中国科学院自动化研究所
INSTITUTE OF AUTOMATION
CHINESE ACADEMY OF SCIENCES

归结原理

张文生 研究员

中国科学院自动化研究所

讲课内容

一．起因

二．命题逻辑的归结原理

三．置换与合一

四．一阶谓词的归结原理

五．归结原理的完备性

六．效率的提高

起因

- 自动定理证明
- 定理: $(F_1 \wedge F_2 \wedge \ldots \wedge F_n) \rightarrow G$
- 证明公式永真
- 证明公式的非永假
- 化为前束合取范式
- 化为Skolem范式
- 化为子句集
- 子句集不可满足

- Herbrand定理(Version 1)
  - 子句集S是不可满足的，当且仅当对应于S的任一棵完备语义树, 都存在一棵有限的封闭语义树。
- Herbrand定理(Version 2)
  - 子句集S是不可满足的，当且仅当存在一个有限不可满足的S的基础实例集合S’。

例子

- S={P(x,g(x),y,h(x,y),z,k(x,y,z)),
  ~P(u,v,e(v),w,f(v,w),x)}
  - H_0={a}
  - H_1={a,g(a),h(a,a),k(a,a,a),e(a),f(a,a)}
- 基础实例集:
  - S_0={ P(a,g(a),a,h(a,a),a,k(a,a,a)),
    ~P(a,a,e(a),a,f(a,a),a)}
  - S_1有6*6*6 + 6*6*6*6 = 1512个元素;
  - H_5有10^{64}数量级的元素，S_5有10^{256}数量级的元素.

- 如果可以不从基础实例出发，而直接从S出发，则可以避免大的计算量
- 归结原理:
  - 检查子句集S中是否含有空子句，或者能*推导*出空子句
- 推导不是任意定义的，必须保证推导出的结果是原来子句集合（逻辑公式）的逻辑结论
  - 例如，证明c_1->~c_2永真

- 归结原理是J.A.Robinson在1965年提出的，被认为是定理机器证明的重大突破

讲课内容

一. 起因

二. 命题逻辑的归结原理

三. 置换与合一

四. 一阶谓词的归结原理

五. 归结原理的完备性

六. 效率的提高

- 归结原理是Davis单文字规则的扩展
  - 如果在S中存在只有一个文字的基础子句L， 消去在S中带有这个文字L的所有子句得到S’， 如果S’为空, 则S是相容的; 否则, 从S’中删去~L, 得到S’’。 S’’不可满足当且仅当S不可满足。
- 例:
  - C_1: P
  - C_2: $\sim P \vee Q$
  - C_3: Q
- 互补对：原子与原子的非构成互补对

- 扩展
  - 例子:
  - C_1: P∨Q
  - C_2: ~P∨R
  - C_3: Q∨R

- C_1: 打伞 ∨ 不下雨
- C_2: 不打伞 ∨ 不被淋湿
- C_3: 不下雨 ∨ 不被淋湿

- 归结原理：
  - 对任何两个子句C_1和C_2，如果一个在C_1中的文字L_1和一个在C_2中的文字L_2构成互补对，则分别从C_1和C_2中删除L_1和L_2，并将C_1和C_2的剩余部分构成析取式C，则C称为C_1和C_2的归结式。
- 例：
  - C_1: $P \vee Q \vee \sim T$
  - C_2: $\sim P \vee R$
  - C: $Q \vee \sim T \vee R$ （C_1与C_2的归结式）

- 例：
  - C_1: $\sim P \vee Q$
  - C_2: $\sim P \vee R$
  - C_1与C_2没有互补对，所以没有归结式！
- 互补对每次只能取一对
  - C_1: $P \vee Q$
  - C_2: $\sim P \vee \sim Q$
  - C: $Q \vee \sim Q$ / $P \vee \sim P$

逻辑结论

- 子句C_1和C_2的归结式C是C_1和C_2的逻辑结论。
- 证明:
  - 令$C_1=L \vee C_1'$, $C_2=\sim L \vee C_2'$.
  - $C = C_1' \vee C_2'$.
    - 设$C_1 \wedge C_2$为真, 证C为真。

归结的例子

设公理集：

P,

$(P \wedge Q) \rightarrow R$,

$(S \vee T) \rightarrow Q$,

T,

求证：R

子句集：

(1) P

(2) $\sim P \vee \sim Q \vee R$

(3) $\sim S \vee Q$

(4) $\sim T \vee Q$

(5) T

(6) $\sim R$（目标求反）

化子句集：

$(P \wedge Q) \rightarrow R$

=> $\sim(P \wedge Q) \vee R$

=> $\sim P \vee \sim Q \vee R$

$(S \vee T) \rightarrow Q$

=> $\sim (S \vee T) \vee Q$

=> $(\sim S \wedge \sim T) \vee Q$

=> $(\sim S \vee Q) \wedge (\sim T \vee Q)$

=> $\{\sim S \vee Q, \sim T \vee Q\}$

子句集:

(1) P
(2) ~P∨~Q∨R
(3) ~S∨Q
(4) ~T∨Q
(5) T
(6) ~R（目标求反）

归结:

(7) ~P∨~Q	(2, 6)
(8) ~Q	(1, 7)
(9) ~T	(4, 8)
(10) nil	(5, 9)

- 例2
  - S={P∨Q，~P∨Q，P∨~Q，~P∨~Q}

(1) P∨Q

(2) ~P∨Q

(3) P∨~Q

(4) ~P∨~Q

(5) Q (1,2)

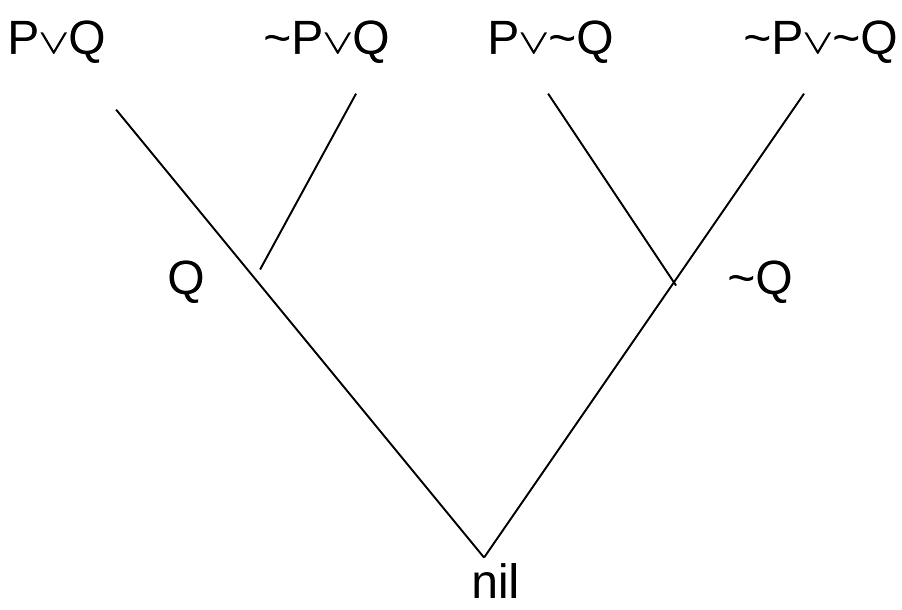
(6) ~Q (3,4)

(7) nil (5,6)

- 定义：
  - 给定一个子句集合S，从S到子句C的一个推演是一个有限的子句序列C_1 ,…, C_k，使得每个C_i 或是S中的一个子句，或是C_1到C_{i-1}中的某些子句的一个归结式，而C_k=C。如果C=nil，则这个推演称为S的一个证明。

推演树

- S={P∨Q，~P∨Q，P∨~Q，~P∨~Q}



讲课内容

一. 起因

二. 命题逻辑的归结原理

三. 置换与合一

四. 一阶谓词的归结原理

五. 归结原理的完备性

六. 效率的提高

- 例:
  - C_1: $P(x) \vee Q(x)$
  - C_2: $\sim P(f(x)) \vee R(x)$
- 没有互补对;
- 例:
  - C_1: $P(y) \vee Q(y)$ $\{y/x\}$
  - C_1: $P(f(x)) \vee Q(f(x))$ $\{f(x)/y\}$

  - C: $R(x) \vee Q(f(x))$

置换

- 定义: 置换是一个形如$\{t_1/v_1,\ldots, t_n/v_n\}$的有限集，其中每个$v_i$是变量，$t_i$是不同于$v_i$的项（常量、变量或函数）($v_i \neq t_i$)。当$i \neq j$时，$v_i \neq v_j$。
  - 无元素组成的置换称为空置换，记为ε;

- 例子:
  - {a/x, w/y, f(s)/z}, {g(x)/x}是置换;
  - {x/x}, {y/f(x)}不是置换;

实例

- 置换的结果称为实例;
- 定义: 令$\theta=\{t_1/v_1,\ldots, t_n/v_n\}$是一个置换，E是一个表达式，则$E\theta$是一个同时用项$t_i$代替E中变量$v_i$所得到的表达式($1\le i\le n$)。$E\theta$称为E的实例。
- 例子:
  - $E=P(x, y, z)$, $\theta=\{a/x, f(b)/y, c/z\}$
    - $E\theta=P(a, f(b), c)$
  - $E=P(x, y, z)$, $\theta=\{y/x, z/y\}$
    - $E\theta=P(y, z, z)$. $E\theta\neq P(z, z, z)$

置换的复合

- 例子:
  - E=P(x, y, z)
  - θ={a/x, f(z)/y, w/z}
  - Eθ=P(a, f(z), w)
  - λ={t/z, g(b)/w}
  - Eθλ=P(a, f(t), g(b))
  - θλ={a/x, f(t)/y, g(b)/z}

复合置换

- 定义： 令$\theta=\{t_1/x_1,\ldots, t_n/x_n\}$, $\lambda=\{u_1/y_1,\ldots, u_m/y_m\}$是两个置换. 则$\theta$与$\lambda$的复合是一个置换, 记为$\theta\circ\lambda$. (先$\theta$后$\lambda$)
  - 构成$\{t_1\lambda/x_1,\ldots, t_n\lambda/x_n,\ u_1/y_1,\ldots, u_m/y_m\}$;
  - 如果$y_j\in\{x_1,\ldots, x_n\}$, 则删除$u_j/y_j$;
  - 如果$t_k\lambda=x_k$, 则删除$t_k\lambda/x_k$;

- 例子:
  - $\theta=\{t_1/x_1, t_2/x_2\}=\{f(y)/x, z/y\}$
  - $\lambda=\{u_1/y_1, u_2/y_2, u_3/y_3\}=\{a/x, b/y, y/z\}$
  - $\theta\circ\lambda=\{t_1\lambda/x_1, t_2\lambda/x_2, u_1/y_1, u_2/y_2, u_3/y_3\}$
    $=\{f(b)/x, y/y, a/x, b/y, y/z\}$
  - 删除$\{a/x, b/y\}$;
  - 删除$\{y/y\}$;

合一

- $E_1\theta=E_2\theta$?
- 定义：如果$E_1\theta=\ldots=E_n\theta$，则称置换θ为 $\{E_1, \ldots, E_n\}$的合一子。
- 定义：如果对$\{E_1, \ldots, E_n\}$存在这样的合一子，则称集合$\{E_1, \ldots, E_n\}$是可合一的.
- 例1:
  - E={P(a,y), P(x, f(b))}, θ={a/x, f(b)/y}.
  - E={P(a,b), P(x, f(b))}

最一般合一子

- mgu(most general unifier)

- 定义：如果对E的每个合一子θ, 都存在一个置换λ, 使得θ=γ°λ，则称合一子γ是集合$\{E_1,\ldots,E_n\}$的最一般合一子。

- **例子:**
  - **$E=\{P(x,y), P(x,f(b))\}$**
    - **$\theta_1=\{a/x, f(b)/y\}$**
    - **$\theta_2=\{b/x, f(b)/y\}$**
    - **$\gamma=\{f(b)/y\}$**
    - **$\theta_1=\gamma \circ \{a/x\}$**
    - **$\theta_2=\gamma \circ \{b/x\}$**

- 是否存在寻找E的mgu的一般算法?
- 如何寻找E的mgu?

- 合一算法的考虑:
  - 消除两个谓词之间项的差别. {P(x,…), P(a,…)}

- 非空表达式集W的差别集:
  - 从左向右, 在W中的所有表达式, 遇到第一个不相同符号, 提取从这个符号开始的子表达式, 由此构成一个集合, 称为W的差别集, 记为D.

- 例子:
  - W={P(x,f(y,z),z， w), P(x,a), P(x, g(z),z,b)}
  - D={f(y,z), a, g(z)}

合一算法

- 1. K=0, W_k=W, γ_k=ε.
- 2. 如果W_k是单一的, 停机, γ_k是W的mgu.
  否则，求出W_k的差别集D_k.
- 3. 如果在D_k中存在元素v_k与t_k，使v_k是一个未出现在t_k中的变量， 转4;
  否则，停机， W是不可合一的。
- 4. 令$\gamma_{k+1}=\gamma_k \circ \{t_k/v_k\}$， $W_{k+1}=W_k \circ \gamma_{k+1}$.
- 5. K=K+1. 转2.

例子

- 求W={P(a,x,f(g(y))), P(z,f(z),f(u))}的mgu.
  - $D_0=\{a,z\}$. $\gamma_1=\varepsilon\circ\{a/z\}=\{a/z\}$.
  - $W_1=W_0\cdot\gamma_1=\{P(a,x,f(g(y))), P(a,f(a),f(u))\}$

  - $D_1=\{x,f(a)\}$. $\gamma_2=\gamma_1\circ\{f(a)/x\}=\{a/z, f(a)/x\}$.
  - $W_2=W_1\cdot\gamma_2=\{P(a,f(a),f(g(y))), P(a,f(a),f(u))\}$

  - $D_2=\{g(y),u\}$. $\gamma_3=\gamma_2\circ\{g(y)/u\}=\{a/z,f(a)/x, g(y)/u\}$
  - $W_3=W_2\cdot\gamma_3=\{P(a,f(a),f(g(y)))\}$
  - γ_3是mgu.

例子

- 求W={Q(f(a), g(x)), Q(y, y)}的mgu.
  - D_0={f(a),y}. $\gamma_1 = \varepsilon \circ \{f(a)/y\} = \{f(a)/y\}$.
  - $W_1 = W_0 \cdot \gamma_1$ ={Q(f(a), g(x)), Q(f(a), f(a))}

  - D_1={g(x), f(a)}.
  - 不可合一, 没有mgu.

例子

- 求W={P(f(y), y), P(x, a)}的mgu.
  - $D_0=\{f(y),x\}$.
  - $\gamma_1= \varepsilon \circ \{f(y)/x\}= \{f(y)/x\}$.
  - $W_1= W_0 \cdot \gamma_1 =\{P(f(y), y), P(f(y), a)\}$

  - $D_1=\{y, a\}$.
  - $\gamma_2=\gamma_1 \circ \{a/y\}= \{f(y)/x\} \circ \{a/y\} = \{f(a)/x, a/y\}$.
  - $W_2= W_1 \cdot \gamma_2 =\{P(f(a),a)\}$
  - γ_2是mgu.

讲课内容

- 定义:
  - 如果一个子句C中, 两个或更多的文字有相同的谓词符号, 且它们有mgu λ, 则$C\lambda$称为C的因子.
  - 如果$C\lambda$是单元子句, 则称$C\lambda$为C的单元因子.

- 例子:
  - $C=P(x) \vee P(f(y)) \vee \sim Q(x)$
  - $P(x)$和$P(f(y))$, $\lambda=\{f(y)/x\}$
  - $C\lambda= P(f(y)) \vee \sim Q(f(y))$

一阶谓词的归结

- 定义: 令C_1与C_2是两个子句, 它们没有共同的变量. 设L_1与L_2分别是C_1与C_2的两个文字, 如果L_1与$\sim L_2$有mgu λ, 则子句

$$(C_1\lambda - L_1\lambda) \cup (C_2\lambda - L_2\lambda)$$

称为C_1与C_2的二元归结式;

L_1与L_2称为被归结文字。

- 例子：
  - C_1: $P(x) \vee Q(x)$
  - C_2: $\sim P(a) \vee R(x)$

  - 重命名C_2: $\sim P(a) \vee R(y)$
  - $L_1=P(x)$, $L_2=\sim P(a)$
  - L_1与$\sim L_2$有mgu $\lambda=\{a/x\}$

  - $(C_1\lambda - L_1\lambda) \cup (C_2\lambda - L_2\lambda)$
    $=(\{P(a),Q(a)\} - \{P(a)\}) \cup (\{\sim P(a), R(y)\} - \{\sim P(a)\})$
    $=\{Q(a)\} \cup \{R(y)\}$
    $=\{Q(a), R(y)\}$
  - $Q(a) \vee R(y)$ 是C_1与C_2的二元归结式.

- 定义：子句C_1与C_2的归结式包括：
  - C_1与C_2的二元归结式;
  - C_1的因子与C_2的二元归结式;
  - C_1与C_2的因子的二元归结式;
  - C_1的因子与C_2的因子的二元归结式;

- 例子:
  - $C_1=P(x) \vee P(f(y)) \vee R(g(y))$
  - $C_2=\sim P(f(g(a))) \vee Q(b)$
  - C_1的因子C_1'是$P(f(y)) \vee R(g(y))$
  - C_1'与C_2的二元归结式是 $R(g(g(a))) \vee Q(b)$

例子

- F_1: $(\forall x)(C(x) \rightarrow (W(x) \wedge R(x)))$
- F_2: $(\exists x)(C(x) \wedge O(x))$
- G: $(\exists x)(O(x) \wedge R(x))$
- 证明G是F_1与F_2的逻辑结论.

- 化成标准式:

(1)$\sim C(x) \vee W(x)$
(2)$\sim C(x) \vee R(x)$
(3)$C(a)$
(4)$O(a)$
(5) $\sim O(x) \vee \sim R(x)$

- 归结:

(6)$R(a)$ $\{a/x\}$ (2)(3)
(7)$\sim O(a)$ $\{a/x\}$ (5)(6)
(8)nil (4)(7)

例子

1．能阅读的都是有文化的. R（x），L（x）
2．海豚是没有文化的.　　D（y），~L（y）
3．某些海豚是有智能的.　D（z），I（z）
证明：某些有智能的并不能阅读.　I（w），~R(w)

将文字叙述变成逻辑公式表达：
(∀x) (R（x）→ L（x）)
(∀y) (D（y）→ ~L（y）)
(∃z) (D（z）∧ I（z）)
(∃w) (I（w）∧ ~R(w))

$(\forall x)(R(x) \rightarrow L(x))$
$(\forall y)(D(y) \rightarrow \sim L(y))$
$(\exists z)(D(z) \wedge I(z))$
$(\exists w)(I(w) \wedge \sim R(w))$

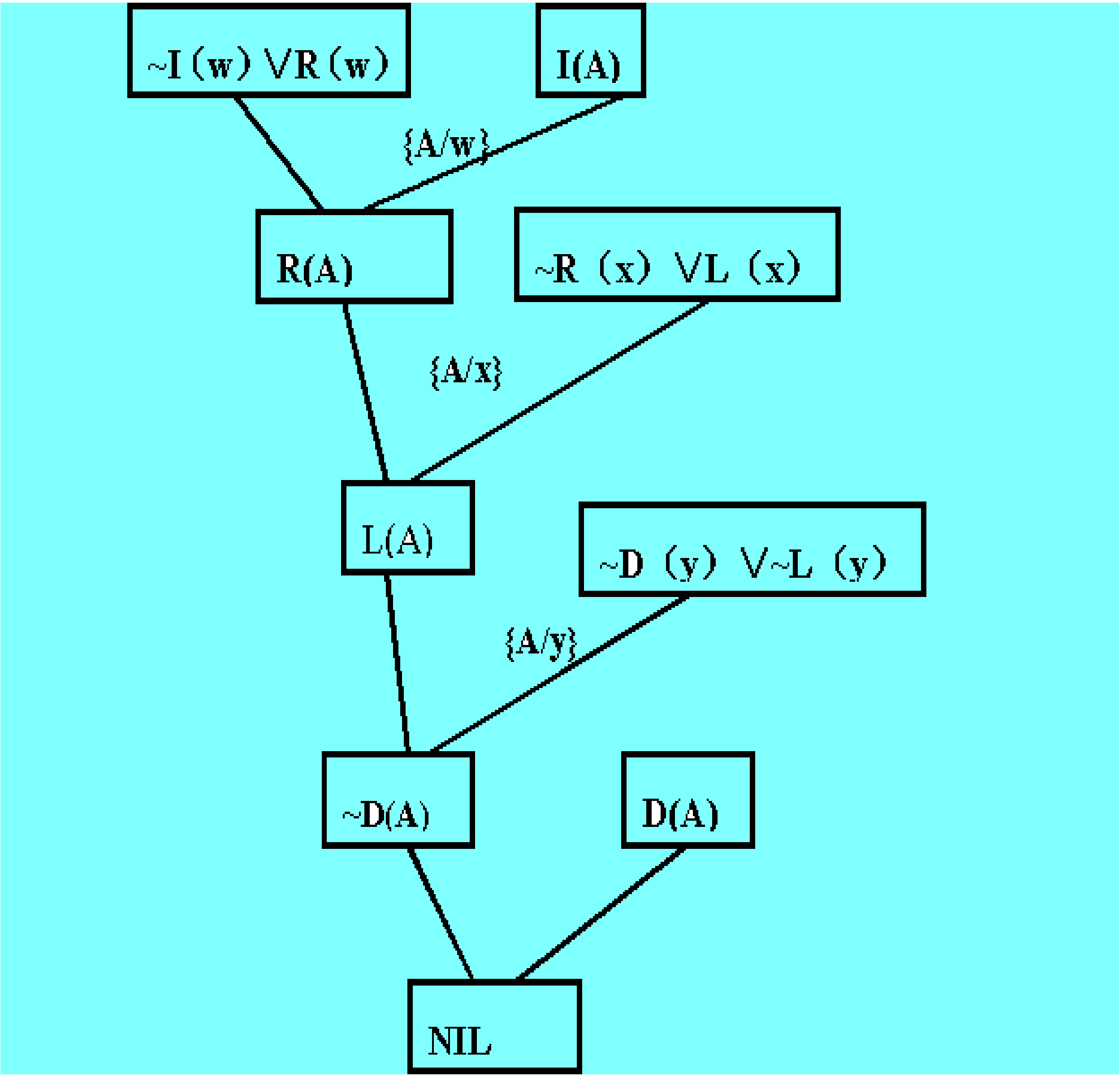
- 化为子句集:

(1) $\{\sim R(x) \vee L(x)\}$
(2) $\{\sim D(y) \vee \sim L(y)\}$
(3) $\{D(A), I(A)\}$

- 目标的否定

$(\forall w)[\sim I(w) \vee R(w)]$
(4) $\{\sim I(w) \vee R(w)\}$

子句集:
~R（x）∨L（x）
~D（y）∨~L（y）
D(A)
I（A）
~I（w）∨R（w）



讲课内容

一．起因

二．命题逻辑的归结原理

三．置换与合一

四．一阶谓词的归结原理

五．归结原理的完备性

六．效率的提高

- 定理: 一个子句集合S是不相容的，当且仅当存在一个从S到nil的反演。

- 难点: 存在性.
  - 构造性
  - C_1 ,…, C_k
  - 语义树

提升引理

- 引理：
  - 如果C_1’和C_2’是子句C_1和C_2的实例, C’是C_1’和C_2’的归结式, 则存在C_1和C_2的归结式C, 使C’是C的实例。

例子

- C_1 : $P(x) \vee Q(f(x))$
- C_2 : $\sim Q(y) \vee R(y)$

- C_1': $P(a) \vee Q(f(a))$ $\{a/x\}$
- C_2': $\sim Q(f(a)) \vee R(f(a))$ $\{f(a)/y\}$

- C' : $P(a) \vee R(f(a))$
- C : $P(x) \vee R(f(x))$

- 定理: 一个子句集合S是不相容的，当且仅当存在一个从S到nil的反演。

讲课内容

一．起因

二．命题逻辑的归结原理

三．置换与合一

四．一阶谓词的归结原理

五．归结原理的完备性

六．效率的提高

- **归结原理比Herbrand定理有了明显的进步;**
- **盲目的归结会产生组合爆炸问题;**
- **不必要的归结式 → 不必要的归结式;**

- **例子:**

- $S=\{P\vee Q, \sim P\vee Q, P\vee\sim Q, \sim P\vee\sim Q\}$

- 盲目归结过程:
- $S_0=S$
- $S_i=\{C_1, C_2$的归结式$|C_1\in S_0\cup S_1\cup\ldots\cup S_{i-1}, C_2\in S_{i-1}\}$
- 具体过程:
  - S_0: (1)$P\vee Q$ (2)$\sim P\vee Q$ (3)$P\vee\sim Q$ (4)$\sim P\vee\sim Q$
  - S_1: (5)Q (1)(2) (6)P (1)(3)
  - (7)$Q\vee\sim Q$ (1)(4) (8)$P\vee\sim P$ (1)(4) ……. (12)$\sim Q$
  - S_2: (13) $P\vee Q$ (1)(7) (14)$P\vee Q$ (1)(8)
  - …….
  - (39) nil (5)(12)

效率的提高

- **1965: Wos, G.A.Robinson, Curson, 支持集归结;**
- **1967: Slagle, 语义归结;**
- **1970: Loveland, Luckham, 线性归结;**
- **1971: Boyer, 锁归结;**
- **1978: 刘叙华, 锁语义归结;**
- **1979: 王湘浩,刘叙华, 广义归结;**

- 限制参加归结的子句
- 限制子句中被归结的文字
- 限制归结的方式

非常感谢同学们的光临

欢迎交流提问