定理证明辅助工具 Isabelle 剖析与应用

郭慧梅 缪淮扣 陈怡海
(上海大学计算机工程与科学学院 上海 200072)

摘 要 Isabelle 是一个通用的定理证明器,应用领域广泛。介绍 Isabelle 逻辑系统的功能和构成,分析了 Isabelle 的规格说明语言、验证系统的特点,并给出了用 Isabelle 逻辑系统来构造 Z 规格说明的定理证明的方法。

关键词 逻辑系统 定理证明器 形式化方法

ANALYSIS AND APPLICATION OF THEOREM-PROVING AIDING TOOLS——ISABELLE

Guo Huimei Miao Huaikou Chen Yihai
(*School of Computer Engineering and Science, Shanghai University, Shanghai 200072, China*)

Abstract Isabelle is a generic theorem proving environment. Its application area is broad. The function and structure of Isabelle are introduced, and the features of Isabelle's logic system are analyzed. The method to construct theorem proving of Z specification by using Isabelle's logic system is given.

Keywords Logic system Theorem prover Formal method

0 引 言

在过去的几十年间,研究人员提出并实现了许多定理证明工具。最初研究的重点是如何让机器来自动完成数学定理(如群论)的证明过程。这些工具通常是基于归结反演的方法,代表性的例子有 Otter,SETHEO 等工具,它们能连续数日运行并能求解一些非常困难的定理证明问题。为了实现自动化,证明工具应用了许多特殊的算法、数据结构和优化算法来加快归结的效率。

逐渐地,定理证明技术被应用于处理和计算机科学更为相关的问题。定理证明的一个发展趋势是交互式定理证明,工具允许用户对证明的搜索过程有更多的控制,特别是通过证明工具提供的策略机制来引导证明的过程。与最初的定理证明工具相比,证明工具不只是简单地告诉用户,定理为真或为假,而是有更为形式的证明过程。

定理证明工具的一个最新的发展趋势是逻辑框架的概念。证明工具采用元逻辑的表示法。元逻辑规定了证明是如何从原始的推理规则中构造的。这些工具通常配备有各种庞大的理论(理论是由逻辑中的常量,类型,公理,定理,推理规则组成)。在使用定理证明器进行定理证明之前,用户必须提供(或选择)一个对象逻辑。对象逻辑定义了逻辑系统,逻辑的语法和推理规则。

Isabelle[1] 正是基于这一发展趋势而开发的定理证明辅助工具。Isabelle 是英国剑桥大学的 Lawrence C. Paulson 和他的合作者于 1986 年共同开发完成。目前,其许多工作由德国慕尼黑工业大学的 Tohias Nipkow 来完成。

Isabelle 是一种通用的定理证明器,它为证明系统的开发提供了一个通用框架。Isabelle 用函数型语言 ML[2] 来编写,使用自然演绎规则来进行定理证明。它支持对数学公式的形式化描述,并为这些公式的逻辑演算提供了证明工具。Isabelle 主要应用于数学证明的形式化,特别是形式化验证,包括对计算机硬件和软件的正确性验证,以及对计算机语言和协议的属性的验证。

1 Isabelle 的逻辑系统

Isabelle 系统作为一个通用的定理证明辅助工具,一方面,它可以作为快速原型推理系统的通用框架;另一方面,它所支持的对象逻辑,为用户提供了一个良好的定理证明环境。

与其它的定理证明辅助工具相比,Isabelle 逻辑系统的特点突出表现在以下两个方面:

1) *支持多种对象逻辑*

绝大多数定理证明辅助工具仅能支持单一的对象逻辑尤其是高阶逻辑 HOL,如 PVS,而 Isabelle 系统支持多种对象逻辑,包括直觉主义一阶逻辑(IFOL),建设性类型理论(CTT),高阶逻辑(HOL),基于序列演算的一阶逻辑(LK)和模态逻辑等。所有的对象逻辑都是建立在 Pure Isabelle 这一基础之上的,如图 1 所示。Pure Isabelle 实现了元逻辑并提供了基本的数据结构:类型、项、基调、定理和理论。

Isabelle 的这一特点充分体现了其系统的通用性和灵活性,

收稿日期:2005 - 08 - 22。基金项目:国家自然科学基金项目(60373072,60673115),上海市教委科技发展基金(05AZ70)。郭慧梅,硕士生,主研领域:软件工程,形式化方法。

万方数据

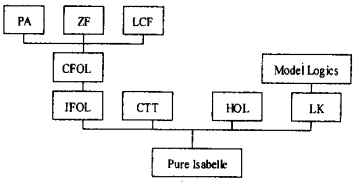

图 1　Isabelle 支持的对象逻辑

用户可以根据自己的需要来选择对象逻辑。

2) 支持定义新的逻辑

Isabelle 最显著的特点在于它支持定义新的逻辑。最基本的 Isabelle 系统是一个直觉主义高阶逻辑的定理证明工具,我们称该逻辑为元逻辑。实例化这一通用系统可支持其他对象逻辑。通过在 Isabelle 系统中定义对象逻辑具体和抽象的句法以及推理规则,我们就可以实现一个新的逻辑系统。

Isabelle 的逻辑系统实际上是分层的理论结构。一个理论包含一组类型、变元、定义和定理等。每个理论文件记录了某些类型、常数、公理、定义和定理,同时具有指向它的上级理论的指针,这样,所有的理论就构成了分层的树形结构。最基本的理论定义了最基本的类型和公理,在此基础上,逐步构成各种数据类型和经过证明的定理,并为以后更高层的理论及相关的定理证明所利用。

在 Isabelle 系统中构造一个新的逻辑理论的最好方法是在 Isabelle 支持的对象逻辑的基础上构造。例如,构造一个对表及其操作进行形式化的理论,如图 2 所示,在纯理论的基础上,选择一个系统支持的对象逻辑 FOL(一阶逻辑)。FOL 只包含经典的理论,没有对自然数和表进行定义,因此我们对其进行扩展,分别形成自然数的理论 Nat 和表的理论 List,合并这两个理论,并将其扩展为一个定义表的长度的理论 Length,即用自然数来表示表的长度。

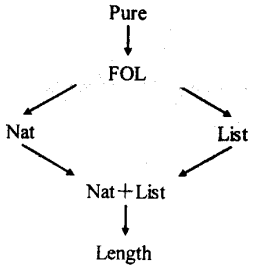

图 2　表的长度的理论定义

2　Isabelle 的规格说明语言

一般来说,如果规格说明语言的表达能力很强,那么其相应的证明系统的推理能力就会减弱。反之,对于一个高度机械化的定理证明器,它的规格说明语言的表达能力会受到很大的限制。如 Boyer-Moore 定理证明器利用了无类型、无量词的结构性很强的描述语言,因此推理证明能力很强。客观地说,Isabelle 的规格说明语言不如某些定理证明器的规格说明语言的表达能力强(如 PVS),但它具有自己的特色,主要体现在以下几个方面:

1) 具有丰富的类型系统

Isabelle 的规格说明语言基于强类型语言 ML,其强类型机制可以帮助用户及时纠正程序的类型错误,保持类型前后的一致性。Isabelle 具有丰富的类型系统,包括元组类型、函数类型和多态类型等。多态类型是其中一种具有特色的类型,以'a,'b 等来表示。有些函数没有固定的类型,例如定义一个相等函数,其结果原封不动地回送其自变量值,不管它的自变量是数值型、布尔型还是函数型。对这样的函数,我们无法确定其具体的类型,就可以用多态类型来表示。多态类型增强了 Isabelle 类型系统表示的灵活性。

2) 句法易于扩展

Isabelle 使用类型化的 λ 演算(typed λ-calculus)来表示句法。要实现一个新的逻辑证明系统,就必须在 Isabelle 系统中定义对象逻辑具体和抽象的句法以及推理规则。Isabelle 系统提供了对类、类型和项的定义。通过添加额外的类、类型和项,Isabelle 的句法得以扩展,为逻辑系统的定义奠定了良好的基础。

3) 支持模块化的设计

理论是 Isabelle 语言的基本模块,其基本结构如下:

```
T(理论名) = S1(父理论名) + … + Sn +
类说明
类型说明
类型属性说明
常量说明
转换规则说明
元逻辑定义
规则说明
End
```

新建的理论 T 继承了其父理论 S1…Sn 的类型、常量和规则等,并通过定义新的类、类型、常量和规则等对父理论进行扩充。当执行理论 T 时,它所继承的父理论会由系统自动载入,有效地避免了重复的理论定义。

4) 例子

下面通过定义一个表的理论 List 为例来说明上述特点。

```
Theory List = FOL +
types 'a list
arities list::(term)term
consts Nil::'a list
       ":"::['a,'a list]=>'a list (infixr 60)
       app::['a list,'a list,'a list]=>0
       rev::['a list,'a list]=>0
rules  appNil "app(Nil,ys,ys)"
       appCons "app(xs,ys,zs)"
       revNil "rev(Nil,Nil)"
       revCons "[|rev(xs,ys);app(ys,x:Nil,zs)|]==>rev(x:xs,
zs)"
end
```

新定义的理论 List 基于父理论 FOL。类型定义 types 引入了类型构造符 'a list,其中 'a 表示表中的元素是多态类型。arity 是对类型的属性的说明。对于类型构造符 list,它的属性就是类型的类。consts 部分声明了四个常量:空表 Nil,表构造符":"、表的连结 app 和表的逆置 rev。rules 定义了若干条有关表的操作规则,这些规则可以用到以后的定理证明当中。

上述示例充分显示了 Isabelle 系统类型定义的多样性和灵活性,逻辑结构的严密性,以及理论定义的模块化和可扩充性。

3　Isabelle 的定理证明器

证明一个定理,就是要找出一个公理或定理序列。根据序列中的前面的元素(公理或已经证明的定理)利用推理规则可以得到其后面的元素,最后得到的就是要证明的定理。

在 Isabelle 系统中对定理证明的构造方法有两种:前向证明和后向证明。前向证明是从定理的前提和公理、定理、定义等推

万方数据

导出定理的结论。后向证明是一种基于目标的定理证明方法。证明的过程从需要证明的目标开始,应用推理规则,将目标不断地分解为子目标,直到所有的子目标得到证明。后向证明是 Isabelle 系统中常用的定理证明构造方法。下面分别论述 Isabelle 定理证明器的几个特色:

1) 具有强大的规则库

在定理证明的过程中,需要用到各种基本的规则。定理证明工具所提供的规则库中的规则越多,证明的过程就越容易。如前所述,Isabelle 系统的每一个理论中都包含了相关的规则和定理,同时,用户可以根据自己的需要添加定理,并对其进行证明。如果新添加的定理通过证明是正确可行的,系统将存储定理,并且可以应用到以后的定理证明当中。

2) 灵活高效的命令集

用 Isabelle 进行定理证明的过程中,通常用到两种命令:一种是证明命令,另一种是辅助命令。辅助命令主要是用来检查证明的状态,并控制其显示。在证明命令中,较常用的证明命令的形式为:apply(method)。其中,method 是证明操作,如命令 apply(auto)是对子目标应用证明策略 auto,简化子目标。当然还有许多其它的证明命令,可以参阅 Isabelle 用户手册[3]。值得一提的是,Isabelle 提供了在理论库中进行定理查找的命令 thms_containing。执行此命令,即可以在库中迅速找出相关的定理。例如:thms_containingx < y x <= y,系统就会给出所有包含"<"和"<="关系的定理。这使定理的查找更加方便快捷。

3) 证明过程的可读性强,自动化程度高

定理的证明有时是一个非常复杂的过程,特别是对于一些大型的定理证明,其过程不可能一蹴而就,需要不断的尝试才能成功。Isabelle 不仅可以显示证明每一步的状态的变化,而且能够自动保存最终的证明脚本,便于用户随时查看。同时,随着 Isabelle 系统的不断改进和完善,证明语言不但易于机器接受,而且易于广大用户理解,可读性不断增强。

Isabelle 以人机交互的形式实现定理的证明,并通过应用策略和策略组来支持自动证明。其中,高层的证明由人来进行控制,底层的简单证明由机器来自动完成,这样既保证了证明过程的理性进行,又节省了大量的精力和时间。

4 使用 Isabelle 构造 Z 规格说明的嵌入式定理证明系统

Z[6]是一种表达能力丰富的规格说明语言,它在软件工程界和工业界得到了广泛的应用。但是,目前对 Z 的工具支持十分有限,大多数工具只提供了 Z 规格说明的语法检查和类型检查,而缺少有效的定理证明器提供推理的机器支持。因此,我们考虑将 Z 嵌入到 Isabelle 中来实现定理证明。

将一种逻辑系统嵌入到一个已有的定理证明系统有两种不同的方法:一种是句法嵌入,把定理证明器自身使用的逻辑作为元逻辑,被嵌入的逻辑通过在元逻辑中引入新的句法,并且把对象逻辑中的推理规则表达为元逻辑中的公理来实现,如 Isabelle/DC 系统。另一种是语义嵌入,是指用定理证明器实现的元逻辑来描述对象逻辑的语义,并在证明系统中通过使用推理方法得到对象逻辑中的推理规则。Z 没有一个统一的定律库,使用语义嵌入的优点是能从语义定义中推理出 Z 的定律。因此,我们采用语义嵌入的方法。

高阶逻辑(HOL)是 Isabelle 支持最好的一种对象逻辑。Isabelle/HOL 具有强人的描述能力,能够较好地描述 Z 的数学定义,同时它的集合理论库为 Z 数学工具库的定义提供了良好的基础。因此我们选择 Isabelle/HOL 系统作为 Z 定理证明工具的开发基础。

经过初步研究,将 Z 语义嵌入 Isabelle/HOL 系统可以分为三个步骤:

(1) 将 Z 语言中的逻辑运算符号定义为常量,并采用 Isabelle 系统中的注释机制说明符号的具体句法;

(2) 使用高阶逻辑来定义符号的语义;

(3) 使用 Isabelle/HOL 系统提供的推理机制从 Z 的语义定义中推导出证明中所需要的 Z 基本定律。

根据 Z 标准定义中的数学工具库的层次关系,可以将 Z 在 Isabelle/HOL 系统中的理论定义分为六大部分:集合 ZSet,关系 ZRel,函数 ZFun,数 ZInt,有穷集合 ZFin 和序列 ZSeq。

各理论间的层次关系图如图 3 所示。

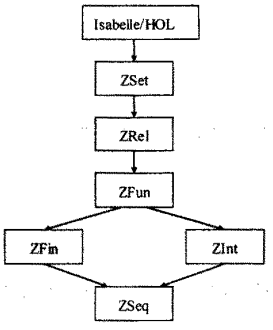

图 3 理论层次关系图

每一个理论分别定义了关于 Z 的基本操作和相关定律。通过定义,将 Z 的语义嵌入到 Isabelle/HOL 系统中,我们得到了一个 Z 规格说明语言的嵌入式定理证明系统,应用这一系统,可以进行进一步的 Z 的定理证明的研究。

5 总 结

Isabelle 作为一个通用的定理证明工具,已经广泛应用于许多领域,其逻辑系统的通用性和灵活性也得到了广大用户的认可。随着 Isabelle 系统的不断完善,越来越多的用户使用它来开发适合自身需要的定理证明系统,如本文作者给出的用 Isabelle 构造 Z 规格说明的嵌入式定理证明系统。

尽管 Isabelle 是辅助定理证明的有效工具,但仍有许多方面需要进一步的完善。例如,Isabelle 拥有大量的规则和策略,这使得工具的证明能力非常强大,但同时也给用户带来了一定的麻烦。因为用户首先必须判断,使用哪一种策略或命令才能有利于目标的最终实现。因此,在策略或命令的有效组织和使用上还有待进一步研究。同时,还应增强规格说明语言的表达能力,使用户界面更友好,提高证明的效率。

参 考 文 献

[1] Lawrence C Paulson. Introduction to Isabelle. University of Cambridge, Computer Laboratory, 2004, 3.

[2] Tobias Nipkow, Lawrence C Paulson, Markus Wenzel. Isabelle HOL: A Proof Assistant for Higher-Order Logic. LNCS 2283. Springer-Verlag, 2004, 4.

[3] Lawrence C Paulson. The Isabelle Reference Manual. University of Cambridge, Computer Laboratory, 2004, 4.

[4] Wenzel M. The Isabelle/Isar reference manual. Technical report, 2003. 3. Available with online documentation.

[5] Paulson L C. Isabelle: A Generic Theorem Prover, Volumn 828 of Lecture Notes in Computer Science, Spring-Verlag, 1994: 283 - 298.

(下转第 43 页)

万方数据

A 是 BC 的中点,显然新的点就在 BC 所在的直线上;对于 $AB \perp CD$,如果 B 是垂足,则新的点就在 CD 所在直线上;而对于 $AB//CD$,如果被动点是 B,则新的点要在 A 或 B 所在直线上……等等。

如果结论中的点没有被动点,则本系统认为无法使用反证法。对于这一问题,还有待进一步研究。

如图 3 中 P,Q。任取其一,如 Q,然后找到 Q 所在线段,在线段上作一个新点,如 M。假设 $PM//BC$,把该结论作为条件放到推理信息库中。

1.3 推　理

对于一道命题,本文目前是由用户决定使用直接法还是反证法。下面以反证法为例予以说明推理过程。对于每一次推出的新结论,都要检查是否产生了矛盾,这里有三方面的含义:

- 和已知推理信息库发生矛盾,如库中已经存在 $AB \neq CD$,但新结论正是 $AB = CD$,另一方面如果库中已经存在 $\angle ABC = 90°$,而新结论却是 $\angle ABC = 45°$;
- 二是违背几何知识,如假设推理信息库中有 $\angle ABC = 90°$ 及 $\angle ACB = 90°$,由 $\angle ACB + \angle ABC + \angle BAC = 180°$ 得到 $\angle BAC = 0°$,显然是错误的;
- 唯一性出现问题,如线段的中点只能有一个,过一点作另一直线的垂足只能有一个等等。

由于否定性谓词对应有肯定性谓词,因此对于肯定型结论或否定型结论,只需要在相对应的语句中检查即可。反证法推理流程图如图 4 所示。

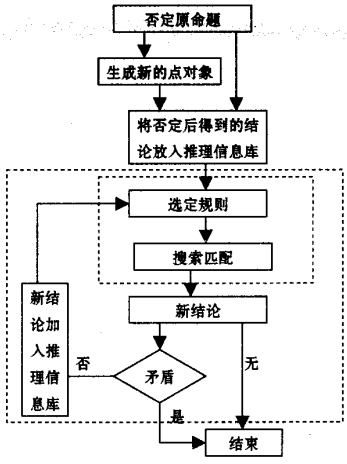

图 4　推理流程图

其中虚线框表示内部有循环,对于每一轮的搜索匹配,要将库中规则依次使用,只要有新结论推出,就要进行下一轮搜索匹配。

2 运行实例

如图 5 所示,已知:梯形 $ABCD$,$AB//CD$,$AC = AB + CD$,E 是 BD 的中点,且 AE 是 $\angle BAC$ 的平分线,AE 的延长线和 CD 的延长线交于点 F。

证明:CE 是 $\angle ACD$ 的平分线。

这道命题很简单,用直接法也很容易得证。为了用反证法,本文假设 CE 不是 $\angle ACD$ 的平分线。这里点 E 是被动点,对原命题的否定,就要增加新的点。这是关于角平分线的谓词,通过分析,新点应该在 AF 线段上。因此在 AF 上作一点 G,连接 CG,假设 CG 是 $\angle ACD$ 的平分线。证明过程见图 6。

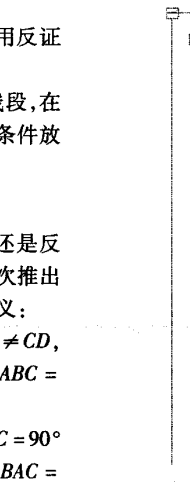

图 5　实例

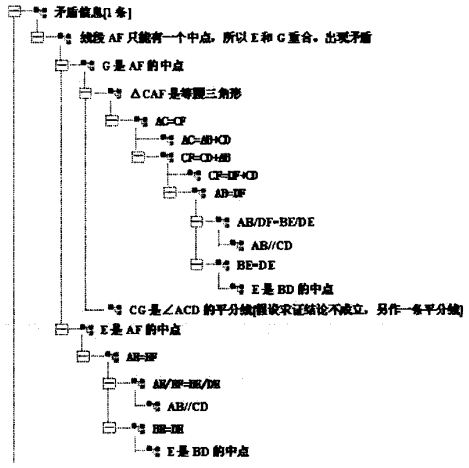

图 6　证明过程

3 结束语

本文给出的反证法算法结合前推搜索法,能够证明一些利用前推搜索法不能证明的命题,或者能够比较容易推出用前推搜索法不易证明的命题。实验证实了该算法是可行的,但何时及对哪类命题计算机自动选择反证法,仍然是一个难题。本文是由用户选择使用反证法。下一步,我们需要对几何问题进行总结,找出一定的规律,使得自动推理软件能够智能选择使用何种推理方法。

参 考 文 献

[1] 张景中. 平面几何新路. 四川教育出版社,1992.
[2] 张景中,高小山,周咸青. 基于前推法的几何信息搜索系统. 计算机学报,1996,19(10).
[3] 吴文俊. 几何定理机器证明的基本原理. 科学出版社,1984.
[4] Charles N Fischer, Richard J LeBlanc. 编译器构造 C 语言描述. 郑启龙,姚震,译. 机械工业出版社,2005.
[5] 郭四稳. 基于数据库技术的自动推理系统. 博士论文,2001.
[6] 洪加威. 能用例证法证明几何问题吗. 中国科学,1986,3:234-242.
[7] 李卫华,张黔,刘娟. 归纳法推理系统[J]. 计算机学报,1996(3).
[8] 赵沁平,李波,罗玉龙. 关于类比推理的若干问题的研究[J]. 计算机科学,1993(2).
[9] 徐明,胡守仁. 基于事例推理的检索模型研究[J]. 计算机科学,1993(4).
[10] 张仰森,黄改娟. 人工智能实用教程[M]. 北京:北京希望电子出版社,2002.

(上接第 16 页)

[6] 缪淮扣,李刚,朱关铭. 软件工程语言 - Z. 上海科技文献出版社,1999.
[7] 韩俊刚,杜慧敏. 数字硬件的形式化逻辑. 北京大学出版社,2001.
[8] Bowen J, Gordon M. A shallow embedding of Z in HOL, information and Software Technology, 1995, 37(5-6): 269-276.

万方数据