数理逻辑

郑为杰
e-mail: zhengweijie@hit.edu.cn

哈尔滨工业大学（深圳）计算机学院

2023年11月

逻辑蕴含的定义

设$\Gamma \subseteq Form(L^P), A \in Form(L^P)$，如果对任意赋值$v$，

- 当v对Γ中的任意公式赋值为1时（即对任意的$B \in \Gamma$,有$B^v = 1$），有v对命题公式A的赋值也为1（即$A^v = 1$），
- 则称Γ可以语义推出A，或称Γ可以逻辑推出A，或称Γ可以逻辑蕴含A，或称A是Γ的逻辑结果，记为$\Gamma \Rightarrow A$

逻辑蕴含

$\Gamma \Rightarrow A$，如果对任意赋值v，当v对Γ中的任意公式赋值为1时（即对任意的$B \in \Gamma$,有$B^v = 1$），有v对命题公式A的赋值也为1（即$A^v = 1$）

例：试证$\{A, A \to B\} \Rightarrow B$

证明：只需证明对任意的指派v,当 $A^v = 1$，$(A \to B)^v = 1$时，$B^v = 1$

由$(A \to B)^v = 1 - A^v + A^v B^v = 1$

故$A^v B^v = A^v$

又由 $A^v = 1$，知$B^v = 1$

逻辑蕴含

$\Gamma \Rightarrow A$，如果对任意赋值v，当v对Γ中的任意公式赋值为1时（即对任意的$B \in \Gamma$,有$B^v = 1$），有v对命题公式A的赋值也为1（即$A^v = 1$）

例：试证 $\{\neg A, B \rightarrow A\} \Rightarrow \neg B$

证明：只需证明对任意的指派v，当 $(\neg A)^v = 1, (B \rightarrow A)^v = 1$时，$(\neg B)^v = 1$

由$(B \rightarrow A)^v = 1 - B^v + B^v A^v = 1$，知$B^v A^v = B^v$

由$(\neg A)^v = 1 - A^v = 1$，知$A^v = 0$

从而$B^v = A^v B^v = 0$，$(\neg B)^v = 1 - B^v = 1$

逻辑等价的定义

- 设$A, B \in Form(L^P)$，如果$A \Rightarrow B$并且$B \Rightarrow A$,则称A和B逻辑等价，记为$A \Leftrightarrow B$
- 推论：设$A, B \in Form(L^P)$，$A \Leftrightarrow B$当且仅当对任意的赋值v都有$A^v = B^v$

证明:

必要性：若$A^v = 1$，则由$A \Leftrightarrow B$，有$A \Rightarrow B$，故$B^v = 1$；若$A^v = 0$，则$B^v = 0$，否则若$B^v = 1$，由 $A \Leftrightarrow B$有$B \Rightarrow A$,必有$A^v = 1$与$A^v = 0$矛盾

充分性：由对任意的指派v，都有$A^v = B^v$知，对于任意的指派v，当A^v=1，则B^v=1，$A \Rightarrow B$；对于任意的指派v，当B^v=1，则A^v=1，$B \Rightarrow A$；故，$A \Leftrightarrow B$

逻辑蕴含的性质

- $A \Rightarrow B$当且仅当$A \longrightarrow B$是永真式
- 必要性：如果$A \Rightarrow B$，那么$A \longrightarrow B$是永真式。

证明：对任意指派v，往证$(A \longrightarrow B)^v = 1$

若 $A^v = 1$，由$A \Rightarrow B$知$B^v = 1$

则有$(A \longrightarrow B)^v = 1 - A^v + A^v B^v = 1$

若$A^v = 0$，有$(A \longrightarrow B)^v = 1 - A^v + A^v B^v = 1$

故$A \longrightarrow B$是永真式。

逻辑蕴含的性质

- $A \Rightarrow B$当且仅当$A \longrightarrow B$是永真式
- 充分性：如果$A \longrightarrow B$是永真式，那么$A \Rightarrow B$

证明：对任意指派v，有$(A \longrightarrow B)^v = 1$，若$A^v = 1$

有$(A \longrightarrow B)^v = 1 - A^v + A^v B^v = B^v = 1$

即$B^v = 1$，得证$A \Rightarrow B$

逻辑等价的性质

- $A \Leftrightarrow B$当且仅当$A \leftrightarrow B$是永真式
- 必要性：如果$A \Leftrightarrow B$，那么$A \leftrightarrow B$是永真式

证明：由$A \Leftrightarrow B$，对任意指派v，有$A^v = B^v$

$$(A \leftrightarrow B)^v = A^v B^v + (1 - A^v)(1 - B^v)$$

$$= (A^v)^2 + (1 - A^v)^2$$

$$= A^v + (1 - A^v)$$

$$= 1$$

得证 $A \leftrightarrow B$是永真式

逻辑等价的性质

- $A \Leftrightarrow B$当且仅当$A \leftrightarrow B$是永真式
- 充分性：如果$A \leftrightarrow B$是永真式，那么$A \Leftrightarrow B$

证明：由$A \leftrightarrow B$永真，知对任意指派v，有

$$
\begin{aligned}
(A \leftrightarrow B)^v &= A^v B^v + (1 - A^v)(1 - B^v) \\
&= A^v B^v + 1 - A^v - B^v + A^v B^v \\
&= 1
\end{aligned}
$$

从而，
$$
\begin{aligned}
A^v + B^v - 2A^v B^v &= A^v \times A^v + B^v \times B^v - 2A^v B^v \\
&= (A^v - B^v)^2 \\
&= 0
\end{aligned}
$$

从而$A^v = B^v$，由定义的推论知$A \Leftrightarrow B$

逻辑等价的性质

- 逻辑等价是$Form(L^P)$上的等价关系
  - 自反性：对任意的$A \in Form(L^P)$，有$A \Leftrightarrow A$
  - 对称性：对任意的$A, B \in Form(L^P)$，若$A \Leftrightarrow B$则有$B \Leftrightarrow A$
  - 传递性：对任意的$A, B, C \in Form(L^P)$，若$A \Leftrightarrow B$，$B \Leftrightarrow C$，则有$A \Leftrightarrow C$

常用的逻辑等价式

- 设A, B, C是任意的命题公式，分别用1和0表示重言式和矛盾式

1、(对合律) $\neg\neg A \Leftrightarrow A$

证明：对任意v，$(\neg\neg A)^v = 1 - (\neg A)^v$

$$= 1 - (1 - A)^v = A^v$$

2、(幂等律) $A \wedge A \Leftrightarrow A; A \vee A \Leftrightarrow A$

证明：对任意v, $(A \wedge A)^v = A^v A^v = A^v$

从而$A \wedge A \Leftrightarrow A$

对任意v, $(A \vee A)^v = A^v + A^v - A^v A^v$

$$= A^v + A^v - A^v = A^v$$

从而$A \vee A \Leftrightarrow A$

常用的逻辑等价式

- 设A, B, C是任意的命题公式，分别用1和0表示重言式和矛盾式

3、(交换律) $A \wedge B \Leftrightarrow B \wedge A$; $A \vee B \Leftrightarrow B \vee A$

证明：对任意v，有 $(A \wedge \mathrm{B})^v = A^v B^v$

$$= B^v A^v$$

$$= (B \wedge \mathrm{A})^v$$

从而有$A \wedge B \Leftrightarrow B \wedge A$

同理，对任意v，有 $(A \vee \mathrm{B})^v = A^v + B^v - A^v B^v$

$$= B^v + A^v - A^v B^v$$

$$= (B \vee \mathrm{A})^v$$

从而，$A \vee B \Leftrightarrow B \vee A$

常用的逻辑等价式

- 设A,B,C是任意的命题公式，分别用1和0表示重言式和矛盾式

4、（结合律）$(A\wedge B)\wedge C \Leftrightarrow A\wedge(B\wedge C);(A\vee B)\vee C \Leftrightarrow A\vee(B\vee C)$

证明：对任意v，$((A\wedge B)\wedge C)^v = (A\wedge B)^v C^v$

$$= (A^v B^v)C^v = A^v(B^v C^v) = (A\wedge(B\wedge C))^v$$

故$(A\wedge B)\wedge C \Leftrightarrow A\wedge(B\wedge C)$

对任意v，$((A\vee B)\vee C)^v = (A\vee B)^v + C^v - (A\vee B)^v C^v$

$$= A^v + B^v + C^v - A^v B^v - A^v C^v - B^v C^v + A^v B^v C^v$$

又有$(A\vee(B\vee C))^v = A^v + (B\vee C)^v - A^v(B\vee C)^v$

$$= A^v + B^v + C^v - B^v C^v - A^v B^v - A^v C^v + A^v B^v C^v$$

故$(A\vee B)\vee C \Leftrightarrow A\vee(B\vee C)$

常用的逻辑等价式

- 设A, B, C是任意的命题公式，分别用1和0表示重言式和矛盾式

5、（分配律）$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$

$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$

证明：对任意v，$((A \wedge B) \vee (A \wedge C))^v = A^v B^v + A^v C^v - A^v B^v A^v C^v$

$= A^v B^v + A^v C^v - A^v B^v C^v$

$= (A \wedge (B \vee C))^v$

故$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$

同理可证 $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$

常用的逻辑等价式

- 设A,B,C是任意的命题公式，分别用1和0表示重言式和矛盾式

6、（吸收律） $A\wedge(A\vee B)\Leftrightarrow A; A\vee(A\wedge B)\Leftrightarrow A$

证明：对任意v，$(A\wedge(A\vee B))^v=A^v(A\vee B)^v$

$$=A^v(A^v+B^v-A^vB^v)$$

$$=A^vA^v+A^vB^v-A^vA^vB^v$$

$$=A^v+A^vB^v-A^vB^v=A^v$$

故$A\wedge(A\vee B)\Leftrightarrow A$，同理可证$A\vee(A\wedge B)\Leftrightarrow A$

常用的逻辑等价式

- 设A,B,C是任意的命题公式，分别用1和0表示重言式和矛盾式

7、（德摩根律）$\neg(A\vee B)\Leftrightarrow\neg A\wedge\neg B$

$$\neg(A\wedge B)\Leftrightarrow\neg A\vee\neg B$$

证明：对任意v，$(\neg(A\vee B))^v=1-(A\vee B)^v$

$$=1-A^v-B^v+A^vB^v$$

$$(\neg A\wedge\neg B)^v=(\neg A)^v(\neg B)^v$$

$$=(1-A)^v(1-B)^v$$

$$=1-A^v-B^v+A^vB^v$$

故$\neg(A\vee B)\Leftrightarrow\neg A\wedge\neg B$，同理可证$\neg(A\wedge B)\Leftrightarrow\neg A\vee\neg B$

常用的逻辑等价式

- 设A, B, C是任意的命题公式，分别用1和0表示重言式和矛盾式

1、(对合律) $\neg\neg A \Leftrightarrow A$

2、(幂等律) $A \wedge A \Leftrightarrow A; A \vee A \Leftrightarrow A$

3、(交换律) $A \wedge B \Leftrightarrow B \wedge A; A \vee B \Leftrightarrow B \vee A$

4、(结合律) $(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C); (A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$

5、(分配律) $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C); A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$

6、(吸收律) $A \wedge (A \vee B) \Leftrightarrow A; A \vee (A \wedge B) \Leftrightarrow A$

7、(德摩根律) $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B; \neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$

8、(同一律) $A \wedge 1 \Leftrightarrow A; A \vee 0 \Leftrightarrow A$

9、(零一律) $A \wedge 0 \Leftrightarrow 0; A \vee 1 \Leftrightarrow 1$

10、(排中律) $A \wedge \neg A \Leftrightarrow 0; A \vee \neg A \Leftrightarrow 1$

代入定理

- 代入定理：设A是含有命题变元p的永真式，那么将A中p的所有出现均代换为命题公式B，得到的公式（称为A的代入实例）仍为永真式。

例如，$p \to (q \to p)$

$$A^v = [A(p)]^v = [A(p^v)]^v, [A(B)]^v = [A(B^v)]^v,$$

替换定理

- 替换定理：设命题公式A含有子公式C（C为A中的符号串并为命题公式），如果$C \Leftrightarrow D$,那么将A中子公式C的某些出现（未必全部）用D替换得到公式B，必有$A \Leftrightarrow B$

例：试证$P \to Q \Leftrightarrow \neg P \vee Q$

证明：$(P \to Q)^v = 1 - P^v + P^v Q^v$

$$(\neg P \vee Q)^v = (\neg P)^v + Q^v - (\neg P)^v Q^v$$

$$= 1 - P^v + Q^v - (1 - P)^v Q^v$$

$$= 1 - P^v + P^v Q^v$$

故，$P \to Q \Leftrightarrow \neg P \vee Q$

根据替换定理$(P \to Q) \wedge (R \to (P \to Q)) \Leftrightarrow ?$

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

替换定理

- 替换定理：设命题公式A含有子公式C（C为A中的符号串并为命题公式），如果$C \Leftrightarrow D$,那么将A中子公式C的某些出现（未必全部）用D替换得到公式B，必有$A \Leftrightarrow B$

证明：对命题公式A的长度用第二数学归纳法证明。

1、若$|A| = |C|$，则$A = C$。对A中子公式C的某些出现用D替换，

- 要么没有用D替换C 得到$B = C$，$C = A$；则$A \Leftrightarrow B$
- 要么用D替换C 得到$B = D$，$D \Leftrightarrow C$，$C = A$。则$A \Leftrightarrow B$

2、若$A = \neg A_1$，即$|A_1| = |A| - 1$，C 为A的子公式，必然C 为A_1的子公式。将A中子公式C的某些出现用D替换得到公式B，即将A_1中子公式C的某些出现用D替换得到公式B_1，有$B = \neg B_1$。由归纳假设知$A_1 \Leftrightarrow B_1$，对于任意的指派v：

$$A^v = (\neg A_1)^v = 1 - {A_1}^v = 1 - {B_1}^v = (\neg B_1)^v = B^v$$

由逻辑等价定义的推论得$A \Leftrightarrow B$。

替换定理

3、若 $A = A_1 \to A_2$，$|A_1|, |A_2| < |A|$。C 必为 A_1, A_2 的子公式。那么 $B = B_1 \to B_2$ 由归纳假设知 $A_1 \Leftrightarrow B_1$，$A_2 \Leftrightarrow B_2$。对于任意的指派 v:

$A^v = (A_1 \to A_2)^v = 1 - {A_1}^v + {A_1}^v {A_2}^v = 1 - {B_1}^v + {B_1}^v {B_2}^v = (B_1 \to B_2)^v = B^v$，

由逻辑等价定义的推论得 $A \Leftrightarrow B$

4、若 $A = A_1 \wedge A_2$，$|A_1|, |A_2| < |A|$。C 必为 A_1, A_2 的子公式 $B = B_1 \wedge B_2$，由归纳假设知 $A_1 \Leftrightarrow B_1$，$A_2 \Leftrightarrow B_2$。对于任意的指派 v:

$$A^v = (A_1 \wedge A_2)^v = {A_1}^v {A_2}^v = {B_1}^v {B_2}^v = (B_1 \wedge B_2)^v = B^v$$

由逻辑等价定义的推论得 $A \Leftrightarrow B$

5、若 $A = A_1 \vee A_2$，同理可证

6、若 $A = A_1 \leftrightarrow A_2$，同理可证