离散数学(1): 数理逻辑

Discrete Mathematics (1): Mathematical Logic

第四章 归结法

赵永望
zhaoyw@buaa.edu.cn
北京航空航天大学 计算机学院

内 容

- 3.0. 归结法简介
- 3.1. 命题逻辑的归结法
- 3.2. 前束范式和斯科伦范式
- 3.3. 谓词逻辑的归结法

简介

- 自动推理早期的工作主要集中在机器定理证明。
- 机械定理证明的中心问题是寻找判定公式是否是有效的通用程序。
- 对命题逻辑公式，由于解释的个数是有限的，总可以建立一个通用判定程序，使得在有限时间内判定出一个公式是有效的或是无效的。
- 对一阶逻辑公式，其解释的个数通常是任意多个，丘奇（A.Church）和图灵（A.M.Turing）在1936年证明了不存在判定公式是否有效的通用程序。
  - 如果一阶逻辑公式是有效的，则存在通用程序可以验证它是有效的
  - 对于无效的公式这种通用程序一般不能终止。

简介

- 1930年希尔伯特为定理证明建立了一种重要方法，他的方法奠定了机械定理证明的基础。
- 开创性的工作是赫伯特·西蒙（Herbert A. Simon）和艾伦·纽威尔（Allen Newell）的 Logic Theorist。
- 机械定理证明的主要突破是1965年由鲁宾逊（John Alan Robinson）做出的，他建立了所谓归结原理，使机械定理证明达到了应用阶段。
- 归结法推理规则简单, 而且在逻辑上是完备的, 因而成为逻辑式程序设计语言Prolog的计算模型。

简介

- 判断一个公式是否为永真式
- 命题逻辑
  – 可判定, 用真值表即可计算, 但当命题变元较多时, 效率低
  – 更实用得到方法——归结法
- 谓词逻辑
  – 归结法是一个部分终止的算法
  – 当输入语句是永真式时, 判断算法终止并给出正确答案
  – 当输入语句不是永真式时, 判断算法可能不终止, 因而得不出结论

内 容

- 3.0. 归结法简介
- 3.1. 命题逻辑的归结法
- 3.2. 前束范式和斯科伦范式
- 3.3. 谓词逻辑的归结法

基本原理

- $Q_1,\ldots,Q_n \models R$，当且仅当$Q_1\wedge\ldots\wedge Q_n\wedge\neg R$不可满足
- 证明$Q_1,\ldots,Q_n \models R$
  - (1) $Q_1\wedge\ldots\wedge Q_n\wedge\neg R$化为合取范式；
  - (2) 构建Ω子句集合，Ω为$Q_1\wedge\ldots\wedge Q_n\wedge\neg R$合取范式的所有简单析取范式组成集合；
  - (3) 若Ω不可满足，则$Q_1,\ldots,Q_n \models R$。
- 机械式地证明Ω不可满足是关键问题

子句与空子句

- **回顾第一章：文字、简单析取式、合取范式**

定义1.14： 原子公式和原子公式的否定统称为文字。如果一个文字恰为另一个文字的否定，则称它们为相反文字。

– 文字:p, 相反文字:¬p

定义1.15： 设n是正整数，$Q_1,\ldots\ldots,Q_n$都是文字，则称

– $Q_1 \vee \ldots \vee Q_n$为简单析取式

– $Q_1 \wedge \ldots \wedge Q_n$为简单合取式

– 若$R_1,\ldots\ldots,R_n$都是简单析取式，则称$R_1 \wedge \ldots \wedge R_n$为合取范式。

- $(p\vee q\vee r)\wedge(p\vee \neg q\vee r)\wedge(p\vee \neg q\vee r)$

子句与空子句

- 合取范式的语义性质由其包含的简单析取式决定，而与析取式出现的次数和顺序无关
- 将合取范式看作简单析取式的集合，将简单析取式看作文字的集合
- **定义4.1：** 文字的有穷集合称为子句，不包含文字的子句称为空子句，记为□。

概念	公式
文字	文字
子句	简单析取式
子句的集合	合取范式

子句集的可满足性

- **定义4.2：** 如果真值赋值v满足子句集S中的每个子句，则称v满足S。如果至少有一个v满足子句集S，称S是可满足的，否则称S是不可满足的
- 有趣的结论：
  - 子句$p \vee q$和$\neg p \vee r$分别有相反的文字p和$\neg p$
  - 可以去掉相反的文字，将剩余的文字合并，得到新子句$q \vee r$
  - 显然，$p \vee q, \neg p \vee r \vDash q \vee r$

归结子句

- **定义4.3：** 设L_1和L_2是相反的文字，并且分别在子句C_1和C_2中出现，称子句
$$(C_1 - \{L_1\}) \cup (C_2 - \{L_2\})$$
为C_1和C_2的**归结子句**

- 例4.1：$\neg p \vee r \vee s$是子句$\neg p \vee q \vee r$和$\neg q \vee s$的归结子句
- 例4.2：子句$\neg p \vee q$和$\neg p \vee r$没有归结子句，因为它们不包含相反的文字
- 例4.3：子句□是子句p和$\neg p$的归结子句
- 例4.4： 对于子句$p \vee q$和$\neg p \vee \neg q$的
  - $q \vee \neg q$是归结子句
  - $p \vee \neg p$也是归结子句
  - 但□不是

归结定理

- **定理4.1：如果子句 C 是 C_1 和 C_2 的归结子句，则$C_1, C_2 \vDash C$**
  - 证明：设C_1是$p \vee L_1 \vee \cdots \vee L_n$, C_2是$\neg p \vee W_1 \vee \cdots \vee W_m$, 则$C$是$L_1 \vee \cdots \vee L_n \vee W_1 \vee \cdots \vee W_m$
  - 任取满足C_1和C_2的真值赋值v
    - 若$\mathrm{v}(p) = 0$, 则$\mathrm{v}(L_1 \vee \cdots \vee L_n) = 1$
    - 若$\mathrm{v}(p) = 1$, 则$\mathrm{v}(W_1 \vee \cdots \vee W_m) = 1$
  - 无论哪种情况，v都满足C

反驳Refutation

- **定义4.4：** 设S是子句集合，如果子句序列$C_1, \ldots, C_n$满足以下条件，则称该子句序列为S的一个反驳：
  - (1) 对于每个i ≤ n, $C_i \in S$或C_i是C_j和C_k的归结子句, 其中j,k < i
  - (2) C_n是□

反驳的例子

- **例4.5：** 考虑子句集$S = \{p \vee q, \neg p \vee q, p \vee \neg q, \neg p \vee \neg q\}$, 以下子句序列是S的一个反驳
  - (1) $p \vee q$
  - (2) $\neg p \vee q$
  - (3) $p \vee \neg q$
  - (4) $\neg p \vee \neg q$
  - (5) q 由(1)和(2)
  - (6) $\neg q$ 由(3)和(4)
  - (7) $\square$ 由(5)和(6)

软件开发环境国家重点实验室 State Key Laboratory of Software Development Environment

归结法的可靠性和完备性

- **定理4.2：** 子句集合S是不可满足的，当且仅当存在S的反驳

归结法推理

- 我们已知：$A_1, \ldots, A_n \vDash B$, 当且仅当$A_1 \wedge \cdots \wedge A_n \wedge \neg B$不可满足。因此，采取以下步骤证明$A_1, \ldots, A_n \vDash B$
  - (1) 将$A_1, \ldots, A_n, \neg B$分别化为合取范式
  - (2) 取S为上述合取范式中所有简单析取式对应的子句的集合
  - (3) 寻找S的一个反驳。若能找到，则$A_1, \ldots, A_n \vDash B$，否则$A_1, \ldots, A_n \nvDash B$

示例1

- 例题：$P\rightarrow(Q\wedge R) \models (P\rightarrow Q)\wedge (P\rightarrow R)$　　分配律
- 证明：
- $(P\rightarrow(Q\wedge R)) \wedge\neg ((P\rightarrow Q)\wedge (P\rightarrow R))$
- $\Leftrightarrow (\neg P\vee(Q\wedge R)) \wedge ((P\wedge\neg Q) \vee (P\wedge\neg R))$
- $\Leftrightarrow (\neg P\vee Q) \wedge (\neg P\vee R)\wedge(P\vee (P\wedge\neg R)) \wedge(\neg Q\vee (P\wedge\neg R))$
- $\Leftrightarrow (\neg P\vee Q) \wedge (\neg P\vee R)\wedge P \wedge(P\vee \neg R) \wedge(\neg Q\vee P) \wedge (\neg Q\vee\neg R)$
- $(P\rightarrow(Q\wedge R)) \wedge\neg ((P\rightarrow Q)\wedge (P\rightarrow R))$的一个合取范式为
  - $(\neg P\vee Q) \wedge (\neg P\vee R)\wedge P \wedge(P\vee \neg R) \wedge(\neg Q\vee P)\wedge(\neg Q\vee\neg R)$
- 对应的子句集合
  $\Omega=\{ P, P\vee\neg Q, \neg P\vee Q, P\vee\neg R , \neg P\vee R , \neg Q\vee\neg R\}$。

示例1（续）

- $\Omega=\{ P, P\vee\neg Q, \neg P\vee Q, P\vee\neg R , \neg P\vee R , \neg Q\vee\neg R\}$
- $Q_1= P\vee\neg Q$　　$Q_1\in\Omega$
- $Q_2=\neg P\vee Q$　　$Q_2\in\Omega$
- $Q_3=\square$　　$Q_3= (Q_1\text{-}P\text{-}\neg Q) \vee (Q_2\text{-}\neg P\text{-}Q)$

✕

- 一次仅消减一个命题变元

- $Q_1= P$　　$Q_1\in\Omega$
- $Q_2=\neg P\vee Q$　　$Q_2\in\Omega$
- $Q_3= Q$　　$Q_3= (Q_1\text{-}P) \vee (Q_2\text{-}\neg P)$
- $Q_4= \neg P\vee R$　　$Q_4\in\Omega$
- $Q_5= R$　　$Q_5= (Q_1\text{-}P) \vee (Q_4 \text{-} \neg P)$
- $Q_6= \neg Q\vee\neg R$　　$Q_6\in\Omega$
- $Q_7= \neg R$　　$Q_7= (Q_3\text{-}Q) \vee (Q_6 \text{-} \neg Q)$
- $Q_8= \square$　　$Q_8= (Q_5\text{-}R) \vee (Q_7 \text{-} \neg R)$
- $P\rightarrow(Q\vee R) \vdash (P\rightarrow Q) \vee (P\rightarrow R)$　　分配律
- 证毕

软件开发环境国家重点实验室 State Key Laboratory of Software Development Environment

归结法推理

- 例4.6：证明

  $$p \to (q \to r), q \to (r \to s) \vDash p \to (q \to s)$$

  - 将$p \to (q \to r)$化为合取范式$\neg p \vee \neg q \vee r$
  - 将$q \to (r \to s)$化为合取范式$\neg q \vee \neg r \vee s$
  - 将$\neg(p \to (q \to s))$化为合取范式$p \wedge q \wedge \neg s$
  - 取子句集合$S = \{\neg p \vee \neg q \vee r, \neg q \vee \neg r \vee s, p, q, \neg s\}$
  - 给出S的一个反驳如下：
  - (1) $\neg p \vee \neg q \vee r$
  - (2) $\neg q \vee \neg r \vee s$
  - (3) p
  - (4) q
  - (5) $\neg s$

(6) $\neg q \vee \neg r$　　由(2)和(5)

(7) $\neg q \vee r$　　由(1)和(3)

(8) $\neg q$　　由(6)和(7)

(9) $\square$　　由(4)和(8)

软件开发环境国家重点实验室 State Key Laboratory of Software Development Environment

归结法推理

- **例4.7：判断下面推理是否成立**

$$p \wedge q \to r, p \vee q \to \neg r \vDash p \wedge q \wedge r$$

  - 将$p \wedge q \to r$化为合取范式$\neg p \vee \neg q \vee r$
  - 将$p \vee q \to \neg r$化为合取范式$(\neg p \vee \neg r) \wedge (\neg q \vee \neg r)$
  - 将$\neg(p \wedge q \wedge r)$化为合取范式$\neg p \vee \neg q \vee \neg r$
  - 取子句集合$S = \{\neg p \vee \neg q \vee r, \neg p \vee \neg r, \neg q \vee \neg r, \neg p \vee \neg q \vee \neg r\}$
  - 首先归结掉命题变元r，得到子句集合$\{\neg p \vee \neg q\}$, $\neg p \vee \neg q$可满足, 因此S可满足, 因此不成立

软件开发环境国家重点实验室 State Key Laboratory of Software Development Environment

内 容

- 3.0. 归结法简介
- 3.1. 命题逻辑的归结法
- 3.2. 前束范式和斯科伦范式
- 3.3. 谓词逻辑的归结法

前束范式

- 将归结法推广到谓词逻辑，需将谓词逻辑公式化为某种标准形式
- 定义4.5：形式$Q_1y_1 \dots Q_ny_nB$的公式称为前束范式, 其中n为非负整数, 每个Q_i是$\forall$或$\exists$, B是开公式, $y_1 \dots y_n$是不同的变元. $Q_1y_1 \dots Q_ny_n$称为该前束范式的前束词, B称为它的母式
- 例如：$\forall x \exists y \exists z(P(x,y) \rightarrow Q(u,v))$和$P(x,y)$是前束范式, 但$\forall xP(x) \wedge Q(y)$不是前束范式
- 定理: 每一个公式都等值于一个前束范式

化为前束范式

- **将公式化为前束范式的基本步骤：**
  - (1) 消去联结词⊕和↔
  - (2) 将约束变元适当换名，使得约束变元与自由变元不同名，并且量词的各次出现约束不同的变元
  - (3) 将量词提到最外面，化成前束范式
- **例4.8：** $\forall x P(x) \leftrightarrow \neg\exists y Q(x,y)$
- $\Leftrightarrow (\forall x P(x) \to \neg\exists y Q(x,y)) \wedge (\neg\exists y Q(x,y) \to \forall x P(x))$
- $\Leftrightarrow (\forall z P(z) \to \neg\exists y Q(x,y)) \wedge (\neg\exists u Q(x,u) \to \forall v P(v))$
- $\Leftrightarrow (\forall z P(z) \to \forall y \neg Q(x,y)) \wedge (\forall u \neg Q(x,u) \to \forall v P(v))$
- $\Leftrightarrow \exists z \forall y (P(z) \to \neg Q(x,y)) \wedge \exists u \forall v (\neg Q(x,u) \to P(v))$
- $\Leftrightarrow \exists z \exists u \forall y \forall v \big(\big(P(z) \to \neg Q(x,y)\big) \wedge \big(\neg Q(x,u) \to P(v)\big)\big)$

$\forall x(A \to B) \Leftrightarrow \exists x A \to B$ $\quad$ $\forall x(B \to A) \Leftrightarrow B \to \forall x A$

$\exists x(A \to B) \Leftrightarrow \forall x A \to B$ $\quad$ $\exists x(B \to A) \Leftrightarrow B \to \exists x A$

无∃前束范式

- **定义4.6：**不出现存在量词的前束范式称为无∃前束范式，也称**全称公式**
- 例如： $\forall x P(x,y), \forall x \forall y(P(x,y) \rightarrow Q(z))$, $P(x,y)$等都是无∃前束范式, 但$\forall x \exists y P(x,y)$不是

无∃前束范式

- **定义4.7：前束范式A的无∃前束范式A'递归定义如下：**
  - (1) 若A是无∃前束范式, A'为A
  - (2) 若A是$\exists yB$, 则A'为$(B_a^y)'$, 其中a是在B中不出现的常元
  - (3) 若A是$\forall x_1 \ldots \forall x_n \exists yB$, 其中n是正整数, 则$A'$为$(\forall x_1 \ldots \forall x_n B_{f(x_1 \ldots x_n)}^y)'$, 其中f是在B中不出现的n元函数符号

软件开发环境国家重点实验室
State Key Laboratory of Software Development Environment

前束范式转为无∃前束范式

- 例4.9: $\exists x \forall y \exists z \exists u \forall v (P(x,y,z) \to Q(u,v))$
  - $(\exists x \forall y \exists z \exists u \forall v (P(x,y,z) \to Q(u,v)))'$
  - $= (\forall y \exists z \exists u \forall v (P(a,y,z) \to Q(u,v)))'$
  - $= (\forall y \exists u \forall v (P(a,y,f(y)) \to Q(u,v)))'$
  - $= (\forall y \forall v (P(a,y,f(y)) \to Q(g(y),v)))'$
  - $= \forall y \forall v (P(a,y,f(y)) \to Q(g(y),v))$

前束范式和无∃前束范式的关系

- 两者并不等值
  - 例如$\exists x P(x)$的无∃前束范式$P(a)$, 与$\exists x P(x)$不等值
- 对于前束范式A和它的无∃前束范式A', $A' \vDash A$总成立, 而$A \vDash A'$则不一定
- 定理4.3：若A'是前束范式A的无∃前束范式, 则A'可满足当且仅当A可满足

斯科伦范式(Skolem范式)

- 原子公式和原子公式的否定统称为文字。若$A_1, \ldots, A_n$是文字，则$A_1 \vee \cdots \vee A_n$是简单析取式。若$B_1, \ldots, B_n$都是简单析取式，则称$B_1 \wedge \cdots \wedge B_n$为合取范式。
- **定义4.8：** 母式是合取范式的无∃前束范式，称为**斯科伦范式**。
- 每个公式A都可以化为一个斯科伦范式B, 使得A不可满足当且仅当B不可满足, 称B为A的斯科伦范式

化为斯科伦范式

- 例4.10: 求$\forall xP(x,y) \leftrightarrow \neg\forall yQ(x,y)$的斯科伦范式
  - $\forall xP(x,y) \leftrightarrow \neg\forall yQ(x,y)$
  - $\Leftrightarrow (\forall xP(x,y) \rightarrow \neg\forall yQ(x,y)) \wedge (\neg\forall yQ(x,y) \rightarrow \forall xP(x,y))$
  - $\Leftrightarrow (\forall xP(x,y) \rightarrow \exists y\neg Q(x,y)) \wedge (\exists y\neg Q(x,y) \rightarrow \forall xP(x,y))$
  - $\Leftrightarrow (\forall zP(z,y) \rightarrow \exists u\neg Q(x,u)) \wedge (\exists v\neg Q(x,v) \rightarrow \forall wP(w,y))$
  - $\Leftrightarrow \exists z\exists u(P(z,y) \rightarrow \neg Q(x,u)) \wedge \forall v\forall w(\neg Q(x,v) \rightarrow P(w,y))$
  - $\Leftrightarrow \exists z\exists u\forall v\forall w\big(\big(P(z,y) \rightarrow \neg Q(x,u)\big) \wedge \big(\neg Q(x,v) \rightarrow P(w,y)\big)\big)$
  - 再化为无∃前束范式
  - $\Leftrightarrow \forall v\forall w\big(\big(P(a,y) \rightarrow \neg Q(x,b)\big) \wedge \big(\neg Q(x,v) \rightarrow P(w,y)\big)\big)$
  - 最后将母式化为合取范式
  - $\Leftrightarrow \forall v\forall w\big(\big(\neg P(a,y) \vee \neg Q(x,b)\big) \wedge \big(Q(x,v) \vee P(w,y)\big)\big)$

$\forall x(A \rightarrow B) \Leftrightarrow \exists xA \rightarrow B$ $\qquad$ $\forall x(B \rightarrow A) \Leftrightarrow B \rightarrow \forall xA$

$\exists x(A \rightarrow B) \Leftrightarrow \forall xA \rightarrow B$ $\qquad$ $\exists x(B \rightarrow A) \Leftrightarrow B \rightarrow \exists xA$

软件开发环境国家重点实验室 State Key Laboratory of Software Development Environment

内 容

- 3.0. 归结法简介
- 3.1. 命题逻辑的归结法
- 3.2. 前束范式和斯科伦范式
- 3.3. 谓词逻辑的归结法

软件开发环境国家重点实验室 State Key Laboratory of Software Development Environment

本　节　完！

问题与解答？