Teaching Mathematical Logic for Information Security Specialty

LI Zhi-min, CHEN Jian-xin, LU Jun, YE Cong-huan

*School of Computer and Information Science, Xiaogan University, Xiaogan, Hubei Province , China,*432000

wyjlst1970@163.com

Abstract: Mathematical logic is an important basic knownedge for learning in information security specialty. Through learning mathematical logic, students may have a solid foundation in studying professional course and in the future speciality of security software and hardware development. For the purpose of improving quality of teaching mathematical logic, the author proposes his teaching approach from the aspects of focusing on the reasonable extending of teaching content following the framework of Proof Theory, introducing basic knowledge on non-classical logic, introducing information security applications-oriented background knowledge and the imploying of advanced teaching resources and aided teaching tools (for example COQ& Proof web).

Keywords: Mathematical logic; Information security speciality; COQ; ProofWeb

面向信息安全的数理逻辑教学

李志敏，陈建新，卢军，叶从欢

孝感学院计算机与信息科学学院，孝感，中国，432100

wyjlst1970@163.com

【摘要】数理逻辑是信息安全专业其他课程学习的重要基础。通过数理逻辑知识的学习，能为学生专业课程的学习和将来从事信息安全方向软、硬件开发打下坚实的基础。本文就如何提高信息安全专业数理逻辑的教学质量，提出了从证明论的角度整理数理逻辑知识体系，合理介绍非经典逻辑知识体系，注重数理逻辑在信息安全领域中应用背景的介绍，引入数理逻辑教学资源和教学辅助工具（COQ& Proof web）等教学方法。

【关键词】数理逻辑；信息安全专业；COQ；ProofWeb

1 引言

数理逻辑的主要分支包括：逻辑演算(包括命题演算和谓词演算)、模型论、证明论、递归论和公理化集合论。计算机的广泛使用，极大地改变了数理逻辑的地位和作用。数理逻辑已经成为应用数学学科的重要分支。它广泛应用于人工智能、程序描述和验证、形式语言、自动定理证明、算法理论等领域[1]。数理逻辑在人类脑力劳动自动化的进程中，发挥着越来越重要的作用。计算机科学中逻辑的作用体现在如下两个方面:

1) 逻辑是计算机科学若干领域的基础。它运用严格的数学方法研究计算和问题解决的基本原理。

2) 逻辑不仅服务于理论，更为重要的是，逻辑的语言和演算已经成为软件开发技术（VDL,Z,HOL,TAL+等）、数据库系统和知识表示的工具。特别是，逻辑能用作编程语言（例如 PROLOG,DATALOG 等）。

计算机信息安全专业本科生应具有较强的逻辑推理和问题求解能力，并有较好的数学素养。特别地，学生还应对形式系统和形式化方法有一定程度的熟悉。为了达到上述教学目的，《数理逻辑》课程的教学起着重要的基础作用[2]。

本文主要讨论信息安全专业本科生数理逻辑的教学问题。目前，有的高校非常重视数理逻辑的教学，给学生打下了坚实的理论基础，提高了后续学习能力。然而，在实际教学中，多数院校数理逻辑作为离散数学课程的一部分，授课时间仅有二十多个课时。教学内容不断精简，造成学生完成这部分知识的学习过程后，仍然

资助信息：湖北省孝感学院科研资助项目 Z2009019.

978-1-935068-09-9

感觉仅仅知道了一些零碎的概念。对信息安全专业的学生而言，课程知识若不能系统化，就不知道如何应用所学知识解决问题。不利于学生对后续专业课程的学习，影响到学生计算机思维逻辑的正确形成。因此，提高数理逻辑的教学水平和质量，对提高后续课程的学习能力具有重要的意义。

2 从证明论的角度整理数理逻辑知识体系

证明论在许多应用方向起着重要作用，例如，逻辑编程，程序描述等。任何逻辑都有两个重要层面，语义（semantics）和语法 (syntax，也可以称作是 proof theory 或 proof systems)。研究逻辑一般从语义、语法以及二者之间的联系三个方面展开。由于授课时间的限制，普通本科生教材通常只介绍语义，较少介绍语法 （有的教材叫做形式证明或证明技术），基本不讲语义和语法之间关系。我们在学完一般教材介绍的命题逻辑、谓词逻辑以及推理与证明技术之后，应该从以下几个方面整理所学知识，构建知识体系。

2.1 介绍自然演绎系统

教学中首先引导学生得到系统推理规则。自然演绎规则的引入是本科生容易接受的，学生只需要整理一般教材上的重言蕴涵式就可得到表 1 中所述的自然演绎规则。对任何逻辑符号都有如下两种类型的推理规则：

(1)介入规则：依照逻辑符号，从多个公式中产生一个公式。

(2)消去规则：分割公式消去一个逻辑符号。

Table 1. Rules of Natural Deductive System
表 1. 自然演绎系统规则

$\wedge$I	$\dfrac{\alpha,\beta}{\alpha\wedge\beta}$	$\wedge$E	$\dfrac{\alpha\wedge\beta}{\alpha}$ $\dfrac{\alpha\wedge\beta}{\beta}$
$\vee$I	$\dfrac{\alpha}{\alpha\vee\beta}$ $\dfrac{\beta}{\alpha\vee\beta}$	$\vee$E	$\dfrac{\alpha\vee\beta,\ [\alpha]\Rightarrow\gamma,\ [\beta]\Rightarrow\gamma}{\gamma}$
$\rightarrow$I	$\dfrac{[\alpha]\Rightarrow\beta}{\alpha\rightarrow\beta}$	$\rightarrow$E	$\dfrac{\alpha,\ \alpha\rightarrow\beta}{\beta}$
$\neg$I	$\dfrac{[\alpha]\Rightarrow\perp}{\neg\alpha}$	$\neg$E	$\dfrac{[\neg\alpha]\Rightarrow\perp}{\alpha}$
$\perp$I	$\dfrac{\alpha,\neg\alpha}{\perp}$	$\perp$E	$\dfrac{\perp}{\alpha}$
$\forall$I	$\dfrac{\beta(x_i/a_j)}{\forall x_i\beta}$	$\forall$E	$\dfrac{\forall x_i\beta}{\beta(x_i/t)}$
$\exists$I	$\dfrac{\beta(x_i/t)}{\exists x_i\beta}$	$\exists$E	$\dfrac{\exists x_i\beta,\ [\beta(x_i/a_j)]\Rightarrow\gamma}{\gamma}$
=I	$\dfrac{}{t=t}$	=E	$\dfrac{t_1=t_2,\alpha}{\alpha(t_1/t_2)}$

其中⊥表示矛盾，个体常元集合是可数集，t，t_1，t_2 是项，$[\alpha]\Rightarrow\gamma$ 表示 γ 由 α 的证明，x_i/t 表示 x_i 的出现用 t 替换。

模板反证法的形式化就是¬E 规则，在数学和逻辑领域有时受到质疑。如果去掉¬E 规则就可以得到直觉逻辑。进一步，⊥E 规则也省略，就得到极小逻辑。

自然演绎系统对经典一阶逻辑的语义推论关系是完全的。去掉¬E 规则的系统，对直觉逻辑的语义推论关系是完全的。最简单推导（即证明的规范形式）的存在性是证明论中的一个重要问题。介入规则和消去规则是互逆的。若将消去规则用到由介入规则得到的公式上，显然是多余的。 在证明的规范形式里，这样的互逆对是不允许出现的。任何规范推导的过程是：介入规则应用序列的后面是消去规则的序列。不难理解，证明论基本定理成立：任何推导可以变换成规范形式。

自然演绎系统的引入，并适当补充相关知识，使学生对逻辑系统的有了较为深入认识，培养了学生形式化建模的兴趣和基本能力。

2.2 重视范式的理论与应用教学

范式理论是为学习后面的归结原理做准备的。它是数理逻辑的重要内容,在后续课程数据结构、数据库原理、自动定理证明、编译原理、软件工程、计算机网络、人工智能等领域中有广泛的应用。在信息安全专业本科生的教学过程中，范式是一部分易被忽视的教学内容之一。

首先介绍前束范式。任何一阶公式都有与它等价的前束范式，且这样的前束范式不是唯一的。

然后介绍一个特殊的前束范式—Skolem 范式，它是由前束范式消去存在量词得到的。

直接注意到对一个给定的模型，$\forall x_1 \exists y_1 \alpha$ 的真理性含义是存在函数 $Y_1(x)$使得 $\forall x_1 \alpha$ (y_1/ $Y_1(x_1)$)在此模型中取真值。全称 Skolem 范式的想法基于由函数符号 Y_1 扩展的语言。上述函数称为 Skolem 函数。求一个公式的 Skolem 范式，一个重要作用是可以用这个范式来检测该公式是否是可满足的。

2.3 归约一阶句子到命题

对命题逻辑语义，有能行的方法判定推论关系。而且，在不同的架构下，都很容易构造计算的算法。多数实际问题需要一阶逻辑而不是命题逻辑。然而，在一阶逻辑，没有命题逻辑那样的能行算法。这就是为什么 Herbrand 定理显得非常重要。Herbrand 定理归约一阶公式集的不可满足性成为基本公式集的不可满足性。基本公式集可以看成是命题公式集。

设 α 是无量词公式。α 的基本实例是将 α 的变量位置替换成无变量的项得到的。基本实例的逻辑叫做零阶逻辑，它等价于命题逻辑。我们的目标是：

对任意一阶公式集∑找一个零阶公式集$\sum_0$，使得∑是不可满足的当且仅当$\sum_0$不可满足。

实际上，前述目标不可能实现。Davis-Putman 方法给出了证明无量词一阶公式集的不可满足性的步骤如下：

（1）令 H 是$\sum^g$的有限子集，$\sum^g$是∑的基本实例集。

（2）用命题逻辑试证 H 是不可满足的。若获证，终止。否则，扩充 H，继续第（2）步。

由于在通常的情况下，基本实例的数量很大（在很多情况下有无限个），所以直接使用上述方法进行自动推理（定理证明）的几乎是不可行的，因为有许多的基本句不仅与我们的推理无关，而且会推出不必要的结论。人们提出了各种有效的方法来选择或限制用于自动推理的基本句数量。希望能减少需要考虑的基本句的数量，达到提高自动推理的效率的目的。

有一个效率较高的方法是元变量法。在表 1 的 $\forall$ E 规则中 t 是元变量，代表目标语言的项。证明过程中，用什么基本项是不可判定的。此时就用元变量来替换，这样程序会更有效率。随后，寻找证明的过程可能产生元变量的约束条件，并最终构造出正确的项。

对于信息安全专业的本科生，教师应该指导和鼓励学生查阅有关资料，了解现有的提高证明效率的方法，为学生今后工作或继续深造打下良好基础。

2.4 归结原理

有的教材省略了归结原理。由于归结原理在自动定理证明领域地位很重要，我们认为在数理逻辑的本科教学中不能简单处理归结原理的有关知识。

归结是一种简单的演算技术，这种简单性是由于只能用于 Skolem 范式。教学中，先讲清楚命题逻辑归结推理，包括归结证明过程，归结推理规则，通过示例和练习让学生熟练掌握。谓词逻辑的归结推理法的困难在于出现了量词和变元，因此也比较复杂。在建立子句集时，如何消去量词，特别是存在量词是关键。例如要证$\alpha \rightarrow \beta$ 是定理，转化为证明$\alpha \wedge \neg \beta$ 是矛盾式。先将$\alpha \wedge \neg \beta$ 化为前束范式，然后再化为 Skolem 范式，得到仅含全称量词的公式。去掉全称量词化合取范式，便可得到了子句集。对子句集归结过程中，注意使用合一置换得到互补对。

在信息安全专业教学过程中,引导学生设计归结推理程序，是培养学生应用能力的一个重要手段。我们感觉到，数理逻辑课程只有理论没有实践教学环节，不能有效激发学生学习兴趣，不利于学生能力的培养。

3 合理介绍非经典逻辑知识体系

对于信息安全专业的学生来说，了解非经典逻辑知识是必须的。因为在安全协议形式化分析领域，非经典逻辑发挥了重要。

介绍非经典逻辑知识体系时，要注意讲明经典逻辑的系统架构及其局限性。说明非经典逻辑在那些方面克服了经典逻辑的局限性，以及对经典逻辑在那些方面有发展。自 20 世纪初以来，为了解决经典逻辑的异常现象。先后出现了一些非经典逻辑，它们分别从不同角度解决经典逻辑的异常现象。1907 年，荷兰数学家布劳维尔提出在无穷集的推理中排中律不适用的思想，因此成为直觉主义逻辑的创始人。1920 年，波兰逻辑学家卢卡西维茨提出了三值命题演算，建立了历史上最早的多值逻辑系统。非经典逻辑真正作为群体出现是在 20 世纪 60 年代前后。有的非经典逻辑系统是对经典逻辑系统的语法扩展，例如模态逻辑、时态逻辑、道义逻辑、认知逻辑、问句逻辑等。经典逻辑的基本公理、推理规则和基本算子在语法扩展型的

978-1-935068-09-9 © 2010 SciRes.

非经典逻辑中仍然保留原有的。但是为了适应新情况，增加了一些新算子。另外的非经典逻辑系统是与经典逻辑系统的不同在于语义方面。主要是命题真值的取值不同于经典逻辑系统。例如直觉主义逻辑、相干逻辑、多值逻辑、模糊逻辑、量子逻辑、偏逻辑、自由逻辑、次协调逻辑等。

4 介绍数理逻辑的应用前沿

通常本科生学习的数理逻辑的教材，理论讲解多，应用实例少。对数理逻辑应用领域的最新发展几乎没有涉及。因此，教学中有必要介绍数理逻辑的应用领域的有关前沿课题，激发学生追求新知识的愿望。

（1）介绍基于逻辑的软件技术[3]。最初，应用逻辑分析程序的目标是证明现有程序的性质。不久后，情况发生变化：目标变为写出正确的程序。基于逻辑的软件开发技术就是为上述目标服务的。该技术遵循自顶向下的开发策略。现在已经开发出具有程序规范和验证功能系统。例如 ESC/Java 是一个编程工具。能在编译时找到 Java 程序的错误。该系统运用程序验证的技术。再如 PVS 是一个验证系统。规范语言是由支撑工具和定理证明器集成的。

（2）介绍基于知识的系统[3]。它发端于人工智能领域中的自动问题求解。基于知识的系统由知识库和推理引擎两部分组成。传统的编程系统，知识的描述隐藏在代码中，故难于验证和维护。基于知识的系统将知识用描述的形式存于知识库。知识库的内容由推理引擎来解释。

基于知识的系统开发也需要借助于逻辑。例如描述逻辑就是开发者用来描述知识的。

（3）介绍一个大的研究项目。JTP 是一个人造的推理系统，基于 PROLOG 开发。在抽象的最高层，JTP 的架构与表示的语言无关。实现系统使用了一阶逻辑表示语言。JTP 组合了通用推理器和专用推理器。后者嵌入了知识和任务专家。

介绍应用前沿要适合于信息安全专业的教学需要，主要目的是让学生了解新技术及其应用前景，提高学生学习的热情和兴趣，激发自主学习动力。

5 应用 COQ 辅助数理逻辑教学

COQ 是一个定理证明辅助工具[4]。它不仅可以描述规范，而且还可以开发符合规范要求的程序。

COQ 开发以交互的方式进行，充分利用自动搜索工具。COQ 可以开发需要绝对可信的程序，例如电信、运输、能源和银行等领域，这些部门要求程序严格符合规范，对这些程序也要求形式化验证。

COQ 可以用来开发新逻辑系统。人们应用它为模态逻辑、时序逻辑等逻辑系统开发出新的推理系统。

在实际教学中，常用的工具是使用 COQ 开发的 ProofWeb 系统[5]。该系统基于 Web 应用程序的架构，学生学习情况保留在 Web 服务器上。学生本人， 老师和系统可以随时了解学生学习进展。数理逻辑是大学信息安全专业本科以及研究生阶段的基础课程。它的两个最基本，也是最重要的组成部分是“命题演算”和“谓词演算”。在学生自主学习过程中，常常出现一些学生不能判断的近乎正确但并不是完全正确的证明。这是需要教师及时引导他们发现完全正确的证明。然而学生与教师并不一定有见面的机会。这时 ProofWeb 系统可以充当教师的角色，完成引导学生得到正确证明的任务。ProofWeb 系统的使用方法可以访问该系统的官方网站。

信息安全专业的学生了解 COQ 系统的基本理论和应用，为他们后续课程学习准备有力工具。也为将来工作和研究打下良好的基础。

6 结论

本文对数理逻辑教学提出了一些教学建议。着力于增强学生学习兴趣，提高学生自主学习能力，培养研究型学习习惯。目的是让学生形成系统的数理逻辑知识体系，了解基本形式化思想和方法。为今后研究和应用打下良好的基础。

References (参考文献)

[1] QU Wanling GENG Suyun ZHANG Liang. Discrete mathematics[M]. Beijing: Higher Education Press, 2008.
屈婉玲,耿素云,张立昂, 离散数学[M].北京高等教育出版社,2008.

[2] ZHU Hong. Introduction of Discrete mathematics [M].Shanghai: Shanghai Scientific and Technological Publishing House,1996.
朱洪.离散数学教程[M]. 上海:上海科学技术文献出版社, 1996.

[3] M.Ferenczi,A.Pataricza,L.Ronyai.Formal Methods in Computing[M].
Budapest:Akademiai Kiado,2005.

[4] Y.Bertot，P.Casteran. Interactive Theorem Proving and Program Development[M], Spring-Verlag,2009.

[5] Cezary Kaliszyk，Freek Wiedijk.Teaching logic using a state- of-the-art proof assistant[J].Proceedings of PATE'07, H. Geuvers and P. Courtieu editors. Elsevier, 2007.