离散数学

Discrete Mathematics

for Computer Science

计算机学院计科系

薛思清 xuesiqing@cug.edu.cn

第2讲 命题逻辑 Propositional Logic(3)

Mathematical logic is to computer science what calculus is to physics.

—J Strother Moore

我的命题仅仅是'如果…那么…',
并且我的成功仅在于用漂亮的链,
把两个疑虑连接：因为问也徒劳。
如果我的假设是成立的,
或者我所证明的是具有事实的根据,
桥还是存在的，人不必在两侧都爬行,
这样就取得了胜利。
这个摆弄微弱阴影的游戏,
并不需要多少力气,
多么脆弱的魔棍,
却又具有多么深厚的魅力。

——C.R.Wylie, Jr

Histories make men wise; poets, witty; the mathematics, subtle; natural philosophy, deep; moral, grave; logic and rhetoric, able to contend.

——*Bacon Francis*

2.5 形式推理（Formal Reasoning）

- **演绎推理**

  数理逻辑中，应用公认的推理规则(Rules of Inference)从一些前提(Premise)中推导出结论来时，这种推导过程称之为演绎推理(Deduction)或形式证明(Formal Proof)。

Deductive Reasoning vs. Inductive Reasoning

1 推理形式

设$\alpha_1,\alpha_2,\ldots,\alpha_n,\beta$都是命题公式。称由前提$\alpha_1,\alpha_2,\ldots,\alpha_n$推出$\beta$的推理是有效的或正确的，并称$\beta$是$\alpha_1,\alpha_2,\ldots,\alpha_n$的有效结论或逻辑结果（Logical Consequence），

当且仅当

$(\alpha_1\wedge\alpha_2\wedge\ldots\wedge\alpha_n)\rightarrow\beta$是永真式

记为$\alpha_1\wedge\alpha_2\wedge\ldots\wedge\alpha_n\Rightarrow\beta$或$\alpha_1,\alpha_2,\ldots,\alpha_n\Rightarrow\beta$（称为重言蕴含或推理形式）

2.5 形式推理（Formal Reasoning）

示例 写出下述推理关系的推理形式："下午小王或去看电影或去游泳。他没去看电影。所以，他去游泳了。"

解 设 P：小王下午去看电影；Q：小王下午去游泳。于是得到如下推理形式:

前提：$P \vee Q$，$\neg P$

结论：Q

推理形式为:$(P \vee Q) \wedge \neg P \Rightarrow Q$

2.5 形式推理（Formal Reasoning）

讨论

1 符号⇒与→是两个完全不同的符号?

2 推理有效，则所得结论就真实吗?推理是有效的话，那么不可能有：它的前提都为真时而它的结论为假，对吗?

3 可以用真值表在有限步内判定一个结论是否是前提的有效逻辑结论吗?

4 推理方法还有哪些?

→动态推理方法:

公理+推理规则：演绎推理

等值公式（用于等价变换或蕴含推理）以及以下**蕴含推理定律**构成了演绎推理基本规则。

2 推理定律/规则,Rules of proof)

有如下蕴含推理式（α、β、γ均为任意命题公式）：

I_1 合取引入规则 $\alpha,\beta \Rightarrow \alpha\wedge\beta$

I_2 简化规则 $\alpha\wedge\beta \Rightarrow \alpha$， $\alpha\wedge\beta \Rightarrow \beta$

I_5 $\neg(\alpha\rightarrow\beta) \Rightarrow \alpha$， $\neg(\alpha\rightarrow\beta) \Rightarrow \neg\beta$

I_3 附加规则 $\alpha \Rightarrow \alpha\vee\beta$， $\beta \Rightarrow \alpha\vee\beta$

I_4 $\neg\alpha \Rightarrow \alpha\rightarrow\beta$， $\beta \Rightarrow \alpha\rightarrow\beta$

I_6 $\alpha\rightarrow\beta \Rightarrow (\alpha\vee\gamma)\rightarrow(\beta\vee\gamma)$,

$\alpha\rightarrow\beta \Rightarrow (\alpha\wedge\gamma)\rightarrow(\beta\wedge\gamma)$

2.5 形式推理（Formal Reasoning）

I_7 假言推理（又称分离规则）$(\alpha\rightarrow\beta)\wedge\alpha\Rightarrow\beta$

I_8 拒取式(否定后件式) $(\alpha\rightarrow\beta)\wedge\neg\beta\Rightarrow\neg\alpha$

I_9 析取三段论$(\alpha\vee\beta)\wedge\neg\beta\Rightarrow\alpha$

I_{11} 二难推理 $(\alpha\rightarrow\gamma)\wedge(\beta\rightarrow\gamma)\wedge(\alpha\vee\beta)\Rightarrow\gamma$

I_{10} 假言三段论$(\alpha\rightarrow\beta)\wedge(\beta\rightarrow\gamma)\Rightarrow(\alpha\rightarrow\gamma)$

I_{12} 等价三段论$(\alpha\leftrightarrow\beta)\wedge(\beta\leftrightarrow\gamma)\Rightarrow(\alpha\leftrightarrow\gamma)$

I_{13} $(\alpha\rightarrow\beta)\wedge(\beta\rightarrow\alpha)\Rightarrow(\alpha\leftrightarrow\beta)$

$\alpha\leftrightarrow\beta\Rightarrow\alpha\rightarrow\beta$，$\alpha\leftrightarrow\beta\Rightarrow\beta\rightarrow\alpha$

（双否，矛盾律）

3 推理规则

- 前提引入(P)
- 结论引用(T)
- 置换规则(R)
- 代入规则(S)

4 动态推理方法——直接证明

4 动态推理方法——直接证明

示例 证明$(P\vee Q)\wedge(P\rightarrow R)\wedge(Q\rightarrow S)\Rightarrow S\vee R$

证明 (1) $P\vee Q$ P

(2) $\neg P\rightarrow Q$ R,E,(1)

(3) $Q\rightarrow S$ P

(4) $\neg P\rightarrow S$ T,I,(2),(3)

(5) $\neg S\rightarrow P$ R,E,(4)

(6) $P\rightarrow R$ P

(7) $\neg S\rightarrow R$ T,I,(5),(6)

(8) $S\vee R$ R,E,(7)

练习：构造下列推理的证明

前提：$A \vee B$, $B \to C$, $A \to D$, $\neg D$，结论：$C \wedge (A \vee B)$

解 根据合取引入规则，因为已经有前提$A \vee B$，所以只要推出结论C即可：

(1)	$A \to D$	P
(2)	$\neg D$	P
(3)	$\neg A$	T,I (1)(2)
(4)	$A \vee B$	P
(5)	B	T,I (3)(4)
(6)	$B \to C$	P
(7)	C	T, I (5)(6)

4 动态推理方法——间接证明

4 动态推理方法——间接证明

反证法?

矛盾法/(Proof by Contradiction)

——设α，β是命题公式，则$\alpha \Rightarrow \beta$的充要条件是$\alpha \wedge \neg \beta$是矛盾式。

示例 证明$P\rightarrow\neg Q$，$Q\vee\neg R$，$R\wedge\neg S\Rightarrow\neg P$

证明 用反证法。

(1) $\neg(\neg P)$ P(附加)

(2) P R,E,(1)

(3) $P\rightarrow\neg Q$ P

(4) $\neg Q$ T,I,(2),(3)

(5) $Q\vee\neg R$ P

(6) $\neg R$ T,I,(4),(5)

(7) $R\wedge\neg S$ P

(8) R T,I,(7)

(9) $R\wedge\neg R$ T,I,(6),(8),矛盾

因此，假设不成立，原推理形式正确。

5 CP规则(Rule of Condition Proof)

演绎定理

$(\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_k \wedge \alpha) \Rightarrow \beta$ 当且仅当$(\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_k) \Rightarrow \alpha \rightarrow \beta$。

利用演绎定理，许多命题公式，特别是蕴涵式的证明可得到简化，可将蕴涵式的前件作为前提引入来进行证明。

2.5 形式推理（Formal Reasoning）

示例 验证下述推理是否正确。

或者逻辑学难学，或者有多数学生喜欢它；如果数学容易学，那么逻辑学并不难学。因此如果许多学生不喜欢逻辑，那么数学并不容易学。

解 先将命题符号化，首先抽取的基本命题包括：

P：逻辑学难学； Q：有多数学生喜欢逻辑学； R：数学容易学。

则上述推理形式化为：

前提：$P \vee Q$，$R \rightarrow \neg P$

结论：$\neg Q \rightarrow \neg R$

证明：$P \vee Q$，$R \rightarrow \neg P \Rightarrow \neg Q \rightarrow \neg R$

(1) $\neg Q$	P(附加)
(2) $P \vee Q$	P
(3) P	T,I,(1),(2)
(4) $R \rightarrow \neg P$	P
(5) $\neg R$	T,I,(3),(4)
(6) $\neg Q \rightarrow \neg R$	CP

根据CP规则，整个推理正确。

练习

在某一次足球比赛中，四支球队进行了比赛，已知情况如下，问结论是否有效?

前提：若A队得第一，则B队或C队获亚军；

若C队获亚军，则A队不能获冠军；

若D队获亚军，则B队不能获亚军；

A 队获第一。

结论： D队不是亚军。

首先符号化

令P：A 队获冠军；Q：B 队获亚军；R：C 队获亚军；S：D 队获亚军，则

前提：$P\rightarrow(Q\vee R)$，$R\rightarrow\neg P$，$S\rightarrow\neg Q$，P

结论：$\neg S$

推理形式：$P\rightarrow(Q\vee R)$，$R\rightarrow\neg P$，$S\rightarrow\neg Q$，$P\Rightarrow\neg S$

首先符号化

令P：A队获冠军；Q：B队获亚军；R：C队获亚军；S：D队获亚军，则

前提：$P \rightarrow (Q \vee R)$，$R \rightarrow \neg P$，$S \rightarrow \neg Q$，P

结论：$\neg S$

推理形式：$P \rightarrow (Q \vee R)$，$R \rightarrow \neg P$，$S \rightarrow \neg Q$，$P \Rightarrow \neg S$

证明：	（1）P	P
	（2）$P \rightarrow (Q \vee R)$	P
	（3）$Q \vee R$	T, I, (1), (2)
	（4）$R \rightarrow \neg P$	P
	（5）$P \rightarrow \neg R$	R, E, , (4)
	（6）$\neg R$	T, I, (1), (5)
	（7）Q	T, I, (3), (6)
	（8）$S \rightarrow \neg Q$	P
	（9）$Q \rightarrow \neg S$	R, E, , (8)
	（10）$\neg S$	T, I, (7), (9)

因此，该结论是有效的。

More...

简化版本

The Proof Rules

Conjunction (Conj) $\dfrac{A, B}{A \wedge B}$		*Simplification (Simp)* $\dfrac{A \wedge B}{A}$ and $\dfrac{A \wedge B}{B}$
Addition (Add) $\dfrac{A}{A \vee B}$ and $\dfrac{A}{B \vee A}$		*Disjunctive Syllogism (DS)* $\dfrac{A \vee B, \neg A}{B}$ and $\dfrac{A \vee B, \neg B}{A}$
Modus Ponens (MP) $\dfrac{A, A \to B}{B}$		*Conditional Proof (CP)* $\dfrac{\text{From } A, \text{ derive } B}{A \to B}$
Double Negation (DN) $\dfrac{\neg\neg A}{A}$ and $\dfrac{A}{\neg\neg A}$	*Contradiction (Contr)* $\dfrac{A, \neg A}{\text{False}}$	*Indirect Proof (IP)* $\dfrac{\text{From } \neg A, \text{ derive False}}{A}$

示例

If I think, then I exist.

If I do not think, then I think.

Therefore, I exist.

A : “I think”

B : “I exist”

Premises: $A \rightarrow B$, $\neg A \rightarrow A$

Conclusion: B

1.	$A \rightarrow B$	P
2.	$\neg A \rightarrow A$	P
3.	$\neg B$	P [for B]
4.	$\neg\neg A$	P [for $\neg A$]
5.	A	4, DN
6.	B	1, 5, MP
7.	False	3, 6, Contr
8.	$\neg A$	4–7, IP
9.	A	2, 8, MP
10.	False	8, 9, Contr
11.	B	3, 8–10, IP
	QED.	

Derived Rules

Modus Tollens (MT) (Latin for "mode that denies") $\dfrac{A \to B, \quad \neg B}{\neg A}$	*Proof by Cases (Cases)* $\dfrac{A \vee B, \quad A \to C, \quad B \to C}{C}$
Hypothetical Syllogism (HS) $\dfrac{A \to B, \quad B \to C}{A \to C}$	*Constructive Dilemma (CD)* $\dfrac{A \vee B, \quad A \to C, \quad B \to D}{C \vee D}$

Proof of Modus Tollens (MT):

$$\frac{A \to B, \quad \neg B}{\neg A}.$$

1.	$A \to B$		P
2.	$\neg B$		P
3.		$\neg\neg A$	P [for $\neg$ A]
4.		A	3, DN
5.		B	1, 4, MP
6.		False	2, 5, Contr
7.	$\neg A$		3–6, IP
	QED.		

Proof of Proof by Cases (Cases,Dilemma) $\dfrac{A \vee B, \quad A \to C, \quad B \to C}{C}$.

1.	$A \vee B$	P
2.	$A \to C$	P
3.	$B \to C$	P
4.	$\quad \neg C$	P [for C]
5.	$\quad \neg A$	4, MT
6.	$\quad B$	1, 5, DS
7.	$\quad C$	3, 6, MP
8.	$\quad$ False	4, 7, Contr
9.	C	4–8, IP
	QED.	

Proof of Hypothetical Syllogism (HS)

$$\frac{A \to B, \quad B \to C}{A \to C}$$

1.	$A \to B$	P
2.	$B \to C$	P
3.	A	P [for $A \to C$]
4.	B	1, 3, MP
5.	C	2, 4, MP
6.	$A \to C$	3–5, CP
	QED.	

Proof of Constructive Dilemma (CD)

$$\frac{A \vee B, \quad A \to C, \quad B \to D}{C \vee D}$$

1.	$A \vee B$	P
2.	$A \to C$	P
3.	$B \to D$	P
4.	$\quad A$	P [for $A \to C \vee D$]
5.	$\quad C$	2, 4, MP
6.	$\quad C \vee D$	5, Add
7.	$A \to C \vee D$	4–6, CP
8.	$\quad B$	P [for $B \to C \vee D$]
9.	$\quad D$	3, 8, MP
10.	$\quad C \vee D$	9, Add
11.	$B \to C \vee D$	8–10, CP
12.	$C \vee D$	1, 7, 11, Cases
	QED.	

Proof $A \vee B \equiv B \vee A$

1 Proof of $A \vee B \rightarrow B \vee A$

1.	$A \vee B$			P
2.		$\neg(B \vee A)$		P [for $B \vee A$]
3.			$\neg\neg A$	P [for $\neg A$]
4.			A	3, DN
5.			$B \vee A$	4, Add
6.			False	2, 5, Contr
7.		$\neg A$		3–6, IP
8.		B		1, 7, DS
9.		$B \vee A$		8, Add
10.		False		2, 9, Contr
11.	$B \vee A$			2, 7–10, IP
	QED			1, 11, CP.

The proof of $B \vee A \rightarrow A \vee B$ is similar.

Proof $A \rightarrow B \equiv \neg A \lor B$

1 Proof of $(A \rightarrow B) \rightarrow (\neg A \lor B)$

2 Proof of $(\neg A \lor B) \rightarrow (A \rightarrow B)$

1 Proof of (A → B) → (¬ A ∨ B)

1.	$A \to B$	P
2.	$\neg(\neg A \vee B)$	P [for $\neg A \vee B$]
3.	$\neg A$	P [for A]
4.	$\neg A \vee B$	3, Add
5.	False	2, 4, Contr
6.	A	3–5, IP
7.	B	1, 6, MP
8.	$\neg A \vee B$	7, Add
9.	False	2, 8, Contr
10.	$\neg A \vee B$	2, 6–9, IP
	QED	1, 10, CP.

2 Proof of $(\neg A \lor B) \rightarrow (A \rightarrow B)$

1.	$\neg A \lor B$	P
2.	A	P [for $A \rightarrow B$]
3.	$\neg\neg A$	2, DN
4.	B	1, 3, DS
5.	$A \rightarrow B$	2–4, CP
	QED	1, 5, CP.

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

1 Proof of $\neg (A \vee B) \rightarrow (\neg A \wedge \neg B)$

2 Proof of $(\neg A \wedge \neg B) \rightarrow \neg (A \vee B)$

1 Proof of ¬ (A ∨ B) → (¬ A ∧ ¬ B)

1.	$\neg(A \vee B)$	P
2.	$\quad \neg\neg A$	P [for $\neg A$]
3.	$\quad A$	2, DN
4.	$\quad A \vee B$	3, Add
5.	$\quad$ False	1, 4, Contr
6.	$\neg A$	2–5, IP
7.	$\quad \neg\neg B$	P [for $\neg B$]
8.	$\quad B$	7, DN
9.	$\quad A \vee B$	8, Add
10.	$\quad$ False	1, 9, Contr
11.	$\neg B$	7–10, IP
12.	$\neg A \wedge \neg B$	6, 11, Conj
	QED	1, 6, 11, 12, CP.

2 Proof of $(\neg A \wedge \neg B) \rightarrow \neg(A \vee B)$

1.	$\neg A \wedge \neg B$	P
2.	$\quad \neg\neg(A \vee B)$	P [for $\neg(A \vee B)$]
3.	$\quad A \vee B$	2, DN
4.	$\quad \neg A$	1, Simp
5.	$\quad B$	3, 4, DS
6.	$\quad \neg B$	1, Simp
7.	$\quad$ False	5, 6, Contr
8.	$\neg(A \vee B)$	2–7, IP
	QED	1, 8, CP.

More...

Formal System (形式系统)

Formal System

A *formal system* F has three components:

- ***Formal language*** (symbols + certain expressions called *formulas*);
- ***Axioms*** (certain formulas);
- ***Rules of inference***.

By Richard E. Hodel

The formal system ADD.

Language There are three symbols: $+$, $=$, and $|$. A formula is any expression of the form $x + y = z$, where x, y, and z are expressions that use just the symbol $|$. For example, $||| + || = |||||$ is a formula, but $|| + + = ||$ and $|| = | + |$ are not formulas.

Axioms The only axiom is the formula $| + | = ||$.

Rules of inference There are two rules of inference:

$$\text{R1: } \frac{x + y = z}{x| + y = z|} \qquad \text{R2: } \frac{x + y = z}{y + x = z}$$

Definition 3: Let F be a formal system. A *proof in* F is a finite sequence $A_1, \ldots, A_n$ of formulas of F such that for $1 \le k \le n$, one of the following conditions is satisfied: (1) A_k is an axiom of F; (2) $k > 1$ and A_k is the conclusion of a rule of inference whose hypotheses are among the previous formulas $A_1, \ldots, A_{k-1}$. A proof in F can be displayed schematically as follows:

$$
\begin{array}{ll}
(1) & A_1 \\
 & \vdots \\
 & \vdots \\
 & \vdots \\
(n) & A_n.
\end{array}
$$

If $A_1, \ldots, A_n$ is a proof in F with $A_n = A$, we say that $A_1, \ldots, A_n$ is a *proof of* A and that A is a *theorem of* F; we denote this by $\vdash_F A$. When the formal system F under discussion is understood, we often omit the subscript F and simply write $\vdash A$.

Example

The formula $|| + ||| = |||||$ is a theorem of the formal system ADD. To show this, it suffices to write out a formal proof:

(1)	$\| + \| = \|\|$	AXIOM
(2)	$\|\| + \| = \|\|\|$	R1
(3)	$\|\|\| + \| = \|\|\|\|$	R1
(4)	$\| + \|\|\| = \|\|\|\|$	R2
(5)	$\|\| + \|\|\| = \|\|\|\|\|$	R1

In summary, $\vdash_{ADD} || + ||| = |||||$ as required. $\square$

Definition 4: A formal system F is *decidable* if there is an algorithm that, given an arbitrary formula A of F, decides (YES or NO in a finite number of steps) whether $\vdash_F A$. If there is no such algorithm, we say that F is *undecidable*.

One of the most important questions we can ask about a formal system is whether it is decidable. Later we will see that propositional logic is decidable and that first-order logic is undecidable. As a rather trivial example for now, the formal system ADD is decidable ∎

Formal Axiom Systems

Soundness(可靠性)

All proofs yield theorems that are tautologies.

Completeness(完备性)

Any tautology can be proven as a theorem in the axiom system.

Consistent(一致性)?

Examples

Frege-Lukasiewicz Axioms

1. $A \to (B \to A)$.
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$.
3. $(\neg A \to \neg B) \to (B \to A)$.

Hilbert-Ackermann Axioms

1. $A \vee A \to A$.
2. $A \to A \vee B$.
3. $A \vee B \to B \vee A$.
4. $(A \to B) \to (C \vee A \to C \vee B)$.

Frege-Lukasiewicz Axioms

1. $A \to (B \to A)$.

2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$.

3. $(\neg A \to \neg B) \to (B \to A)$.

Lemma 1. $A \to A$ is provable from the axioms.

In the following proof, B can be any wff, including A.

1.	$(A \to ((B \to A) \to A)) \to ((A \to (B \to A)) \to (A \to A))$	Axiom 2
2.	$A \to ((B \to A) \to A)$	Axiom 1
3.	$(A \to (B \to A)) \to (A \to A)$	1, 2, MP
4.	$A \to (B \to A)$	Axiom 1
5.	$A \to A$	3, 4, MP

QED.

「华容道」

- 这个游戏由一个底盘、一个大正方形、四个竖长方形、一个横长方形和四个小正方形构成；
- 游戏开始时，在底盘上，按照规定的格式摆放各个方块。
- 移动方块只能水平或垂直按顺序移动，不许做90°旋转，也不可越过其它方块移动。

【形式系统】？

语言（词汇表）：游戏的基本材料是构成游戏的元素；

公理：规定了游戏开始之前的初始条件，不符合这个条件游戏无法开始

推理规则：从初始状态「推导」，我们可以得到许多「中间结果」，如果这些「中间结果」最终导致「定理」「大正方形位于底部出口」这个命题为真，那么可称之为「辅助定理」。

「计算机程序」？

命题逻辑 小结

- 命题、联接词
- 命题公式、命题公式的类型
- 等值公式、等值演算
- 范式
- 推理演算
- 形式系统

✓ 运算表与真值表：析取、蕴含
✓ 等值式
✓ 代入定理
✓ 置换定理
✓ 对偶定理
✓ 演绎定理

✓ 主范式
✓ 演绎推理
✓ 推理规则
✓ 推理定律
✓ 推理方法