自动定理证明

自动定理证明

石纯一 编著

高等教育出版社

内 容 简 介

本书介绍了一阶谓词逻辑的基本知识，重点讨论了一阶谓词逻辑描述下的自动定理证明方法，并对非归结法、不确定和非单调推理方法作了介绍。本书是以人工智能的观点，将一阶谓词逻辑和非标准逻辑视作一种重要的知识表和推理方法的。

可作为大学计算机系研究生和高年级大学生的教材。也可作为从事计的教师和科研人员的参考书。

自 动 定 理 证 明

石纯一 编著

责任编辑 黄丽荣

气象出版社 出版
（北京西郊白石桥路46号）

北京市昌平环球科技印刷厂

气象出版社发行 全国各地新华书店经售

开本：787×1092 1/32 印张：5 字数：111千字

1989年12月第一版 1989年12月第一次印刷

印数：1— 3000 定价：3.60元

ISBN 7-5029-0298-8/TP·0015

目　录

前　言

自动定理证明是人工智能的一个重要分支。

"人工智能"术语是在1956年于达特茅斯（Dartmouth）大学召开的学术会议上提出的，人工智能学科一般认为也是1956年开始的。

人工智能是研究使计算机能够完成表现出人类智能的任务。中心课题是计算机实现智能的原理、制造类似于人脑的智能计算机，以及使计算机更聪明些实现高层次的应用系统。

实现高层次的应用包括使机器由"知道干什么"提高到"知道怎么干"；由"数值计算"过渡到"符号处理"。而符号处理主要不是靠推理而是强调知识，特别是专门领域的独到的经验知识的获取、表示和利用。

计算机会不会思维，或说机器能不能有智能，以及智能是什么？这个问题的讨论已有相当悠久的历史了。笛卡儿曾对制造有理智的机器发生过兴趣，毕达哥拉斯提出宇宙为数的和谐学说，莱布尼兹发展了思维是一种计算的观点，提出人类思维的字母表的想法。

1958年Simon和Newell这两位启发式程序设计创始人提出不到10年时间计算机将成为世界象棋冠军，计算机将找到并证明当时还未被证明的重要数学定理。大部分心理学理论将采用计算机程序形式。但30年过去了，这种乐观的预言都没有实现，这说明人们对机器思维的研究遇到了困难。

当今对机器智能研究有乐观派，确信可建立机器智能或

人工智能；有反对派，认为人的思维与人工智能实质上没有共同之处；还有怀疑派。

我们对计算机能不能思维的问题，可以这样来理解，这问题涉及到辩证唯物主义与机械唯物论观点上的区别。人的思维过程不是神，人脑是物质的，从而就应该可认识，一旦知道规律便可由机器来实现。然而不可绝对化，因为人脑在发展，机器又要人来制造，从这意义上说不能完全由机器代替人脑，部分地代替是没有问题的。

自动定理证明就是让计算机来证明定理，也可称机器定理证明或定理证明自动化。自动定理证明方法属自动推理方法，自然是一种智能行为。首先由数学定理的证明开始研究的，数学定理的证明集中地体现了人类的演绎思维能力。自动定理证明广泛地应用于人工智能的各领域，如规划问题、程序综合以及逻辑程序语言 prolog 的实现都与定理证明方法密切相关。然而当今可提供的证明方法，多数尚属机械方法，因为证明过程常有很强的技巧和窍门，这又难于规律化，计算机就难于模仿，从而所给方法智能味还不浓。

自动定理证明有几种途径。

自然推导法是仿照数学证明定理的过程，教给机器来实现。从人工智能观点说，这是最自然的道路了，然而这是很困难的。人在证明中使用了许多经验知识启发式方法，从各种可能的证明方案中删除大量的可能的试探而走捷径。1957 年 Newell-Shaw-Simon 给出了命题逻辑的定理证明方法，1960年 Slagle 给出了启发式不定积分求解程序。70 年代出现了 MACSYMA 系统可以处理微分积分和化简表达式等已超过多数专家的水平。

对一类问题找出可行算法或称判定方法。如 Church、

Turing 证明了一阶逻辑是不可判定的。对初等几何、初等代数的判定法也有不少研究，我国数学家吴文俊1977年给出了初等几何中不考虑点的之间关系的情况下定理证明的机械化方法，甚至很困难的定理也可得到证明。

计算机辅助证明应该说是当前最有前途的了。当今的方法尚不能证明复杂困难的定理，在证明某个定理的过程中，遇到的大量计算推理人又难于完成时借助于机器，而人更多地考虑证明思路，这种人机结合是较现实可行的。

一阶谓词逻辑表示下的定理证明问题，是有特殊意义的证明问题，首先一阶谓词逻辑有很强的表达能力，凡可计算的函数就可由一阶谓词表达；其次一阶谓词逻辑是一种重要的人工智能的知识表示方法和推理方法，理论较系统较完整。1930年 Herbrand 给出了一阶谓词逻辑的半可判定算法，1960年Gilmore 在计算机上实现了，1965年 Robinson 提出了归结方法，当时认为是定理证明的重要突破，70年代出现了非归结方法。这些都是这本书的基本内容。

全书共分六章，首先介绍了作为人工智能一种重要的知识表示方法和推理方法的一阶谓词逻辑（命题逻辑认为读者是熟悉的）。然后给出了命题逻辑和谓词逻辑的定理证明方法，重点讨论了 Herbrand 半可判定算法和归结原理。还对非归结法以及非标准逻辑下的不确定推理方法、非单调推理方法做了讨论。

第一章　一阶谓词逻辑

在命题逻辑里，是把简单命题（非真即假的简单陈述句）作为基本单元或作为不可分的原子来看待的，不再对简单命题的内部结构进行分析了。如命题“张三是学生”在命题逻辑中是作为基本单元考虑的，然而对这命题仍可作分解，有主词和谓词之分，这样的细分好处是对两个不同的命题的共同点可进行研究了。像凡有理数都是实数，2/5 是有理数，所以 2/5 是实数。直观看这样的推理应该是正确的，然而在命题逻辑范围，这三个命题只能分别以 p,q,r（小写字母）表示，是相互不同的简单命题，而

$$\begin{array}{l} p \\ q \\ \hline \therefore r \end{array}$$

并不是正确的推理形式，因为 $(p \wedge q) \rightarrow r$ 对任意的命题 p，q，r 来说并非永真式。这样直观的推理在命题逻辑中得不到反映，这不能说不是命题逻辑的局限性。只有对简单命题作进一步的剖析，才能认识这种推理形式和推理规律的正确性，这就需要引入谓词逻辑。将简单命题细分到主词、谓词，引入变量（元），并考虑到表示变量数量上一般与个别的全称量词和存在量词，进而研究它们的形式结构逻辑关系便构成了谓词逻辑，所介绍的内容限于一阶谓词逻辑部分。

对命题的研究采取了这种先整体而后细分的次序似乎有点反常，然而将会看到谓词逻辑较命题逻辑复杂得多。

这一章是为谓词逻辑描述下的机器定理证明作准备的，

同时谓词逻辑也是人工智能中，一种重要的知识表示方法和推理方法，从而是重要的基础。将介绍谓词逻辑的基本概念、等值演算和推理演算。

§1.1 谓词和个体词

1. 谓词

例 张三是学生

李四是学生

这是两个不同命题，限于命题逻辑只能分别以两个不同的符号如 p，q 表示了。然而分析一下这两个命题的共同点，知它们都有主词和谓词，不同的是主词“张三”、“李四”，而谓词“是学生”是相同的，现在强调它们的共同点，设想用大写字母 P 表示“是学生”，这样这两个命题的一致性可由 P 来体现了，但主词还需区别开来，这可由 P（张三）、P（李四）来全面描述这两个命题了。相同的是谓词 P，不同的主词张三、李四。自然一般地说可引入变量 x 表示主词，于是符号

P(x)：表示 x 是学生

在一个命题里，如果主词只有一个，那么表示该主词性质的词称作谓词，如所说的“是学生”便是谓词。

在一个命题里，如果主词多于一个，那么表示这几个主词间相互关系的词称作谓词。如命题“张三和李四是兄弟”这里的“是兄弟”便是谓词，又如

“5 大于 3”这里“大于”是谓词

“张三比李四高”这里“比……高”是谓词

“天津位于北京的东南”这里“位于……东南”是谓词

“A 在 B 上”这里“在……上”是谓词

显然这几个例子都可用符号 P(x,y) 来表示，其中P表示谓词，x,y是相应的两个主词。

凡带有变元的大写符号 P(x),Q(x),R(x)……P(x,y),Q(x,y)，R(x,y)……等均作为谓词来理解。

2. 个体词

在数理逻辑里，不使用主词这个词，而习惯称为个体词，是一个命题中表示思维对象的词。

P（张三），其中的张三是个体词称为个体常项。当谓词以 P(x) 表示时，称变元 x 为个体变元或个体变项，而变项的变化范围叫变项的变程，变项在变程中的取值叫变项的值。

有 n 个个体词的谓词 $P(x_1,\cdots,x_n)$ 叫 n 项（元、目）谓词，如果P是已赋有确定含义的谓词就称为谓词常项，而P表任一谓词时就称为谓词变项。

将个体变项的变程称为个体域或论域以D表示，并可约定谓词逻辑的个体域除明确指明外，一般认为是包括一切事物的一个最广的集合，而谓词变项的变程不做特别声明便指一切关系或一切性质的集合。

论域的概念是重要的，同一谓词在不同论域下它的形式描述可能不同，所取的真假值也可能不同。

3. 命题形式和命题

一般地说谓词 P(x)，Q(x,y) 是命题形式而不是命题。因为当 P,Q 给定后而个体词 x，y 没确定时，仍不能确定 P(x),Q(x,y) 的真值是取真还是取假。

如P(x)表示x是有理数，这样谓词是给定了，是谓词常项了，但个体词还是变项，无法判明P(x)是取真还是取假。

又如 Q(x,y) 表示 x 大于 y，这样谓词是常项了，而个

体词是变项，仍不能判明Q(x,y)的真假值。

仅当谓词变项取定为某个谓词常项，并且个体变项取定为个体常项时，命题形式才化为命题。这时P(3)表示3是有理数，取值为T（真），而Q(2，3)表示2大于3，取值为F（假）。于是P(3)，Q(2,3)是命题。

命题的真假值是明显地依赖于个体变元的论域的。如x的论域为正实数，y的论域为负实数，那么Q(x,y):x>y必取值为T。如果x,y的论域调换，那么Q(x，y)取值就为F，（这里不是对个体x,y的选定，而是选定两个特殊的论域，并理解为对所有的x，所有的y，Q(x,y)均成立而命题化的）。

4. 谓词进一步抽象定义

曾将谓词定义为一个个体的性质或多个个体间的某种关系。可进一步抽象地定义，谓词为给定的个体域到集合{T，F}上的一个映射，这样定义的谓词更广泛。

例如，将命题“房子是黄色的”符号化，可引入谓词YELLOW（HOUSE）表示HOUSE是黄色的，个体词用HOUSE表示了，规定当HOUSE是房子又是黄色的该命题为真。借助于谓词的抽象定义，也可用二元谓词VALUE(COLOR,HOUSE)来描述这命题，而谓词VALUE就是个体到{T,F}的映射，不一定有什么具体的含义。这里只需规定当COLOR取黄色且HOUSE取房子为值时VALUE取值为T。这便说明了谓词的抽象定义给命题形式化带来了方便。

5. 谓词逻辑与命题逻辑

由于命题逻辑较为简单，读者是熟悉的，所以没有论述。可认为谓词逻辑是命题逻辑的推广，命题逻辑是谓词逻辑的特殊情形。因为任一命题都可通过引入谓词，并确定其

相应的含义和个体常项化来表示；也可认为一个命题是没有个体变元的零元谓词。这样说来，在命题逻辑中的许多概念、规则仍可在谓词逻辑中延用，如联结词～，∨，∧，→，↔可照搬到谓词逻辑中无需再做说明，然而谓词逻辑里出现个体变元、量词等概念给我们的讨论带来了复杂性，处理起来难度大得多，最简单又深刻的例子是在命题逻辑中一个公式很容易判定它是否为重言式，然而在谓词逻辑里就没有一般的法则来判定任一公式是否是永真的。

§1.2 函数和量词

1. 函数

对自然语句形式化或对已给的命题形式做分析时，函数的概念是经常使用的。而函数本身的含义是和通常的微积分里的定义是一致的。只须强调的它是某个个体域（不必是实数）到另一个体域的映射。它不是谓词，因为谓词是个体到真假的映射，而函数的值仍是某个个体。

例如，father(x)：表示 x 的父亲

f(x) = x + 2：表示 x 加 2

都是函数。而函数嵌入谓词联合使用是常见的。

例如，P(x)表示 x 是教师则

P(father(x))就表示x的父亲是教师。

又如张三的父母是夫妻，这句话可描述为

MARRIED(father（张三），mother（张三））

其中MARRIED (x,y) 表示x,y是夫妻，是谓词而 father (x),mother(x)是函数。

约定函数符号也用小写字母式单字表示，如 f,g,father …… （这不会与小写字母表示的命题相混淆）。

2. 量词

它是命题里表示个体数量的词，也可以看作是对个体词所加的限制、约束的词。但不是对数量一个，二个，三个……的具体研究，而是只讨论两个最通用的数量限制词，一个是“所有的”；一个是“至少有一个”，它们分别称作全称量词和存在量词。在某种意义上说这是一对对立词。

先讨论全称量词，如“凡事物都是运动的”，这命题中的“凡”就是表示个体变元数量“所有的”词，也可用“一切的”，“任一个”，“每一个”等同义词表示，这句话的意思等于说

对任一事物而言，它都是运动的，或说

对任一 x 而言，x 是运动的。

由于个体 x 的论域是包含一切事物的集合，这句话可描述为

$$(\forall x)\ (x\text{是运动的})$$

或 $$(x)\ (x\text{是运动的})$$

或 $$\forall x\ (x\text{是运动的})$$

如果 P(x)表示 x 是运动的，那么整个句子便描述为

$$(\forall x)(P(x))$$

或省略括号写成 $(\forall x)P(x)$

（这里除 P(x) 外没有联结词了，外层括号可省略，一般情况不可省，如$(\forall x)(P(x)\vee Q(x))$，括号不可省）。

符号$(\forall x)$读作所有的 x 或一切 x 或任一 x，而$\forall$就是对个体词起约束作用的全称量词。

命题$(\forall x)P(x)$当且仅当对论域中所有的 x，P(x)均为真时，值方为真。

现在讨论存在量词，如“有的事物是动物”，这命题中“有的”就是表示个体变元数量“至少有一个”的词，也可

用“存在一个”，“有一个”，“某些”等同义词来表示。这句话的意思等于说

有一事物，它是动物

或　有一 x，x 是动物

形式描述为

$$(\exists x)\ (x \text{是动物})$$

也可写成 $\exists x$ (x 是动物)

如果 Q(x) 表示 x 是动物，那么这句话就可写成

$$(\exists x)(Q(x))$$

或省略括号写成 $(\exists x)Q(x)$

符号 $(\exists x)$ 读作至少有一个 x 或存在一个 x 或有某些 x，而 $\exists$ 就是对个体词起约束作用的存在量词。

命题 $(\exists x)\ Q(x)$ 当且仅当在论域中至少有一个 x_0 使 $Q(x_0)$ 为真时，值为真。

3. 约束变元和自由变元

在一个含有量词的命题形式里区分个体是受量词的约束还是不受量词约束是重要的。在定义合式公式以及对个体变元作代入变形时都需区分这两种情形。

量词 $\forall$，$\exists$ 是对命题形式作限制的，如

P(x) 表示 x 是有理数，这里的变元 x 不受任何量词约束，便称作是自由的。而

$$(\forall x)P(x)$$

中两处出现的 x 都是受量词 $\forall$ 的约束，便称作约束变元，受约束的变元也称被量词量化了的变元。

命题形式 P(x)，其中 x 是自由变元，P(x) 不是命题，不能确定真假，然而当 P 为某一确定的谓词常项时，$(\forall x)$ P(x) 其中 x 是约束变元，这里又不出现其他自由变元，这个

命题形式就化为命题了。如 $P(x)$ 表示 x 是有理数，那么 $(\forall x)P(x)$ 表示任一事物 x 都是有理数，这话不真。因为 x 的论域是万物的集合，故 $(\forall x)P(x)=F$。然而命题 $(\exists x)P(x)$ 表示有一个事物 x 是有理数，它是命题而且取值为真。

这样在一命题形式中，当函数，谓词确定为常项后，由命题形式化为命题，一是指定个体变元为常元，二是通过对个体变元量化来实现。

有的命题形式中，如

$$(\forall x)P(x)\vee Q(y)$$

变元 x 是约束的而变元 y 是自由的。

符号 $(\forall x)P(x)$ 和 $(\forall y)P(y)$ 含义是一样的。可分别读作对一切x，x 具有性质P；对一切y，y具有性质P，这两句话除使用个体符号不同外并无差异。或说 $(\forall x)P(x)$ 与 $(\forall y)P(y)$ 同时取真或取假，这样的命题不必加以区别了，于是写成

$$(\forall x)P(x)=(\forall y)P(y)$$

4. 量词的辖域

指的是量词所约束的范围。

如，$(\forall x)R(x,y)$　$R(x,y)$就是$(\forall x)$的辖域

$(\exists x)(\forall y)P(x,y)$　$P(x,y)$ 是 $(\forall y)$ 的辖域，而 $(\forall y)P(x,y)$是$(\exists x)$的辖域。

$(\forall x)P(x)\vee(\forall x)Q(x)$，$P(x)$是第一个量词$(\forall x)$ 的辖域，$Q(x)$是第二个量词$(\forall x)$的辖域。

§1.3 合式公式

象命题逻辑一样，需限定所讨论的命题形式的范围。由于谓词逻辑引入了个体词、量词，从而带来了复杂性。

首先明确所称的谓词逻辑，仅限于对个体词的量化，而不允许量词作用于命题变项或谓词变项。即只研究 $(\exists y)(\forall x)$

$P(x,y)$形式的命题，而不讨论$(\exists p)(Q(x)\rightarrow p)$或$(\exists Q)(Q(x)\vee P(x))$形式的符号，也不讨论谓词的谓词。这样限定的范围通常叫作一级谓词逻辑或狭谓词逻辑。这是相对高阶逻辑而言的。

再明确一下符号。

命题变项以 p,q,r……表示。

个体变项以 x,y,z……或以大写单词表示。

函数以 f,g……或以小写单词表示。

谓词变项以 P，Q，R……或以大写单词表示。

五个联结词仍以～（否定），∨（折取），∧（合取）→（蕴涵），↔（双条件）来表示。

量词有$\forall$，$\exists$。

括号以（ ）表示。

现在的问题是除这些初始符号外，通过它们可形成哪些合法的符号？这就要给出形成规则或说给出合式公式的定义。

将不含量词和联结词的命题形式 $P(x)$，$Q(x,y)$……，称作原子谓词公式，下面递归地定义合式公式（或简称合式）。

（1）命题常项，命题变项和原子谓词公式都是合式公式。

（2）如果A是合式公式则～A也是合式公式。

（3）如果A，B是合式公式，而无变元x，在二者之一中是约束的而在另一个中是自由的。则$(A\wedge B),(A\vee B),(A\rightarrow B),(A\leftrightarrow B)$**都是合式公式（最外层括号可省略）。**

（4）如果A是合式公式，而x在A中是自由变元，则$(\forall x)A,(\exists x)A$**也是合式公式。**