variable in A with an arbitrary formula. Then B must be a tautology.

- $p \vee \neg p$ is a tautology: $(q \wedge r) \vee \neg(q \wedge r)$ is a tautology as well.

Logically Equivalent

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

- A and B are **logically equivalent** (等值) if they always have the same truth value for every truth assignment (of $p_1, \ldots, p_n$)
  - Notation: $A \equiv B$

THEOREM: $A \equiv B$ if and only if $A \leftrightarrow B$ is a tautology.

- $A \equiv B$
- iff for any truth assignment, A, B take the same truth values
- iff for any truth assignment, $A \leftrightarrow B$ is true
- iff $A \leftrightarrow B$ is a tautology

THEOREM: $A \equiv A$; If $A \equiv B$, then $B \equiv A$; If $A \equiv B, B \equiv C$, then $A \equiv C$

QUESTION: How to prove $A \equiv B$?

Proving $A \equiv B$

Method 1: Show that A, B have the same truth table.

Method 2: Rule of Replacement: (替换规则) Replacing a sub-formula in a formula F with a logically equivalent sub-formula gives a formula logically equivalent o the formula F.

Proving $A \equiv B$

EXAMPLE: $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$ **//distributive law**

- Idea: Show that A, B have the same truth table.

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
T	**T**	**T**					
T	**T**	**F**					
T	**F**	**T**					
T	**F**	**F**					
F	**T**	**T**					
F	**T**	**F**					
F	**F**	**T**					
F	**F**	**F**					

Proving $A \equiv B$

EXAMPLE: $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$ **//distributive law**

- Idea: Show that A, B have the same truth table.

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
T	**T**	**T**	**T**	**T**	**T**	**T**	**T**
T	**T**	**F**	**T**	**T**	**T**	**F**	**T**
T	**F**	**T**	**T**	**T**	**F**	**T**	**T**
T	**F**	**F**	**F**	**F**	**F**	**F**	**F**
F	**T**	**T**	**T**	**F**	**F**	**F**	**F**
F	**T**	**F**	**T**	**F**	**F**	**F**	**F**
F	**F**	**T**	**T**	**F**	**F**	**F**	**F**
F	**F**	**F**	**F**	**F**	**F**	**F**	**F**

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

Logical Equivalences

Name	Logical Equivalences	NO.
Double Negation Law 双重否定律	$\neg(\neg P) \equiv P$	1
Identity Laws 同一律	$P \wedge \mathbf{T} \equiv P$	2
	$P \vee \mathbf{F} \equiv P$	3
Idempotent Laws 等幂律	$P \vee P \equiv P$	4
	$P \wedge P \equiv P$	5
Domination Laws 零律	$P \vee \mathbf{T} \equiv \mathbf{T}$	6
	$P \wedge \mathbf{F} \equiv \mathbf{F}$	7
Negation Laws 补余律	$P \vee \neg P \equiv \mathbf{T}$	8
	$P \wedge \neg P \equiv \mathbf{F}$	9

Logical Equivalences

Name	Logical Equivalences	NO.
Commutative Laws 交换律	$P \vee Q \equiv Q \vee P$	10
	$P \wedge Q \equiv Q \wedge P$	11
Associative Laws 结合律	$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$	12
	$P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$	13
Distributive Laws 分配律	$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$	14
	$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$	15
De Morgan's Laws 摩根律	$\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$	16
	$\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$	17
Absorption Laws 吸收律	$P \vee (P \wedge Q) \equiv P$	18
	$P \wedge (P \vee Q) \equiv P$	19

Logical Equivalences

Name	Logical Equivalences	NO.
Laws Involving Implication $\rightarrow$	$P \rightarrow Q \equiv \neg P \vee Q$	20
	$P \rightarrow Q \equiv \neg Q \rightarrow \neg P$	21
	$(P \rightarrow R) \wedge (Q \rightarrow R) \equiv (P \vee Q) \rightarrow R$	22
	$P \rightarrow (Q \rightarrow R) \equiv (P \wedge Q) \rightarrow R$	23
	$P \rightarrow (Q \rightarrow R) \equiv Q \rightarrow (P \rightarrow R)$	24
Laws Involving Bi-Implication $\leftrightarrow$	$P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$	25
	$P \leftrightarrow Q \equiv (\neg P \vee Q) \wedge (P \vee \neg Q)$	26
	$P \leftrightarrow Q \equiv (P \wedge Q) \vee (\neg P \wedge \neg Q)$	27
	$P \leftrightarrow Q \equiv \neg P \leftrightarrow \neg Q$	28

Proving $A \equiv B$

Rule of Replacement: (替换规则) Replacing a sub-formula in a formula F with a logically equivalent sub-formula gives a formula logically equivalent to the formula F.

EXAMPLE: $P \to Q \equiv \neg Q \to \neg P$

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

EXAMPLE: $P \leftrightarrow Q \equiv (\neg P \vee Q) \wedge (P \vee \neg Q)$

$$P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P) \equiv (\neg P \vee Q) \wedge (\neg Q \vee P)$$
$$\equiv (\neg P \vee Q) \wedge (P \vee \neg Q)$$

EXAMPLE: $P \to (Q \to R) \equiv (P \wedge Q) \to R$

$$P \to (Q \to R) \equiv \neg P \vee (\neg Q \vee R) \equiv (\neg P \vee \neg Q) \vee R \equiv \neg(P \wedge Q) \vee R$$
$$\equiv (P \wedge Q) \to R$$

Proving Types of WFFs

EXAMPLE: Show the following WFF is a tautology or a contradiction:

1. $p \to (p \vee \neg q \vee r)$

Hint: $\neg p \vee p \vee \neg q \vee r \equiv T \vee (\neg q \vee r) \equiv T$

2. $\neg((p \vee q) \wedge \neg p \to q)$

Hint: $\neg\big((p \wedge \neg p) \vee (q \wedge \neg p) \to q\big)$
$\equiv \neg\big((q \wedge \neg p) \to q\big) \equiv \neg(\neg(q \wedge \neg p) \vee q) \equiv q \ \wedge \neg p \ \wedge \neg q \equiv F$

Proving Types of WFFs

EXAMPLE: Consider the following task: A company plans to relocate John or Mary to its SF office. If John is relocated, then Ben needs to do extra work. If Mary is relocated, then Lisa will be relocated too. It turns out Ben do not need to do extra work. What is the company's arrangement for its employees?

$$A = ((p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow s) \wedge \neg r$$

Hint:

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

A: $((p\wedge\neg q)\vee(p\wedge s)\vee(q\wedge s))\wedge(\neg p\wedge\neg r)$

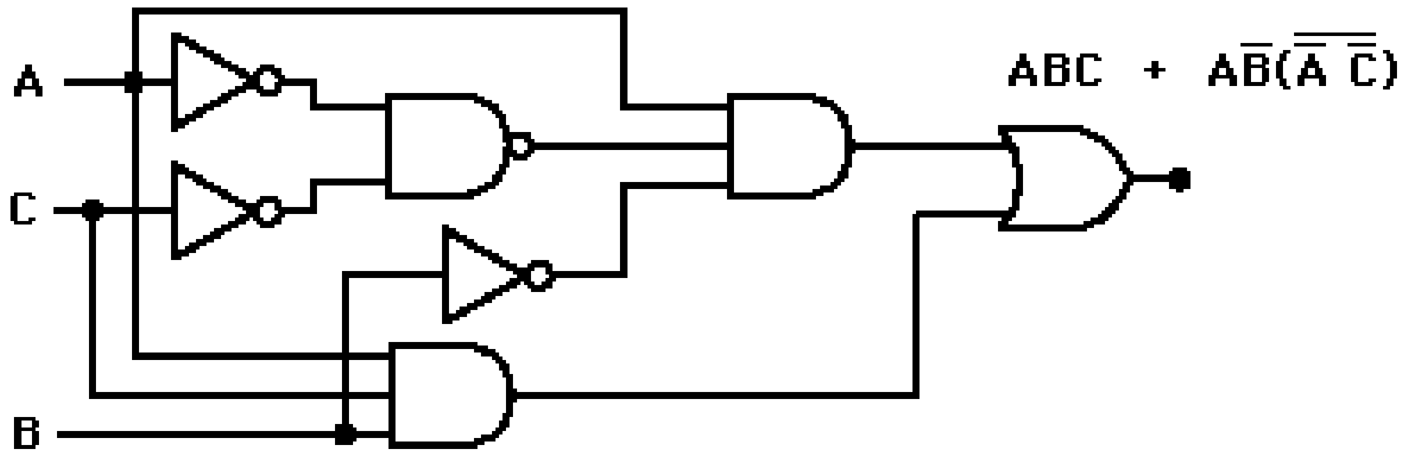
(Distribution Laws) $\equiv ((p\wedge\neg q)\wedge(\neg p\wedge\neg r))\vee((p\wedge s)\wedge(\neg p\wedge\neg r))\vee((q\wedge s)\wedge(\neg p\wedge\neg r))$

(Negation Laws) $\equiv F \vee F \vee ((q\wedge s)\wedge(\neg p\wedge\neg r))$

(Domination Laws) $\equiv ((q\wedge s)\wedge(\neg p\wedge\neg r))$

Example: Simplify Logic Circuits

A	B	C	Out
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1



It can be simplified by:

$ABC + A\bar{B}(\bar{\bar{A}} + \bar{\bar{C}})$	DeMorgan's theorem
$ABC + A\bar{B}A + A\bar{B}C$	sum of products form
$ABC + A\bar{B} + A\bar{B}C$	BA=AB and AA = A
$AC(B + \bar{B}) + A\bar{B}$	
$AC + A\bar{B}$	$B + \bar{B} = 1$
$A(C + \bar{B})$