离散数学：数理逻辑：重言式

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

命题公式的分类

- 命题公式可以从真值的角度进行**分类**
- **重言式**：（永真式）tautology
  命题变元的**所有**赋值都是命题公式的**成真**赋值
- **矛盾式**（永假式、不可满足式）contradiction
  命题变元的**所有**赋值都是命题公式的**成假**赋值
- **可满足式**(contingency)
  命题公式**至少有一个**成真赋值

需要分清的概念

- 永真式**都是**可满足式
- 矛盾式**都不是**可满足式
- 非永真式**并不都是**永假式
- 如果**A**是永真式，则**¬A**就是永假式，反之亦然

重言式的例子和证明

- 例子：对于**任何公式A**
- **A∨¬A**是重言式（排中律）
- **A∧¬A**是矛盾式（矛盾律）
- 采用命题公式的**真值表证明**重言式
- 证明(p∨q)∧¬p→q是重言式

p	q	p∨q	¬p	(p∨q)∧¬p	(p∨q)∧¬p→q
0	0	0	1	0	1
0	1	1	1	1	1
1	0	1	0	0	1
1	1	1	0	0	1

离散数学：数理逻辑：逻辑等价式和逻辑蕴涵式

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

逻辑等价式(logical equivalent)

- 当命题公式**A↔B**是**重言式**时，则称A逻辑等价于B，记作**A ⟚ B**，称作**逻辑等价式**
- 也可以理解为公式A和公式B**等值**
- 逻辑等价体现了两个公式之间的一种**关系**：在任何赋值状况下它们都等值

一些重要的逻辑等价式（A,B,C是任意公式）

- E1：$\neg\neg A \mathrel{|\!\!=\!\!|} A$（双重否定律）
- E2：$A\vee A \mathrel{|\!\!=\!\!|} A$，$A\wedge A \mathrel{|\!\!=\!\!|} A$（幂等律）
- E3：$A\vee B \mathrel{|\!\!=\!\!|} B\vee A$， $A\wedge B \mathrel{|\!\!=\!\!|} B\wedge A$（交换律）
- E4：$(A\vee B)\vee C \mathrel{|\!\!=\!\!|} A\vee(B\vee C)$，$(A\wedge B)\wedge C \mathrel{|\!\!=\!\!|} A\wedge(B\wedge C)$（结合律）
- E5：$A\wedge(B\vee C) \mathrel{|\!\!=\!\!|} (A\wedge B)\vee(A\wedge C)$，$A\vee(B\wedge C) \mathrel{|\!\!=\!\!|} (A\vee B)\wedge(A\vee C)$（分配律）
- E6：$\neg(A\vee B) \mathrel{|\!\!=\!\!|} \neg A\wedge\neg B$， $\neg(A\wedge B) \mathrel{|\!\!=\!\!|} \neg A\vee\neg B$（德摩根律）
- E7：$A\vee(A\wedge B) \mathrel{|\!\!=\!\!|} A$， $A\wedge(A\vee B) \mathrel{|\!\!=\!\!|} A$（吸收律）
- E8：$A\rightarrow B \mathrel{|\!\!=\!\!|} \neg A\vee B$（蕴涵等值式）

一些重要的逻辑等价式（A,B,C是任意公式）

- E9：$A\leftrightarrow B \mathrel{|\!\!=\!\!|} (A\rightarrow B)\wedge(B\rightarrow A)$（等价等值式）
- E10：$A\vee t \mathrel{|\!\!=\!\!|} t$，$A\wedge f \mathrel{|\!\!=\!\!|} f$（零律）
- E11：$A\vee f \mathrel{|\!\!=\!\!|} A$，$A\wedge t \mathrel{|\!\!=\!\!|} A$（同一律）
- E12：$A\vee\neg A \mathrel{|\!\!=\!\!|} t$， $A\wedge\neg A \mathrel{|\!\!=\!\!|} f$（排中律和矛盾律）
- E13：$\neg t \mathrel{|\!\!=\!\!|} f$，$\neg f \mathrel{|\!\!=\!\!|} t$
- E14：$A\wedge B\rightarrow C \mathrel{|\!\!=\!\!|} A\rightarrow(B\rightarrow C)$
- E15：$A\rightarrow B \mathrel{|\!\!=\!\!|} \neg B\rightarrow\neg A$（假言易位）
- E16：$(A\rightarrow B)\wedge(A\rightarrow\neg B) \mathrel{|\!\!=\!\!|} \neg A$（归谬论）
- E17：$A\leftrightarrow B \mathrel{|\!\!=\!\!|} (A\wedge B)\vee(\neg A\wedge\neg B)$（等价等值式2）

逻辑蕴涵式(logical implication)

- 当命题公式$A\rightarrow B$是重言式时，则称A逻辑蕴涵B，记作$A\models B$，称作逻辑蕴涵式
- 也可以理解为公式A的所有成真赋值都是公式B的成真赋值
- 每个逻辑等价式可以看作两个逻辑蕴涵式，也就是说$A \mathrel{|\!\!=\!\!|} B$也有$A\models B, B\models A$
  A和B等值，所以A→B和B→A都是重言式
- 逻辑蕴涵体现了两个公式AB之间的另一种关系：在任何赋值状况下只要A真，B都真

一些重要的逻辑蕴涵式（A,B,C是任意公式）

- I1：$A\models A\vee B$
- I2：$A\wedge B\models A$
- I3：$A\wedge(A\rightarrow B)\models B$
- I4：$(A\rightarrow B)\wedge\neg B\models\neg A$
- I5：$\neg A\wedge(A\vee B)\models B$
- I6：$(A\rightarrow B)\wedge(B\rightarrow C)\models A\rightarrow C$
- I7：$(A\rightarrow B)\wedge(C\rightarrow D)\models(A\wedge C)\rightarrow(B\wedge D)$
- I8：$(A\leftrightarrow B)\wedge(B\leftrightarrow C)\models A\leftrightarrow C$

逻辑结果

- 逻辑蕴涵经常会被推广为$\Gamma\models B$的形式
- 其中Γ是一系列公式，表示B是Γ的逻辑结果
- 即：使Γ中每一个公式成真的赋值，都是公式B的成真赋值
- 即Γ中的所有公式的合取逻辑蕴涵B
- 当Γ中仅包含一个公式A时，就是$A\models B$；
- 如果Γ中不包含任何公式，记做$\models B$，表示“B永真”

逻辑等价式和逻辑蕴涵式的几个重要性质

- 命题公式关系的自反、对称、传递等性质
- $A \mathrel{|\!\!=\!\!|} B$当且仅当$\models A\leftrightarrow B$
- $A\models B$当且仅当$\models A\rightarrow B$
- 若$A \mathrel{|\!\!=\!\!|} B$，则$B \mathrel{|\!\!=\!\!|} A$
- 若$A \mathrel{|\!\!=\!\!|} B$， $B \mathrel{|\!\!=\!\!|} C$，则$A \mathrel{|\!\!=\!\!|} C$
- 若$A\models B$，则$\neg B\models\neg A$
- 若$A\models B$， $B\models C$，则$A\models C$
- 若$A\models B$，$A \mathrel{|\!\!=\!\!|} A'$ ，$B \mathrel{|\!\!=\!\!|} B'$ ，则$A'\models B'$

离散数学：数理逻辑：代入原理和替换原理

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

重言式的代入原理(rule of substitution)

- 将**重言式A**中的某个**命题变元p**的所有出现都代换为**命题公式B**，
- 得到的命题公式记作**A(B/p)**，A(B/p)也是**重言式**。
- 因为重言式A的真值与p的取值状况无关，恒为t，
- 所以将p全部代换后的公式A(B/p)的真值也恒为t

重言式的代入原理(rule of substitution)

- **注意**：仅**代换部分出现**本原理不成立，为什么？
- **注意**：如果B中包含了p或者A中的其它变元，本原理还成立么？

命题公式的替换原理(rule of replacement)

- 将**命题公式A**中的**子公式C**的**部分**出现替换为和C逻辑等价的**公式D**（C⟚D），
- 得到的命题公式记作B，则**A⟚B**。
- 因为C和D（在任何赋值下）等值，所以用D替换C不会改变A的真值
- **注意**：不要求全部出现都替换

代入原理RS与替换原理RR的区别

	代入原理RS	替换原理RR
使用对象	任意永真式	任意命题公式
代换对象	任意命题变元	任意子公式
代换物	任意命题公式	任意与代换对象等价的命题公式
代换方式	代换同一命题变元的所有出现	代换子公式的某些出现
代换结果	仍为永真式	与原公式等价

离散数学：数理逻辑：证明逻辑等价式和蕴涵式

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

证明逻辑等价式和逻辑蕴涵式

- **真值表法**：要证明A ⫤⊨ B，A ⊨B，只要：
  分别列出A↔B和A→B的真值表，最后一列全为真即可。
- **对赋值进行讨论**：要证明A ⊨B，只要证明：
  A的任意一个成真赋值都是B的成真赋值，或者
  B的任意一个成假赋值都是A的成假赋值。
  ☛如果证明了A ⊨B和B ⊨A，那么就证明了A ⫤⊨ B。
- **推演法**：利用已知的重言式、逻辑等价式和逻辑蕴涵式，采用**代入原理**和**替换原理**进行推演。

讨论赋值法证明逻辑等价式：(A∨B)→C ⫤⊨ (A→C)∧(B→C)

- **先证明(A∨B)→C ⊨(A→C)∧(B→C)**
- 假设α是(A∨B)→C任意一个**成真赋值**，这样会有两种情况：
- α(A∨B)=f：于是α(A)=α(B)=f，就有α(A→C)=α(B→C)=t
- 或者，
- α(A∨B)=t，α(C)=t：于是α(A→C)=α(B→C)=t
- 上述两种情况都得到α((A→C)∧(B→C))=t，得证。

讨论赋值法证明逻辑等价式：(A∨B)→C ⫤⊨ (A→C)∧(B→C)

- **再证明(A→C)∧(B→C) ⊨(A∨B)→C**
- 反过来，假设α是(A∨B)→C任意一个**成假赋值**，这样只有一种情况：
- α(A∨B)=t，α(C)=f
- 当α(A)=t，α(C)=f时，α(A→C)=f；
- 当α(B)=t，α(C)=f时，α(B→C)=f，
- 不管如何，都有α((A→C)∧(B→C))=f
- 得证。

推演法证明逻辑等价式：(A∨B)→C ⫤⊨ (A→C)∧(B→C)

- (A∨B)→C
- ⫤⊨ ¬(A∨B)∨C（**蕴涵等值式，代入原理**）
- ⫤⊨ (¬A∧¬B)∨C（**德摩根律，替换原理**）
- ⫤⊨ (¬A∨C)∧(¬B∨C)（**分配律，代入**）
- ⫤⊨ (A→C)∧(¬B∨C)（**蕴涵等值式，替换**）
- ⫤⊨ (A→C)∧(B→C)（**蕴涵等值式，替换**）

推演法证明逻辑蕴涵式：A∧B ⊨¬A→(C→B)

- A∧B
- ⊨B（**I2：A∧B ⊨A**）
- ⊨¬C∨B（**I1：A ⊨A∨B，代入**）
- ⊨C→B（**蕴涵等值式，代入**）
- ⊨A∨(C→B)（**I1：A ⊨A∨B，代入**）
- ⊨¬A→(C→B)（**蕴涵等值式，代入**）

离散数学：数理逻辑：范式及基本术语

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

范式：概念及基本术语

- 每个命题公式都会存在**很多**与之逻辑等价的公式
- **范式**：在命题公式的多个逻辑等价的形式中，较为符合“**标准**”或“**规范**”的一种形式

范式：概念及基本术语

- **文字**(literals)：命题常元、变元和它们的否定
- 前者称**正**文字，后者称**负**文字，如：$p, \neg q, t$
- **析取子句**(disjunctive clauses)：文字或者若干文字的析取，如：p, $p\vee q$, $\neg p\vee q$
- **合取子句**(conjunctive clauses)：文字或者若干文字的合取，如：p, $p\wedge q$, $\neg p\wedge q$
- **互补文字对**(complemental pairs of literals)：指一对正文字和负文字，如：p和$\neg p$

析取范式(disjunctive normal form)

- 公式A’称作公式A的**析取范式**，如果：
- A’ $\Leftrightarrow$ A
- A’为合取子句或者若干合取子句的析取
- $p\to q$的析取范式为**$\neg p\vee q$**（合取子句$\neg p$和q的析取）
- $((p\to q)\wedge\neg p)\vee\neg q$的析取范式为**$\neg p\vee(q\wedge\neg p)\vee\neg q$**

合取范式(conjunctive normal form)

- 公式A’称作公式A的**合取范式**，如果：
- A’ $\Leftrightarrow$ A
- A’为析取子句或者若干析取子句的合取
- $p\to q$的合取范式为**$\neg p\vee q$**（析取子句$\neg p\vee q$）
- $((p\to q)\wedge\neg p)\vee\neg q$的合取范式为**$(\neg p\vee t)\wedge(\neg p\vee\neg q)$**或**$\neg p\vee\neg q$**

离散数学：数理逻辑：求范式一般步骤

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

求命题公式的范式

- 利用**逻辑等价式**和**代入原理**、**替换原理**，可以求出任一一个公式的析取范式和合取范式
- 求$\neg p\to\neg(p\to q)$的析取范式及合取范式
- $\neg p\to\neg(p\to q)$
- $\Leftrightarrow\neg p\to\neg(\neg p\vee q)$
- $\Leftrightarrow p\vee\neg(\neg p\vee q)$
- $\Leftrightarrow p\vee(p\wedge\neg q)$（**析取范式**）
- $\Leftrightarrow(p\vee p)\wedge(p\vee\neg q)$
- $\Leftrightarrow p\wedge(p\vee\neg q)$（**合取范式**）
- $\Leftrightarrow p$

范式用于重言式和矛盾式的识别

- 重言式识别
- 合取范式中每个析取子句都包含了至少一个互补文字对：(p∨¬p∨q)∧(p∨q∨¬q)
- 矛盾式识别
- 析取范式中每个合取子句都包含了至少一个互补文字对：(p∧¬p∧q)∨(p∧q∧¬q)

求析取范式或合取范式的一般步骤

- 消去公式中的联结词→和↔
- p→q化为¬p∨q（蕴涵等值式）
- p↔q化为(¬p∨q)∧(p∨¬q)或者(p∧q)∨(¬p∧¬q)（等价等值式）
- 利用德摩根律将否定联结词¬向内深入，最后只作用于文字，再将¬¬p化为p
- 利用分配律，最后得到需要的析取或者合取范式

范式的唯一性问题

- 一个公式的析取范式或合取范式都不是唯一的
- p, p∨(p∧¬q), (p∧q)∨(p∧¬q)都是¬p→¬(p→q)的析取范式
- p, p∧(p∨¬q), (p∨q)∧(p∨¬q)都是¬p→¬(p→q)的合取范式
- 公式的析取范式有可能同时又是合取范式
- ¬p∨q既是p→q的析取范式又是合取范式
- 能否找到“最为规范”的范式？
- 具备唯一性的范式

离散数学：数理逻辑：主范式

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

主范式的定义

- 主析取范式(major disjunctive form)
- 公式A'称作公式A(p1, p2, ...pn)的主析取范式，如果：
- A'是A的析取范式
- A'中每一个合取子句里p1, p2, ...pn均恰出现一次
- 主合取范式(major conjunctive form)
- 公式A'称作公式A(p1, p2, ...pn)的主合取范式，如果：
- A'是A的合取范式
- A'中每一个析取子句里p1, p2, ...pn均恰出现一次

主范式的存在及唯一性？

- 主析取范式（或主合取范式）存在吗？
- 如果存在的话，唯一吗？
- 我们以主析取范式为例，来证明存在性和唯一性

主析取范式存在唯一性证明：约定

- 首先，合取子句中的文字按照其包含的变元下标**从小到大排列**
- 对于包含所有变元p1, p2, ...pn的并排列好文字顺序的合取子句，我们称为**极小项**(min term)，记作m_i
- 其中i是一个整数，i对应的**n位二进制**表示描述了对应下标的变元在合取子句中的否定状态
- 如果该位是**0**，表示合取子句中的该位是一个**负文字**，否则是正文字
- 例p1∧p2∧p3记作m_7（7=111）；p1∧¬p2∧¬p3记作m_4（4=100）
- **主析取范式是极小项按照其下标从小到大排列的析取**

主析取范式存在唯一性证明：极小项赋值引理

- 极小项只有**唯一**的成真赋值，
- 且成真赋值中每个变元的取值等于**极小项下标**的二进制形式中变元下标所对应的二进制位的值：
- p1∧p2∧p3（m**7**）的唯一成真赋值是**p1=1, p2=1, p3 =1**
- p1∧¬p2∧¬p3（m**4**）的唯一成真赋值是**p1=1, p2=0, p3 =0**

主析取范式存在唯一性证明：主析取范式的成真赋值

- 极小项和主析取范式的关系
- 主析取范式包含的极小项的成真赋值也是主析取范式的**成真赋值**
- 主析取范式的任一一个成真赋值是其**包含**的某个极小项的成真赋值
- 主析取范式**不包含**的极小项的成真赋值是主析取范式的成假赋值

主析取范式存在唯一定理：存在性证明

- **任何命题公式A(p1, p2, ...pn)的主析取范式都是存在的，并且是唯一的。**
- 假设A'是公式A(p1, p2, ...pn)的析取范式
- 如果A'中某个合取子句Ai既不包含pj，也不包含¬pj，那么我们将Ai展成如下形式：
- Ai ⊨| Ai∧1 ⊨| Ai∧(pj∨¬pj) ⊨| **(Ai∧pj) ∨(Ai∧¬pj)**
- 将合取子句中重复出现的命题变元，矛盾式消去，将重复出现的合取子句消去
- p∧p ⊨| p； p∧¬p ⊨| 0； Ai∨Ai ⊨| Ai
- 最后将所有的合取子句**整理变元顺序**，成为**极小项**，并得到**主析取范式A''**

主析取范式存在唯一定理：唯一性证明

- 反证法：**假设**公式A(p1, p2, ...pn)存在两个**不同**的主析取范式**B**和**C**
- 由于A ⊨| B且A ⊨| C，所以B ⊨| C
- 因为B和C是两个**不同**的主析取范式，那么一定存在**某个极小项mi**只出现在B或者只出现在C中，不妨设mi只出现在B中，不出现在C中，这样：
- mi的成真赋值是**B的成真**赋值，却是**C的成假**赋值
- **与B ⊨| C矛盾**
- 所以B和C必然相同，也就是说公式A(p1, p2, ...pn)的主析取范式是**唯一**的
- 存在性证明还给出了主析取范式的**构造步骤**。

命题公式A(p1, p2, ...pn)的等值分类

- 具有相同主析取范式的公式都是**等值**的，属于同一个等值类，否则属于不同的等值类
- 虽然公式的数量无限多，但**等值类的数量**是**有限**的：
- 极小项的数量为**$N=2^n$**；
- 由极小项**组合**成的主析取范式的数量为**2^N**；
- 等值类的数量等于主析取范式的数量

主合取范式：具有和主析取范式对称的性质

- **极大项**和**成假赋值**
- 主合取范式的**存在性**和**唯一性**
- 主合取范式的**构造步骤**
- 命题公式A(p1, p2, …pn)的**等值分类**

离散数学：数理逻辑：联结词集完备性

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

联结词集完备性：真值函数

- 每一个等值类都对应唯一的真值函数 **F(p1, p2, …pn)**
- 真值函数每个变元的**定义域**是{0, 1}，**值域**是{0, 1}
- 真值函数与相应等值类中的每个命题公式**等值**
  特别的，与主析取范式（或主合取范式）等值
- 真值函数与等值类是**一一对应**的

联结词集完备性：功能完备集

- 如果任意一个真值函数都可以用**仅**包含某个**联结词集**中的联结词的命题公式表示，则称这个联结词集为**功能完备集**
- 要点：命题公式中用到的所有联结词
- 目前使用的**{¬,∧,∨,→,↔}**是功能完备集
- 还有其它的功能完备集吗？
  我们注意到任意真值函数都可以用**主析取范式**来表示，而主析取范式中只有三种联结词：¬,∧,∨
- **{¬,∧,∨}**是功能完备集

冗余联结词

- 在一个联结词集中，如果某个联结词可以用集合中**其它联结词**来**定义**，则这个联结词称作冗余联结词
- {¬,∧,∨,→,↔}是否存在冗余联结词？
- **A→B ╞╡ ¬A∨B**，所以**→**是冗余联结词
- {¬,∧,∨,↔}中还有冗余联结词吗？
- {¬,∧,∨}中还有冗余联结词吗？

功能完备集证明和极小集

- {¬,→}是功能完备集
- 证明思路：从一个**已知**的功能完备集中去掉冗余联结词，直至得到{¬,→}
- **极小**的功能完备集
- 如果一个功能完备集中**不含冗余**联结词，则称这个功能完备集为极小的。
- {¬,→}，{¬,∧}，{¬,∨}都是极小功能完备集

仅包含单个联结词的功能完备集

- 定义联结词↓（Peirce记号）
- $p{\downarrow}q \dashv\vDash \neg(p\vee q)$
- $\{\downarrow\}$是功能完备集
- 证明思路：用↓去定义已知功能完备集中的每一个联结词，如$\{\neg,\vee\}$
- $\neg p \dashv\vDash \neg(p\vee p) \dashv\vDash p{\downarrow}p$
- $p\vee q \dashv\vDash \neg\neg(p\vee q)$
- $\dashv\vDash \neg(p{\downarrow}q) \dashv\vDash (p{\downarrow}q){\downarrow}(p{\downarrow}q)$

非功能完备集证明

- 如何证明某个联结词集合不是功能完备集？
- 并没有统一的证明方法
- $\{\wedge\}$不是功能完备集，因为不能构成矛盾式
- 不能仅用重言式、逻辑等价式和代入、替换原理推演证明

非功能完备集证明

- $\{\neg,\leftrightarrow\}$不是功能完备集，
- 我们注意到，由$\{\neg,\leftrightarrow\}$组成的命题公式其成真赋值的个数总是偶数，
- 不能表示那些成真赋值个数为奇数的真值函数

离散数学：数理逻辑：形式系统和证明、演绎

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

形式系统

- 重言式反应了人类逻辑思维的基本规律
- 排中律$A\vee\neg A \dashv\vDash t$
- 矛盾律 $A\wedge\neg A \dashv\vDash f$
- 假言推理$A\wedge(A\rightarrow B) \vDash B$
- 归谬推理$(A\rightarrow B)\wedge\neg B \vDash \neg A$
- 穷举推理$(A\vee B)\wedge(A\rightarrow C)\wedge(B\rightarrow C) \vDash C$

形式系统

- 真值计算、以代入原理、替换原理进行推演
- 难以反应人类思维推理过程，
- 需要建立严密的符号推理体系

形式系统

- 形式系统是一个**符号体系**
- 系统中的概念由符号表示，推理过程即符号变换的过程
- 以若干最基本的重言式作为基础，称作**公理**（axioms）
- 系统内符号变换的依据是若干确保由重言式导出重言式的规则，称作**推理规则**（rules of inference）
- 公理和推理规则确保系统内由**正确的前提**总能得到**正确的推理结果**

证明与演绎：证明Proof

- 公式序列A1,A2,…,Am称作Am的一个**证明**，如果Ai(1≤i≤m)：
- 或者是**公理**；
- 或者由Aj1,…,Ajk(j1,…,jk<i)用**推理规则推得**。
- 当这样的证明存在时，称Am为系统的**定理**(theorem)，记作├*Am（*是形式系统的名称），或者简记为**├Am**

证明与演绎：演绎Deduction

- 设**Γ**为一公式集合。公式序列A1,A2,…,Am称作Am的**以Γ为前提的演绎**，如果Ai(1≤i≤m)：
- 或者是**Γ中的公式**
- 或者是**公理**
- 或者由Aj1,…,Ajk(j1,…,jk<i)用**推理规则推得**。

证明与演绎：演绎Deduction

- 当有这样的演绎时， Am称作Γ的**演绎结果**，
- 记作Γ├*Am（*是形式系统的名称），或者简记为**Γ├Am**
- 称Γ和Γ的成员为Am的**前提**(hypothesis)
- **证明**是**演绎**在Γ为空集时的**特例**

离散数学：数理逻辑：命题演算形式系统

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

命题演算形式系统PC(Proposition Calculus)

- 我们将命题以及重言式变换演算构造为形式系统，称为**命题演算形式系统PC**
- 首先，是PC的**符号系统**
- **命题变元**：p,q,r,s,p1,q1,r1,s1,…
- **命题常元**：t,f
- **联结词**：¬,→（注意是**功能完备集**）
- **括号**：(,)
- **命题公式**：（高级成分，规定了字符的合法组合方式）
  命题变元和命题常元是公式
  如果A,B是公式，则(¬A)，(A→B)均为公式（结合优先级和括号省略约定同前）
  只有有限次使用上面两条规则得到的符号串才是命题公式

命题演算形式系统PC(Proposition Calculus)

- PC的**公理**（A,B,C表示任意公式）
- **A1**:A→(B→A)
- **A2**:(A→(B→C))→((A→B)→(A→C))
- **A3**:(¬A→¬B)→(B→A)
- PC的**推理规则**（A,B表示任意公式）
- A, A→B / B（**分离规则**）

PC的性质：合理性Soundness

- 如果公式A是系统PC的**定理**，则A是**重言式**（如果$\vdash_{PC}$A，则$\models$A）
- 如果A是公式集合Γ的**演绎结果**，那么A是Γ的**逻辑结果**（如果Γ$\vdash_{PC}$A，则Γ$\models$A）
- 说明了PC中的定理和演绎结果都**合乎逻辑**

PC的性质：合理性Soundness说明

- 首先，PC中的公理A1,A2,A3都是**重言式**；
- 其次，PC的分离规则是“**保真**”的，就是如果A真，A→B真，总有B真。
- 这样：
- 由公理和规则**导出**的定理都是**重言式**
- 由**Γ**、公理和规则**导出**的公式，在Γ中的公式都为**真**时也为**真**

PC的性质：一致性(consistency)

- 没有公式A，
- 使得$\vdash_{PC}$A和$\vdash_{PC}$¬A同时成立（**不会出现自相矛盾**）
- 由PC的合理性容易证明

PC的性质：完备性(completeness)

- 如果公式A是**重言式**，
- 则A一定是PC中的**定理**（如果$\models$A，则$\vdash_{PC}$A）
- 如果公式A是公式集合Γ的**逻辑结果**，
- 则A一定是Γ的**演绎结果**（如果Γ$\models$A，则Γ$\vdash_{PC}$A）。
  证明很难，略。
- **合乎逻辑**的命题，在PC中一定能**推导**出来

离散数学：数理逻辑：PC中的证明

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

证明定理：$\vdash_{PC}A\to A$

- 1] $(A\to((A\to A)\to A))\to((A\to(A\to A))\to(A\to A))$：**公理A2**
- 2] $A\to((A\to A)\to A)$：**公理A1**
- 3] $(A\to(A\to A))\to(A\to A)$：**对1,2使用分离规则**
- 4] $A\to(A\to A)$：**公理A1**
- 5] $A\to A$：**对3,4使用分离规则**
- 上述5个公式构成的**序列**，即为**证明**

PC的公理（A,B,C表示任意公式）
A1:$A\to(B\to A)$
A2:$(A\to(B\to C))\to((A\to B)\to(A\to C))$
A3:$(\neg A\to\neg B)\to(B\to A)$

演绎：$\{A,B\to(A\to C)\}\vdash B\to C$

- 1] A：**前提**
- 2] $B\to(A\to C)$：**前提**
- 3] $A\to(B\to A)$：**公理A1**
- 4] $B\to A$：**对1,3用分离规则**
- 5] $(B\to(A\to C))\to((B\to A)\to(B\to C))$：**公理A2**
- 6] $(B\to A)\to(B\to C)$：**对2,5用分离规则**
- 7] $B\to C$：**对4,6用分离规则**

PC的公理（A,B,C表示任意公式）
A1:$A\to(B\to A)$
A2:$(A\to(B\to C))\to((A\to B)\to(A\to C))$
A3:$(\neg A\to\neg B)\to(B\to A)$

离散数学：数理逻辑：三个元定理

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

演绎定理

- 对任意公式集合**Γ**和公式**A,B**
- $\Gamma\vdash A\to B$当且仅当$\Gamma\cup\{A\}\vdash B$
- 当$\Gamma=\varnothing$时，$\vdash A\to B$当且仅当$\{A\}\vdash B$，或$A\vdash B$
- 证明**必要性**：
- 有$A\to B$，加上A，分离规则得到B
- 证明**充分性**：
- 有B，以及公理A1:$B\to(A\to B)$，分离规则得到$A\to B$

归谬定理

- 对任何公式集合**Γ**和公式**A,B**，
- 若$\Gamma\cup\{\neg A\}\vdash B$，$\Gamma\cup\{\neg A\}\vdash\neg B$，
- 那么$\Gamma\vdash A$
- 意义：
- 如果同一组前提能推导出**相互矛盾**的结果，说明这组前提之间相互**不一致**，
- 也就是说总有一些前提是其余前提的**对立面**。

穷举定理

- 对任何公式集合**Γ**和公式**A,B**
- 若$\Gamma\cup\{\neg A\}\vdash B$，$\Gamma\cup\{A\}\vdash B$
- 那么$\Gamma\vdash B$
- 意义：
- 如果一个前提能推出结论，这个前提的**反面**也能推出同样的结论，
- 说明结论的**成立**与此前提是否成立**无关**。

元定理简化证明：⊢¬¬A→A

- ¬¬A→(¬A→¬¬A)：公理A1
- 由演绎定理就有：{¬¬A,¬A}⊢¬¬A
- ¬A→(¬¬A→¬A)：公理A1
- 由演绎定理证明了：{¬A,¬¬A}⊢¬A，也就是{¬¬A, ¬A}⊢¬A
- 上面两个前提，用归谬定理得到{¬¬A}⊢A
- 再用演绎定理，有⊢¬¬A→A

元定理简化证明：⊢(A→C)→(((B→C)→((¬A→B)→C))

- 根据演绎定理，只需要证明{A→C,B→C,¬A→B}⊢C
- 因为{A→C,B→C,¬A→B,A}⊢C是显然的
- {A→C,B→C,¬A→B,¬A}⊢C是易证的
- 根据穷举定理{A→C,B→C,¬A→B}⊢C得证

离散数学：数理逻辑：定理判定问题

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

形式系统构造了一个符号串集合

- 形式系统定义就是符号串集合的构造性定义
- 符号体系规定了符号串可能包含的字符（或字符的合法组合模式，词）
  如PC中的命题变元、常元和公式的定义
- 公理规定了几个集合中的符号串（或者这种符号串的模式）
  如PC中的公理，实质是公理模式
- 推理规则规定了从集合中已知符号串变换生成集合中其它符号串的方法
  如PC中的分离规则

定理判定问题：符号串的构造过程

- 形式系统中的定理就是在集合中的符号串
- 定理的证明过程就是符号串的构造过程
- 这个过程需要在有限步内结束

定理判定问题：定理判定问题

- 给定一个命题公式，判定是否形式系统中的定理，给出定理的证明
- 给定一个符号串，判定是否在集合里，给出构造的过程
- 能否单靠形式系统本身的公理和推理规则在有限步骤内判定定理和非定理？

一个简单的形式系统MIU

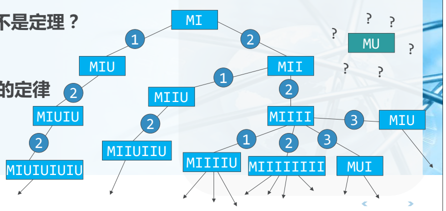
- 符号系统：M, I, U组成的串
- 初始串：MI
  公理：MI
- 规则1：如果串的最后一个符号是I，则可以加上一个U
  如果xI是定理，那么xIU也是定理
- 规则2：如果串符合Mx，则可以再加上x而生成Mxx，x代表任何一个由M,I,U组成的串
  如果Mx是定理，那么Mxx也是定理

一个简单的形式系统MIU

- 规则3：如果串中出现连续3个I，则可以用U代替III得到新串
  如果xIIIy是定理，那么xUy也是定理
- 规则4：如果串中出现UU，则可以将UU删去得到新串
  如果xUUy是定理，那么xy也是定理
- 判定问题：MU是否系统中的串？
  MU是否定理？

MIU的定理树

- 由公理和推理规则，我们容易构造**定理树**
- 但无法保证在**有限步骤**内找到定理所在位置
- 那么**MU**到底是不是定理？
- 需要**另寻**方法
- 求助于系统之外的定律



一个MIU的同构系统310

- **M**对应**3**，**I**对应**1**，**U**对应**0**
- 自然数**31**在集合中
- **规则1**：如果集合中有数以1结尾，则添一个0也是集合中的数
- **规则2**：如果集合中有数以3开始，则把3后面的数再重复一次添在末尾也是集合中的数
- **规则3**：如果集合中有数包含111，则把111替换成0也是集合中的数
- **规则4**：如果集合中有数包含00，则去掉00的数也是集合中的数
- 问：**30**是不是集合中的数？

310系统中的判定：回归MIU系统的结论

- 通过分析数的构造规则，我们发现集合中的数**都不可能被3整除**
- 首先，**31**不能被3整除
- 其次，规则1～4都**无法**从不能被3整除的数生成能被3整除的数
- 而30可以被3整除，所以30**不属于**这个集合
- 对照回MIU系统的结论：MU**不是**MIU系统中的定理

PC系统的定理判定问题？

- 一个符合PC符号体系定义的**命题公式**，是否是PC中的**定理**？
- 同样，仅用PC系统中公理和分离规则**难以保证**能在有限步骤判定一个命题公式是否定理

PC系统的定理判定问题？

- 幸运的是，命题演算系统PC有一个非常重要的**同构**：**真值函数运算系统**
- 只需要用**真值表**判定命题公式对应的真值函数是否**重言式**，即可**判定**是否PC中的定理，
- 真值表的运算是**有限步骤**可以完成的。（注意：真值表并不是PC中的成分）