第五章 数学系统

沈榆平
yuping.shen.ilc@gmail.com

中山大学逻辑与认知研究所
2013年11月

数学系统

引论

系统L与K是逻辑演绎的形式系统，但不足于刻画常见的数学理论。简单而言，K是一个"最小的"描述命题与量词的形式系统，而描述数学需要对K增加公理以表示一些数学性质。

等词

- 等词"="是最基本的数学关系之一。但在K中无法得到表示。
- 例如，令谓词符A_1^2解释成为"="，我们无法在K系统得到定理$(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2) \to A_1^2(x_2, x_1))$。而它表示性质$x_1 = x_2 \to x_2 = x_1$。
- 如果希望上述公式成为某个一阶算术系统的定理，则需要对K增加新的描述等词的公理。

带等词的一阶系统

等词

我们来扩充K成为一个带等词的一阶系统，虽然$\mathscr{L}$的符号中没有=号，我们可以假定A_1^2固定地解释成为等词"="关系。现考虑如何增加**合适的**公理以准确地刻画"="关系。

等词公理

- $(E7)\ A_1^2(x_1, x_1)$
- $(E8)\ A_1^2(t_k, u) \to A_1^2(f_i^n(t_1, \ldots, t_k, \ldots, t_n), f_i^n(t_1, \ldots, u, \ldots, t_n))$，其中$t_1, \ldots, t_n, t_k, u$是项，$f_i^n$是$\mathscr{L}$的函数符号。
- $(E9) A_1^2(t_k, u) \to (A_i^n(t_1, \ldots, t_k, \ldots, t_n) \to A_i^n(t_1, \ldots, u, \ldots, t_n))$，其中$t_1, \ldots, t_n, t_k, u$是项，$A_i^n$是$\mathscr{L}$的函数符号。

带等词的一阶系统

等词公理的含义

- $(E7)$表示任何对象与自己相等。
- $(E8)$表示项中相同的项可以互相替换，得到的项仍相等。
- $(E9)$表示关系中相同的项替换后，关系仍成立。

注记

- $(E8)$与$(E9)$是公理模式，可能代表无数条公理。公理的数目取决于语言中函数符号，谓词符号以及常元，变元符号的个数。
- 注意，语言中只要有一个函数符号f_1^1，就有无穷个$(E8)$,$(E9)$的实例。因为可以有无穷多个项：$f_1^1(x_1), f_1^1(f_1^1(x_1)), \ldots$ 若语言中没有函数符号，实例的个数取决于其它符号的个数，可能是有穷的。

带等词的一阶系统

注记

- 注意所有公理都含自由变元。可以等价地换成它们的全称封闭，因为在K中有$\mathscr{A} \vdash_K \mathscr{A}'$及$\mathscr{A}' \vdash_K \mathscr{A}$。
- 由于数学性质的声明中(数学定理)，前提都是"封闭"的，所以使用含自由变元的公理及演绎定理不会产生问题。
- 注意$(E7)$并不是公理模式。它是一个单独的公理，其中出现的变元x_1可以通过以下证明替换成其它变元：

(1)	$A_1^2(x_1, x_1)$	$(E7)$
(2)	$(\forall x_1)A_1^2(x_1, x_1)$	$(1), Gen$
(3)	$(\forall x_5)A_1^2(x_5, x_5)$	(2), 命题4.18
(4)	$(\forall x_5)A_1^2(x_5, x_5) \to A_1^2(x_5, x_5)$	$(K5)$
(5)	$A_1^2(x_5, x_5)$	$(3), (4) MP$

带等词的一阶系统

定义5.3

公理(E7),(E8),(E9)被称为**等词公理**。任何包含这些公理及其实例的K的扩展都称为一个**带等词的一阶系统**。

我们知道，等词是一个自反，对称及传递的关系，令S是一下带等词的一阶系统，这些性质由以下几条S的定理给出:

1. $(\forall x_1)A_1^2(x_1, x_1)$
2. $(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2) \rightarrow A_1^2(x_2, x_1))$
3. $(\forall x_1)(\forall x_2)(\forall x_3)(A_1^2(x_1, x_2) \rightarrow (A_1^2(x_2, x_3) \rightarrow A_1^2(x_1, x_3)))$

下面给出它们在S中的证明。

带等词的一阶系统

第一个定理直接从(E7)使用概括原则即可，第二个定理证明如下：

$$
\begin{array}{lcr}
(1) & A_1^2(x_1,x_2)\to(A_1^2(x_1,x_1)\to A_1^2(x_2,x_1)) & (E9) \\
(2) & (A_1^2(x_1,x_2)\to(A_1^2(x_1,x_1)\to A_1^2(x_2,x_1)))\to & \\
 & ((A_1^2(x_1,x_2)\to A_1^2(x_1,x_1))\to(A_1^2(x_1,x_2)\to A_1^2(x_2,x_1))) & (K2) \\
(3) & (A_1^2(x_1,x_2)\to A_1^2(x_1,x_1))\to(A_1^2(x_1,x_2)\to A_1^2(x_2,x_1)) & (1)(2)M \\
(4) & A_1^2(x_1,x_1)\to(A_1^2(x_1,x_2)\to A_1^2(x_1,x_1)) & (K1) \\
(5) & A_1^2(x_1,x_1) & (E7) \\
(6) & A_1^2(x_1,x_2)\to A_1^2(x_1,x_1) & (4)(5)M \\
(7) & A_1^2(x_1,x_2)\to A_1^2(x_2,x_1) & (3)(6)M \\
(8) & (\forall x_1)(\forall x_2)(A_1^2(x_1,x_2)\to A_1^2(x_2,x_1)) & (7)Ge
\end{array}
$$

带等词的一阶系统

第三个定理证明如下：

$$
\begin{array}{lll}
(1) & A_1^2(x_2,x_1) \to (A_1^2(x_2,x_3) \to A_1^2(x_1,x_3)) & (E9 \\
(2) & A_1^2(x_1,x_2) \to A_1^2(x_2,x_1) & \text{已证} \\
(3) & A_1^2(x_1,x_2) \to (A_1^2(x_2,x_3) \to A_1^2(x_1,x_3)) & (1)(2) \\
(4) & (\forall x_1)(\forall x_2)(\forall x_3)(A_1^2(x_1,x_2) \to (A_1^2(x_2,x_3) \to A_1^2(x_1,x_3))) & Ger
\end{array}
$$

事实上，等价关系并不仅仅是等词"="。因此，等词公理还可以用来表示其它等价关系。

其它等价关系:同余关系

定义关系$R_{mod2} = \{\langle a,b\rangle \in \mathbb{Z} \times \mathbb{Z} | a与b除于2有相同的余数\}$，通常把$aR_{mod2}b$记为$a \equiv b(mod2)$。不难看出，同余关系是一个自反，对称，传递，也即是等价关系。

带等词的一阶系统

命题5.6

如果S是一个一致的带等词的一阶系统，那么S有一个将A_1^2解释为"="的模型。

证明

如果S是一个一致的一阶系统，那么S有一个模型M，其域为D_M。在M中所有S的定理为真。系统中$\bar{A}_1^2$解释成为D_M上的一个等价关系(不一定是=)。现在我们构造一个新的模型M^*，使A_1^2解释成等词$=$。令与x有$\bar{A}_1^2$关系的所有元素为$[x]$ (x在$\bar{A}_1^2$上的等价类) 令M^*的域为$\{[x]|x \in D_M\}$，任何常元符号a_i解释为$[\bar{a}_i]$,函数符号f_i^n解释成为$\hat{f}_i^n$，其中对$y_1, \ldots, y_n \in D_M, \hat{f}_i^n([y_1], \ldots, [y_n]) = [\bar{f}_i^n(y_1, \ldots, y_n)]$，谓词符号$A_i^n$解释成为$\hat{A}_i^n$, $\hat{A}_i^n([y_1], \ldots, [y_n])$成立当且仅当$\bar{A}_i^n(y_1, \ldots, y_n)$成立，其中$\bar{a}_i, \bar{f}_i^n, \bar{A}_i^n$均为相应符号在$M$中的解释。可以证明$M^*$是$S$的一个模型.

带等词的一阶系统

证明

比如，令f为一个一元函数符，$\bar{f}$为其在M中的解释(真实的一元函数)，设$a, b \in D_M$且$[a] = [b]$。我们来证明$[\bar{f}(a)] = [\bar{f}(b)]$。因(E8)及$M$是一个模型，$A_1^2(x_1, x_2) \to A_1^2(f(x_1), f(x_2))$在M中为真。因此在实际的解释中$\bar{A}_1^2(a, b)$蕴含$\bar{A}_1^2(f(a), f(b))$，即$[a] = [b]$蕴含$[\bar{f}(a)] = [\bar{f}(b)]$。同样，$A_1^2$在$M^*$中被解释成为$=$，因为$\hat{A}_1^2([x], [y])$成立当且仅当$\mathscr{A}_1^2(x, y)$成立，当且仅当$[x] = [y]$。(看书上例子)

定义

令S为一个带等词的一阶系统。一个S的标准模型把A_1^2解释成为$=$。

为方便，我们将在以后把A_1^2在$\mathscr{L}$中替换成$=$。

群论

群论是最普通的数学分支之一,它可以被很好地公理化. 在K之上增加了等词公理(E7),(E8),(E9)后,再添加以下公理得到描述群论的系统$\mathscr{G}$:

群公理

- (G1) $f_1^2(f_1^2(x_1,x_2),x_3)=f_1^2(x_1,f_1^2(x_2,x_3))$ (结合律)
- (G2) $f_1^2(a_1,x_1)=x_1$ (左单位元运算)
- (G3) $f_1^2(f_1^1(x_1),x_1)=a_1$ (左逆元运算)

其中,f_1^1通常被解释为逆运算,f_1^2解释为积运算,a_1解释成单位元.

群论

群论实质上是代数的一种形式,我们不打算深入介绍,只在此给出例子:

群论

令单位元为1,积运算为乘法,逆运算为倒数(x^{-1}),论域为正整数根据群公理有:

- $(x_1 * x_2) * x_3 = (x_1 * (x_2 * x_3))$
- $1 * x_1 = x_1$
- $x_1^{-1} * x_1 = 1$

还可以设定单位元为单位矩阵,逆运算为矩阵的转置,积运算为矩阵乘法等等,从而得到关于线性代数的系统.

群论

讨论

群论形式化的一个比较重要的意义在于,群理论中的证明都可转化成形式系统$\mathscr{G}$的证明. 也就是说, $\mathscr{G}$是完全的(当然也是可靠的) . 形式化的思想在群论上得到比较好的应用,我们可以充分地澄清这部分数学的本质. 但是, 是否其它常见的数学理论都可以被完美地形式化呢? 答案是否定的. 著名的哥德尔不完全性定理告诉我们: 对于一个一致的一阶算术系统, 必然存在一些为真的数学命题,在这个系统中不可证明. 我们下面介绍这样的一个系统$\mathscr{N}$.

一阶算术系统$\mathscr{N}$

一阶算术系统$\mathscr{N}$

系统$\mathscr{N}$是在K及(E7-9)的基础上,增加下列公理得到的:

- $(N1)$ $(\forall x_1) \sim (f_1^1(x_1) = a_1)$ (0不是任何数的后继)
- 后继函数: 0的后继是1,1的后继是2,如此类推,但0不是任何数的后继
- $(N2)$ $(\forall x_1)(\forall x_2)(f_1^1(x_1) = f_1^1(x_2) \rightarrow x_1 = x_2)$ (后继相等的数自身也相等)
- $(N3)$ $(\forall x_1)(f_1^2(x_1, a_1) = x_1)$ (任何数加0等于自身)
- $(N4)$ $(\forall x_1)(\forall x_2)(f_1^2(x_1, f_1^1(x_2)) = f_1^1(f_1^2(x_1, x_2)))$
- $(N5)$ $(\forall x_1)(f_2^2(x_1, a_1) = a_1)$ (任何数乘0等于0)
- $(N6)$ $(\forall x_1)(\forall x_2)(f_2^2(x_1, f_1^1(x_2)) = f_1^2(f_2^2(x_1, x_2), x_1))$
- $(N7)$ $\mathscr{A}(a_1) \rightarrow ((\forall x_1)(\mathscr{A}(x_1) \rightarrow \mathscr{A}(f_1^1(x_1))) \rightarrow (\forall x_1)\mathscr{A}(x_1))$对任何$x_1$在其中自由出现的$\mathscr{A}(x_1)$ (归纳原理)

一阶算术系统$\mathscr{N}$

一阶算术系统$\mathscr{N}$

系统$\mathscr{N}$是著名的Peano 公理的(部分)形式化,为方便,我们简单写成

- $(N1)$ $(\forall x_1) \sim (x_1' = 0)$ ($'$为后继函数)
- $(N2)$ $(\forall x_1)(\forall x_2)(x_1' = x_2' \to x_1 = x_2)$
- $(N3)$ $(\forall x_1)(x_1 + 0 = x_1)$
- $(N4)$ $(\forall x_1)(\forall x_2)(x_1 + x_2' = (x_1 + x_2)')$
- $(N5)$ $(\forall x_1)(x_1 \times 0 = 0)$
- $(N6)$ $(\forall x_1)(\forall x_2)(x_1 \times x_2' = x_1 \times x_2 + x_1)$
- $(N7)$ $\mathscr{A}(0) \to ((\forall x_1)(\mathscr{A}(x_1) \to \mathscr{A}(x_1')) \to (\forall x_1)\mathscr{A}(x_1))$ 对任何x_1在其中自由出现的$\mathscr{A}(x_1)$(归纳原理)

一阶算术系统$\mathcal{N}$

一阶算术系统$\mathcal{N}$

经典的Peano算术系统由英语给出,之后被尝试形式化.

1. 零是一个自然数.
2. 对于每一个自然数n,存在另一个自然数n'.
3. 没有自然数的后继为0.
4. 对任何自然数m和n,如果$m' = n'$那么$m = n$.
5. 对任何包含0的自然数集合A,如果$n \in A$那么$n' \in A$的话,则A包含所有自然数.

$\mathcal{N}$不需要关于第1,2的公理,因为它们已经在语言中包括了. 需要指出的是,最后一条归纳原理比$(N7)$要**强**,它本质上是一个二阶逻辑公式. Peano算术没有包括和与积,但它们可以通过后继函数定义出来.

一阶算术系统$\mathscr{N}$

人们通过一些方法可以证明,自然数的算术$\mathbb{N}$是$\mathscr{N}$的一个模型. 也就是说,$\mathscr{N}$所有的定理都是自然数理论中的真命题. 但是,根据我们已掌握的知识,仍有一个非常重要的问题:

一阶算术系统$\mathscr{N}$的完全性

自然数理论中的每一个真的命题都能由$\mathscr{N}$推出么? 答案是否定的. 存在一些为真的自然数理论的命题$\mathscr{A}$(闭公式),既没有$\vdash_{\mathscr{N}} \mathscr{A}$也没有$\vdash_{\mathscr{N}} \sim \mathscr{A}$. 这就是著名的**歌德尔不完全性定理**.

一阶算术系统$\mathscr{N}$

由$\mathscr{N}$的不完全性引出的另外一个重要问题是:

一阶算术系统$\mathscr{N}$的非标准模型

已经知道标准的自然数算术$\mathbb{N}$是$\mathscr{N}$的一个模型. 考虑一个$\mathscr{N}$中不可证的闭公式$\mathscr{A}$($\sim \mathscr{A}$也不可证),显然它代表了一些自然数的性质. 我们知道闭公式在一个解释下要么为真,要么为假. 假设$\mathscr{A}$在自然数下为真,那么$\mathbb{N}$是一个可以解释它的模型. 但由于$\mathscr{A}$不可证,根据我们之前的结论,将$\sim \mathscr{A}$作为公理对$\mathscr{N}$进行扩充也可以得到一个一致的系统, 这个系统也有模型. 因此,将$\mathscr{A}$与$\sim \mathscr{A}$分别当成公理,我们可以得到$\mathscr{N}$的两个扩充,其中一个和自然数理论是相同的, 另一个模型却具有一个完全相反的性质($\sim \mathscr{A}$)! 后者被称为**非标准模型**(与自然数不同), 这一结果促使了一门全新理论的诞生: 非标准分析.

注意: 系统$\mathscr{N}$是否一致尚有争议,它的一致性曾通过了一些其它的方法得到,部分人认为仍值得怀疑.