数理逻辑与近世代数

课程QQ群：556727660

课程内容

主要内容：

◆数理逻辑(28学时)
——命题逻辑
——一阶逻辑

◆近世代数(28学时)
——群、环与域
——格与布尔代数

课程教材

主讲教材:

1. 离散数学及其应用(第2版), 屈婉玲、耿素云、张立昂. 高等教育出版社, 2018.
2. 离散数学引论(第3版), 王义和. 哈尔滨工业大学出版社, 2007.

主要参考教材:

3. 面向计算机科学的数理逻辑—系统建模与推理, Michael Huth & Mark Ryan. 机械工业出版社, 2007.
4. 离散数学及其应用(第7版), Kenneth H. Rosen. 机械工业出版社, 2017.

课程考核

考核：考试成绩80%+平时成绩20%

- **考试成绩**
  - 笔试
  - 闭卷
- **平时成绩**
  - 考勤
  - 作业

第一部分 数理逻辑

引言

逻辑是探究、阐述和确立有效推理原则的学科，最早由古希腊学者亚里士多德(Aristotle，公元前384～前322)创立。

逻辑(logic)一词源于希腊文logoc，有“思维”和“表达思考的言辞”之意。

研究人的思维形式和规律的科学，称为逻辑学。

第一部分 数理逻辑

引言

数理逻辑是用数学方法研究关于推理、证明等问题的学科。

数理逻辑是用数学方法研究推理过程的规律，特别是研究数学证明的科学。

这里所说的数学方法就是引进一整套形式符号系统。所谓推理就是由一个或几个判断推出一个新判断的思维形式。

因为引进了符号系统，所以数理逻辑也称为符号逻辑。

第一部分 数理逻辑

引言

数理逻辑是用数学方法研究推理规律的科学，它采用符号的方法来描述和处理思维形式、思维过程和思维规律。

进一步说，数理逻辑就是研究推理中前提和结论之间的形式关系，这种形式关系是由作为前提和结论的命题的逻辑形式决定的。

第一部分 数理逻辑

数理逻辑的起源和发展

数理逻辑产生前已经有很多数学分支：几何学、数值分析、自然数理论…

这些数学分支只是使用推理，并没有研究它们所共同使用的推理是怎么回事。

莱布尼茨(G.W. Leibnitz，1646-1716)梦想：我将作出一种通用代数, 在其中一切推理的正确性将化归于计算。

第一部分 数理逻辑

数理逻辑的起源和发展

这种思想最早是由德国近代哲学家、数学家、逻辑学家莱布尼兹于1700年在柏林科学院提出的。

问题1：建立一种普遍适用的精确的科学语言

问题2：建立一种推理的演算

莱布尼兹提出的两个问题就是现代数理逻辑思想的来源。

【因此，一般认为莱布尼兹是数理逻辑的创始人】

真正的实现：1879年，标志着数理逻辑成为一个独立的数学分支。

第一部分 数理逻辑

数理逻辑的起源和发展

最早提出用数学方法来描述和处理逻辑问题的是德国数学家莱布尼兹。

1847年，英国数学家布尔(George Boole，1815 - 1864)发表了《逻辑的数学分析》，他用通常的代数符号并以等式来表示逻辑关系。

1854年，他又出版了《思维规律的研究》，介绍现在以他名字命名的“布尔代数”。

布尔建立了一系列的运算法则，利用代数或数学的方法研究逻辑问题，初步奠定了数理逻辑的基础。

第一部分 数理逻辑

数理逻辑的起源和发展

1879年，德国数学家弗雷格(G. Frege，1848 -1925)在《表意符号》一书中建立了第一个比较严格的逻辑演算系统。

英国逻辑学家怀特海(A. N. Whitehead,1861-1947)和罗素(B. Russell，1872 - 1970)合著的《数学原理》一书，对当时数理逻辑的成果进行了总结，使得数理逻辑形成了专门的学科。

【1910-1913年出版的关于哲学、数学和数理逻辑的三大卷巨著】

第一部分 数理逻辑

数理逻辑的研究对象

与传统逻辑在研究对象上没有实质性的区别，都是以逻辑推理本身作为研究的对象。

区别在于研究的工具语言不同：

传统逻辑仍然以自然语言作为主要工具语言；

数理逻辑则是用数学符号语言，即借助于数学的形式化、符号化、公理化方法。

数理逻辑的研究对象

简单的说数理逻辑研究推理：

premises （前提）

↓ reason （推理）

conclusions（结论）

数理逻辑是用数学的方法研究推理，特别是研究数学中的推理。

第一部分 数理逻辑

数理逻辑的研究对象

逻辑学研究“什么是正确的推理”。

正确的推理：保证从正确的前提能得到正确的结论的推理。不一定能保证结论正确。

正确的前提：前提为真

正确的结论：结论为真

备注：前面还说过“有效推理”一词。

第一部分 数理逻辑

数理逻辑的研究对象

例1 举例说明正确的推理：

所有3的倍数的数字之和是3的倍数。 （前提）

10^{10}的数字之和不是3的倍数。 （前提）

10^{10}不是3的倍数。 （结论）

推理正确，且所有命题都为真命题。

第一部分 数理逻辑

数理逻辑的研究对象

例2 举例说明正确的推理：

所有中学生打网球。（前提）
王军不打网球。（前提）
王军不是中学生。（结论）

推理正确，不是所有命题都为真命题。

第一部分 数理逻辑

数理逻辑的研究对象

正确的推理

因此，推理是否正确与前提和结论中命题是否为真命题没有关系。

推理的正确性与什么有关?

第一部分 数理逻辑

数理逻辑的研究对象

正确的推理

例3

S中所有元素有***R***性质。（前提）

a没有***R***性质。（前提）

a不是***S***中的元素。（结论）

推理的正确性与命题的逻辑形式有关。

数理逻辑的研究方法

通常用自然语言陈述命题，自然语言陈述命题会带来不方便。

例4

X认识Y。　　　　（前提）
Y 是足球队长。　　（前提）
X认识足球队长。（结论）

推理正确

第一部分 数理逻辑

数理逻辑的研究方法

通常用自然语言陈述命题，自然语言陈述命题会带来不方便。

例5

X认识A班某同学。（前提）

A班某同学是足球队长。（前提）

X认识足球队长。（结论）

推理不正确

第一部分 数理逻辑

数理逻辑的研究方法

数学方法：引进一整套形式符号系统。

用符号构成的公式来代替自然语言中的命题；
符号构成的公式能精确的表示命题的逻辑形式。

第一部分 数理逻辑

数理逻辑的研究语言

使用两种语言：对象语言、元语言

对象语言：被研究对象的语言称为对象语言。
如我们通常所说的英语学习中的英语就是对象语言。

元语言：用以研究研究对象的语言称为元语言。
如用以研究英语语言的汉语。

第一部分 数理逻辑

数理逻辑的应用

现代数理逻辑除了继续研究数学基础课题外，还扩展到了现代科学技术当中，特别是计算机科学当中。在程序语言、自动机理论、系统测试、机器证明等方面都有不可或缺的应用。

推荐:

数学之美(第2版), 吴军. 人民邮电出版社, 2014.

第一部分 数理逻辑

在计算机科学中的逻辑是为了创建一种语言，使人们能够对计算机科学领域中遇到的情境进行建模，并在这种方式下，对情境进行形式化推理。对情境进行推理意味着构造与其相关的论证，人们希望这个过程形式化，使这些论证经得起严格的推敲，或者能够在计算机上实现。

——《面向计算机科学的数理逻辑》

Logic in Computer Science

第一部分 数理逻辑

相关成果：布尔函数敏感度猜想

1992年，布尔函数敏感度猜想(Boolean Sensitivity)被提出，成为理论计算机科学近三十年来最重要、最令人困惑的开放性问题之一。

2019年，Emory大学华人教授黄皓用7年时间破解。

第一部分 数理逻辑

值得关注：“推理+学习”的难题

在人工智能领域有一个长期存在的“圣杯”问题：什么时候能够把机器学习和逻辑推理很好的融合起来？

——2020年8月7日全球人工智能和机器人峰会

周志华教授《反绎学习》大会报告

第一部分 数理逻辑

广义的数理逻辑：

包括逻辑演算、集合论、模型论、递归论、证明论等部分。

狭义的数理逻辑：

仅指逻辑演算，即命题逻辑演算和一阶(谓词)逻辑演算，这些内容构成数理逻辑其它分支的共同基础。

数理逻辑部分课程内容

主要内容:

命题逻辑

- 命题逻辑基本概念
- 命题逻辑等值演算
- 命题逻辑推理理论

一阶逻辑

- 一阶逻辑基本概念
- 一阶逻辑等值演算与推理

预备知识

主要包括:

- 集合及其运算

  ——交/并/对称差/笛卡尔积等运算及性质

- 映射（或函数）

  ——映射（或函数）

- 关系

  ——关系的定义及性质

- 归纳定义或递归定义

1、集合及其基本运算

集合A与B 的并运算：$A \cup B = \{x \mid x \in A$或者$x \in B\}$

定理1 设A，B，C为任意的三个集合，则

1° 交换律成立，即$A \cup B = B \cup A$;

2° 结合律成立，即$(A \cup B) \cup C = A \cup (B \cup C)$;

3° 幂等律成立，即$A \cup A = A$;

4° 同一律成立，即$\varnothing \cup A = A$;

5° $A \cup B = B \Leftrightarrow A \subseteq B$。

集合及其基本运算

集合A与B 的交运算： $A\cap B=\{x\mid x\in A且x\in B\}$

定理2 设A，B，C为任意的三个集合 ，则

1° 交换律成立，即$A\cap B=B\cap A$;

2° 结合律成立，即$(A\cap B)\cap C=A\cap(B\cap C)$;

3° 幂等律成立，即$A\cap A=A$;

4° 零律成立，即$\varnothing\cap A=\varnothing$;

5° $A\cap B=A\Leftrightarrow A\subseteq B$。

集合及其基本运算

定理3 设A，B，C为任意三个集合，则

1° 交运算对并运算满足分配律，即

$$A\cap(B\cup C) = (A\cap B)\cup(A\cap C);$$

2° 并运算对交运算满足分配律，即

$$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)。$$

定理4 对任何集合A，B，$\cap$和$\cup$吸收律成立，即

3° $A\cap(A\cup B)=A$;

4° $A\cup(A\cap B)=A$。

集合及其基本运算

集合A与B 的差运算：$A \backslash B = A - B = \{x \mid x \in A$且$x \notin B\}$

集合A与B 的对称差运算：

$$A \oplus B = A \Delta B = (A \backslash B) \cup (B \backslash A) = (A \cup B) - (A \cap B)$$

定理5 设A，B，C为任意三个集合，则

1° 结合律成立，即$(A \Delta B) \Delta C = A \Delta (B \Delta C)$；

2° $A \Delta \varnothing = A$;

3° $A \Delta A = \varnothing$;

4° 交换律成立，即$A \Delta B = B \Delta A$;

5° 交运算关于对称差满足分配律，即

$$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)。$$

集合及其基本运算

集合A与B的**笛卡尔(乘)积**：

$$A \times B = \{(a, b) \mid \forall a \in A \text{且} \forall b \in B\}$$

例：设$A = \{1, 2, 3\}$，$B = \{1, 2\}$，则

$A \times B = \{(1,1),(1,2),(2,1),(2,2),(3,1),(3,2)\}$

性质 对任意有穷集合A，B，如果用$|A|$，$|B|$分别表示A和B中元素的个数，则$|A \times B| = |A| \times |B|$。

2、映射：映射的定义

设X和Y是两个非空集合，一个从X到Y的映射f是一个法则，根据f，对X中每个元素x都有Y中唯一确定的元素y与之对应。

设X和Y是两个非空集合，一个从X到Y的映射是一个满足以下两个条件的$X\times Y$的子集f:

(1)对X的每一个元素x，存在一个$y\in Y$，使得$(x, y)\in f$;

(2)若(x, y)、$(x, y')\in f$，则$y=y'$。

在这个定义中，性质(2)称为“单值性”。

f是X到Y的映射常记为f：$X\to Y$。

映射：几个重要的结论

从X到Y的所有映射之集记为Y^X，即$Y^X=\{f\mid f:X\to Y\}$。

性质1 设X，Y均为有穷集合，$|X|=n$，$|Y|=m$，且$n\geq 1$，$m\geq 1$，则$|Y^X|=m^n$。

性质2 设X为有穷集合，$|X|=n$，且$n\geq 1$，则从X到X共有$n!$个双射。

3、关系的定义

定义1 设A, B为集合，A与B的笛卡儿积记作$A\times B$，且

$$A\times B = \{(x, y) \mid x\in A 且 y\in B\}。$$

定义2 设A, B为集合, $A\times B$的任一子集R称为从A到B的一个二元关系。

如果$A=B$，则称R为A上的一个二元关系。

计数: $|A|=n$, $|A\times A|=n^2$, $A\times A$的子集有2^{n^2}个。

所以A上有2^{n^2}个不同的二元关系。

例如： $|A| = 3$, 则A上有512个不同的二元关系。

关系的性质

定义3 设 R 为A上的关系,

(1) 若$\forall x\in A$都有$(x, x)\in R$, 则称 R 为 A 上的自反关系。

(2) 若$\forall x\in A$都有$(x, x)\notin R$, 则称 R 为 A 上的反自反关系。

(3) 若$\forall x, y\in A$, 只要$(x, y)\in R$, 就有$(y, x)\in R$, 则称 R为 A上的对称关系。

(4) 若$\forall x, y\in A$, 只要$(x, y)\in R$且$(y, x)\in R$, 就有$x=y$, 则称 R 为A上的反对称关系。

(5) 若$\forall x, y, z\in A$, 只要$(x, y)\in R$且$(y, z)\in R$, 就有$(x, z)\in R$， 则称 R 是A上的传递关系。

关系性质成立的充要条件(判别)

定理1 设R为A上的关系, 则

(1) R 在A上自反当且仅当 $I_A \subseteq R$。

(2) R 在A上反自反当且仅当 $R \cap I_A = \varnothing$。

(3) R 在A上对称当且仅当 $R=R^{-1}$。

(4) R 在A上反对称当且仅当 $R \cap R^{-1} \subseteq I_A$。

(5) R 在A上传递当且仅当 $R \circ R \subseteq R$。

4、归纳定义

用自身定义自身称作递归定义或归纳定义。

归纳定义：

1）基础条款：规定某些元素为待定义集合成员，集合其它元素可以从基本元素出发逐步确定；

2）归纳条款：规定由已确定的集合元素去进一步确定其它元素的规则；

3）终极条款：规定待定义集合只含有基础条款和归纳条款所确定的成员。

基础条款和归纳条款称作“完备性条款”，必须保证毫无遗漏产生集合中所有成员；
终极条款又称“纯粹性条款”，保证集合中仅包含满足完备性条款的那些对象。

归纳定义

用自身定义自身称作递归定义或归纳定义。

例如：集合A的递归定义如下：

（1）$3 \in A$；

（2）若x，$y \in A$，则$x + y \in A$；

（3）只有有限次使用（1）和（2）得到的数属于A。

不难得出：A是3的所有正整数倍组成的集合，即

$$A = \{3n \mid n \in Z^+\}$$

问题

问题1：考虑下面的推理：

只要A曾到过受害者房间并且11点前没离开，A就是嫌疑犯。

A曾到过受害者房间。

如果A在11点前离开，看门人会看见他。

看门人没有见到他。

所以，A是嫌疑犯。

问题2(苏格拉底三段论):

凡是人都会死的。

苏格拉底是人。

所以，苏格拉底也会死的。

问题1

只要A曾到过受害者房间并且11点前没离开，A就是嫌疑犯。

A曾到过受害者房间。

如果A在11点前离开，看门人会看见他。

看门人没有见到他。

所以，A是嫌疑犯。

该推理是否正确？（何谓推理正确？）

如何形式化（符号化）证明该推理正确？

1) 命题符号化;

2) 形式化证明该推理正确。

问题1

设 p: A到过受害者房间，q: A在11点前离开，
r: A是嫌疑犯，s: 看门人看见A，

则有

前提：$(p\wedge\neg q)\rightarrow r$, p, $q\rightarrow s$, $\neg s$

结论：r

证明

① $q\rightarrow s$	前提引入
② $\neg s$	前提引入
③ $\neg q$	①②拒取式
④ p	前提引入
⑤ $p\wedge\neg q$	③④合取引入
⑥ $(p\wedge\neg q)\rightarrow r$	前提引入
⑦ r	⑤⑥假言推理