关于描述计算机科学数学对象的形式系统的无矛盾性问题

侯广坤

(计算机科学系)

摘　要

本文证明了〔2〕中提出的系统是无矛盾的。空的系统中的所有公式都是可推出公式。本文找到了不可推出公式。将系统中的公式与命题代数的公式对应，可推出公式必对应真公式，而$\overline{\Lambda=\Lambda}$对应的是原始假公式，从而得到$\overline{\Lambda=\Lambda}$是不可推出的，因而系统是非空(无矛盾)的。

在文〔2〕中提出了计算机科学数学对象的形式系统的构造，并用S来表示此系统。本文继续文〔2〕的工作，讨论S的无矛盾性问题。

在数理逻辑[3,4]中得知，如果某系统是矛盾的，那末系统中的任何公式都是可推出的。为了证明S的无矛盾性，只要证明S中的公式$\overline{\Lambda=\Lambda}$在$S$中不可推出。

定义1　在字公理算术中，不包含量词的公式称为原始公式。

在原始公式中考察有如下形式的命题和谓词：

$$\tau_1=\tau_2 \qquad \text{或} \qquad \tau_1<\tau_2.$$

若τ_1和τ_2是常量，则它们是具体的基本命题；若τ_1和τ_2是递归项，而且至少有一个包含变量，则它们是具体的基本谓词。基本谓词中的变量用字代替，所得到的是上述形式的基本命题。在文〔2〕中得知，任何递归常项都必有Σ^*中的字与之对应，而且是唯一的。设τ_1和τ_2对应的唯一的Σ^*中的字分别为z_1和z_2。

定义2　如果(1)对于$\tau_1=\tau_2$，τ_1和τ_2所对应的z_1和z_2从Λ开始的λ-函数相同，且作用的次数相同；(2)对于$\tau_1<\tau_2$，在τ_1和τ_2所对应的z_1和z_2是可比较的情况下，且z_1从Λ开始λ-函数的作用次数比z_2的要小，那么上述形式的命题常量称为基本原始真的。否则(包括$\tau_1<\tau_2$时对应的z_1和z_2是不可比较的)，称为基本原始假的。

命题1　如果上述形式的基本命题是基本原始真的，则它在受约字公理算术中为可推出的。

证明　在$\tau_1=\tau_2$为基本原始真时，根据递归项的代入规则得到它在受约算术中的可推出性。若$\tau_2<\tau_1$基本原始真，则它可以由公理Ⅶ出发[2]，通过代入规则而得到。〔证毕〕。

命题2　任意基本命题都是递归的。

证明从略。

命题1和命题2给出了S中的可推出公式同基本命题之间的对应关系，而基本谓词又可以代换成基本命题，但基本命题和基本谓词是十分特殊的原始公式。在原始公式中还有可能包含不同于基本命题的命题变元，和不同于基本谓词的谓词变元。为了将所有的原始公式同命题代数的公式对应，用讨论命题代数公式的真值来阐述原始公式的某些性质，我们作如下的对应变换：谓词演算的公式同命题代数的公式的对应问题，在谓词演算的无矛盾性证明中[3,4]已经解决；在原始公式中的非递归谓词用递归谓词代替，所有的变量用Σ^*中的字代替。经过上述的代换，根据文〔2,3,4〕中的结果，所得到的公式是由形如$\tau_1<\tau_2$，$\tau_1=\tau_2$的基本命题和其它命题代数的公式组成。然后将形如$\tau_1<\tau_2$，$\tau_1=\tau_2$的公式中的原始真式，用T代替；原始假式用F代替；其它公式用任意的方式代入T或F，不过相同的表达式必须以相同的方式代替。这样得到的结果是具有确定真值的命题代数的公式。并且这个过程可在有限步完成。

定义3　设有原始公式，如果(1)它在公理算术中是可推出的，(2)上述代入后所得到的公式的真值为T，则称为原始真公式。如果只有条件(2)，则称为狭义原始真的。

要考虑S中的任意公式，首先必须将它们变换为“标准型”——导出公式：

$$(\forall x_1)\cdots(\forall x_n)[(\mathscr{A}_1 V\cdots V\mathscr{A}_n)\&(\mathscr{B}_1 V\cdots V\mathscr{B}_m)\&\cdots\&(C_1 V\cdots VC_p)] \qquad (\alpha)$$

或

$$(\exists x_1)\cdots(\exists x_n)[\mathscr{A}_{11}\&\cdots\&\mathscr{A}_{1p_1}V\cdots V\mathscr{A}_{k1}\&\cdots\&\mathscr{A}_{kp_k}) \qquad (\beta)$$

很显然，公式(α)与(β)互为对偶。为了建立同原始真式有直接联系的正规公式，引出三个运算及与它对偶的另外三个运算。为简便起见，文中直接使用了外因子、质被加项等概念(可在有关证明论的书中找到[3,4])。

运算1　若在(α)中外因子(例如$\mathscr{A}_1$)的质被加项中的全称量词有如下形式：$(\forall z)\mathscr{A}_1'(z)$，则可以将量词符号提出作为外量词。如果由此量词所约束的变量在其它公式出现过，则将此变量换名。这个运算称为提取全称量词符号。在提取全称量词符号$(\forall z)$后，公式(α)将变成如下形式：

$$(\forall x_1)\cdots(\forall x_n)(\forall z)[(\mathscr{A}_1'(z)V\cdots V\mathscr{A}_n)\&(\mathscr{B}_1 V\cdots V\mathscr{B}_m)\&\cdots].$$

运算1*　提取在公式(β)的存在量词。

运算2*　设公式(α)有如下形式的被加项：$(\exists z)\mathscr{A}_1'(z)$。

此时在$\mathscr{A}_1 V\cdots V\mathscr{A}_n$中补充上被加项$\mathscr{A}_1'(C)$，其中$C$为递归项，但不包含在公式$(\mathscr{A}_1 V\cdots V\mathscr{A}_n)\&\cdots\&(C_1 V\cdots VC_p)$中作为约束变量的那些变量。如果此运算作用于$\mathscr{A}_1$，则公式$(\alpha)$变为如下形式：

$$(\forall x_1)\cdots(\forall x_n)[(\exists z)\mathscr{A}_1' V\mathscr{A}_1'(C)V\mathscr{A}_2 V\cdots V\mathscr{A}_n)\&\cdots].$$

这个运算称为存在量词的分离运算。

运算2*　作用在(β)上的全称量词分离运算。

运算3　这个运算对于公式(α)中的一个被加项是乘积且同时不是原始公式的情况，令它是$\mathscr{A}_{11}\&\mathscr{A}_{12}\&\cdots\&\mathscr{A}_{1r}$。运算将包含在被加项的外因子变为$(\mathscr{A}_{11}V\mathscr{A}_2 V\cdots V\mathscr{A}_n)$

$\& \cdots \& (\mathscr{A}_{1r} V \mathscr{A}_2 V \cdots V \mathscr{A}_n)$，将公式$(\alpha)$变为

$(\forall x_1)\cdots(\forall x_n)[(\mathscr{A}_{11} V \mathscr{A}_2 V \cdots V \mathscr{A}_n) \& \cdots \& (\mathscr{A}_{1r} V \mathscr{A}_2 V \cdots V \mathscr{A}_n) \& (\mathscr{B}_1 V \cdots V \mathscr{B}_m) \& \cdots]$。

这个运算称为分配律运算。

运算3* 对于(β)的分配律运算。

上述六个运算不同于推理规则，运算的目的是将S中的任意公式同命题代数的公式对应。在谓词演算中得知，任意S中的公式都可以等值地变为形如(α)或(β)的导出公式。

定义4 如果某公式是原始真式，或析取的形式，且其中一个成份是原始真的，则称它为基本正规。

定义5 如果形如(α)的公式的每一个外因子是基本正规的，或借助于运算1,2,3，将它变为上述形式的公式，则称它为正规的公式。

狭义基本正规和狭义正规公式的定义同定义4，定义5类似。

上述的六个运算实际上是等值变换。谓词的递归性相对于上述六个运算是封闭的。因此证明S中的一些结论时，只要在受约字公理算术中进行就足够了。

定理1 由正规公式使用字公理算术的推理规则而推出的公式也是正规的。

证明 按各个推理规则证明。

(1) 命题变元和谓词变元的代入规则。只考虑谓词变元的代入规则。

设正规公式$\mathscr{A}$包含只有一个变量的谓词$A(t)$。令公式$\mathscr{N}$是由公式$\mathscr{A}$用公式$\mathscr{B}(t)$代替其中的$A(t)$所得到的公式，需证$\mathscr{N}$是正规的。

首先设$\mathscr{A}$是原始真式，使用分配律运算将$\mathscr{A}$变换为合取范式$\mathscr{A}'$，仍然是原始真的。取$\mathscr{A}'$中的任意因子，而且将因子中包含谓词$A(t)$的被加项分离出来，得到如下的形式

$$A(x_1)V\cdots VA(x_p)V\overline{A}(y_1)V\cdots V\overline{A}(y_q)VL. \tag{1}$$

因$\mathscr{A}'$为原始真，此因子也是原始真的。

现在要证明公式

$$\Sigma(x_i=y_j)VL \tag{2}$$

是原始真，其中Σ表示$1\leqslant i\leqslant p$，$1\leqslant j\leqslant q$时所有可能的数对(i,j)的$(x_i=y_j)$的析取。公式(1)是原始真的，如果在其中所有形如$A(\ \ )$的谓词变元用递归谓词代替仍然得到原始真式。令$s_1,s_2,\cdots,s_p$不包含在(1)中，而且将谓词$A(t)$用如下公式代替

$$\prod_i \overline{(s_i=t)},$$

其中Π表示在$i=1,2,\cdots,p$时的合取。因$\prod\limits_i(s_i=t)$是递归的，因而如下公式是原始真的：

$$\prod_i\overline{(s_i=x_1)}V\prod_i\overline{(s_i=x_2)}V\cdots V\prod_i\overline{(s_i=x_p)}V\overline{\prod_i\overline{(s_i=y_1)}}V\cdots V\overline{\prod_i\overline{(i_i=y_q)}}VL.$$

代入时L不变，因L不包含$A(\ \ )$。再变换得

$$\prod_i\overline{(s_i=x_1)}V\cdots V\prod_i\overline{(s_i=x_p)}V\sum_i(s_i=y_1)V\cdots V\sum_i(s_i=y_q)VL.$$

在上述公式中的s_i用x_i代替，得原始真式：

$$\prod_i \overline{(x_i = x_1)} \vee \cdots \vee \prod_i \overline{(x_i = x_p)} \vee \cdots \vee \sum_i (x_i = y_1) \vee \cdots \vee \sum_i (x_i = y_q) \vee L.$$

在被加项$\prod_i \overline{(x_i = x_j)}(j = 1,2,\cdots p)$中都包含一个原始假因子，经命题代数的等值变换后，得式(2)是原始真的。将(2)式又进行等值变换得如下原始真式：

$$\prod_{i,j} \overline{(x_i = x_j)} \to L.$$

从另一方面，看如下公式

$$A(x_1) \vee \cdots \vee A(x_p) \vee \overline{A}(y_1) \vee \cdots \vee \overline{A}(y_q) \vee \overline{x_i = y_j},\ i = 1,2,\cdots,p,\ j = 1,2,\cdots q.$$

在这个公式中的$A(t)$用公式$\mathscr{B}(t)$代替，得

$$\mathscr{B}(x_1) \vee \cdots \vee \mathscr{B}(x_p) \vee \overline{\mathscr{B}}(y_1) \vee \cdots \vee \overline{\mathscr{B}}(y_q) \vee \overline{x_i = y_j}. \tag{3}$$

在(3)式中有被加项$\mathscr{B}(x_i) \vee \overline{\mathscr{B}}(y_j) \vee \overline{x_i = y_j}$。根据原始真式的定义所作的代入，有

$$\mathscr{B}(z_i) \vee \overline{\mathscr{B}}(z_j) \vee \overline{(z_i = z_j)},$$

其中$z_i, z_j \in \Sigma^*$。若$z_i = z_j$，则$\overline{\mathscr{B}}(z_i) \vee \overline{\mathscr{B}}(z_j)$为$T$，否则$\overline{z_i = z_j}$为$T$。因此此被加项是原始真的。从而得到式(3)是正规的。且如下公式也是正规的：

$$\mathscr{B}(x_1) \vee \cdots \vee \mathscr{B}(x_p) \vee \overline{\mathscr{B}}(y_1) \vee \cdots \vee \overline{\mathscr{B}}(y_q) \vee \prod_{i,j} \overline{(x_i = x_j)}. \tag{4}$$

往证如下公式也是正规的，

$$\mathscr{B}(x_1) \vee \cdots \vee \mathscr{B}(x_p) \vee \overline{\mathscr{B}}(y_1) \vee \cdots \vee \overline{\mathscr{B}}(y_q) \vee L. \tag{5}$$

因式(4)是正规的，根据正规公式的定义，考察使用运算1,2,3,时所构成的公式(4)的正规段

$$R_0, R_1, \cdots, R_m.$$

因为$\prod \overline{(x_i = y_j)}$是原始公式，所以它不需经运算1,2,3,就进入公式R_0的外因子之中，可认为它是原始真式的一部分。将R_0中的任意外因子中的原始真部分表示成$\eta \vee \prod_{i,j} \overline{(x_i = y_j)}$。如果在$R_i$中的所有$\prod_{i,j} \overline{(x_i = y_j)}$表示成$L$，则在$R_0$中的一个外因子的原始真部分表示成$\eta \vee L$。但是，如上所证，公式$\prod_{i,j} \overline{(x_i = y_j)} \to L$是原始真式，当$\prod_{i,j} \overline{(x_i = y_j)}$为$T$时，必然$L$为$T$。那么若$\eta \vee \prod_{i,j} \overline{(x_i = y_j)}$是原始真部分，则不论是$\eta$为真，还是$\prod_{i,j} \overline{(x_i = y_j)}$为真，$\eta \vee L$都为真。所以$\eta \vee L$是原始真式。因而从(4)用$L$代替$\prod_{i,j} \overline{(x_i = y_j)}$仍然得到正规公式。

从另一方面，公式(5)是用公式$\mathscr{B}(t)$代替范式$\mathscr{A}'$中的外因子中的$A(t)$所得到的公式。$\mathscr{A}'$是A的合取范式，所以用公式$\mathscr{B}(t)$代替$\mathscr{A}$中的谓词变元保持公式的正规性。

(2) 自由变量代换规则；约束变量换名规则；量词约束第一和第二规则。它们保持公式的正规性证明较简单，从略。

(3) 推断规则。设$\mathscr{A}$和$\mathscr{A} \to \mathscr{B}$是正规的，往证$\mathscr{B}$也是正规的。将公式$\mathscr{A}$写成$(\alpha)$的形式

$$(\forall x_1) \cdots (\forall x_n)((\mathscr{A}_{11} \vee \cdots \vee \mathscr{A}_{1p}) \& \cdots \& (\mathscr{A}_{m1} \vee \cdots \vee \mathscr{A}_{m,pm})). \tag{6}$$

这个公式是正规的，可以应用运算1,2,3变换成如下形式

$$(\forall x_1)\cdots(\forall x_n)(\forall y_1)\cdots(\forall y_q)((\mathscr{A}_0^{(1)} V \mathscr{D}_0^{(1)})\&\cdots\&(\mathscr{A}_0^{(q)} V \mathscr{D}_0^{(q)})) \quad (7)$$

其中所有的$\mathscr{A}_0^{(i)}$——原始真式。公式$\mathscr{A}\to\mathscr{B}$的导出公式是$\overline{\mathscr{A}}V\mathscr{B}'$而公式$\overline{\mathscr{A}}$写成$(\beta)$的形式

$$(\exists x_1)\cdots(\exists x_n)(\overline{\mathscr{A}}_{11}\&\cdots\&\overline{\mathscr{A}}_{1p_1}V\cdots V\overline{\mathscr{A}}_{m1}\&\cdots\&\overline{\mathscr{A}}_{m,pm}). \quad (8)$$

如果对于(8)式上作用的运算是原作用(6)式运算的对偶运算，则得

$$(\exists x_1)\cdots(\exists x_n)(\overline{\mathscr{A}}_0^{(1)}\&\overline{\mathscr{D}}^{(1)}V\cdots V\overline{\mathscr{A}}_0^{(q)}\&\overline{\mathscr{D}}_0^{(q)}).$$

使用运算1*,2*,3*不推翻正规性，因而得

$$(\exists x_1)\cdots(\exists x_n)(\overline{\mathscr{A}}_0^{(1)}\&\overline{\mathscr{D}}^{(1)}V\cdots V\overline{\mathscr{A}}_0^{(q)}\&\overline{\mathscr{D}}^{(q)})V\mathscr{B}' \quad (9)$$

是正规的。但$\overline{\mathscr{A}}_0^{(i)}$是原始假的(因$\overline{\mathscr{A}}_0^{(i)}$——原始真式)，所以(9)式的最右边是正规的。又$\mathscr{B}'$是$\mathscr{B}$的导出公式，则$\mathscr{B}$是正规的。〔证毕〕

定理2　在S中可推出公式是正规的。

证明　若公式在S中可推出，则它在受约字公理算术中也是可推出。又一般量词约束规则包含了受约量词的约束规则。因此我们只需证明受约字公理算术中可推出公式是正规的。而且可以使用定理1的结果。我们只需证明受约字公理算术中的所有公理是正规的即可。

命题演算是完全的，所以它的公理和导出公式是命题代数的永真公式，它们是原始真公式，是正规的。

谓词演算中的第一个公理的导出公式是

$$(\exists x)\overline{\mathscr{A}}(x)VA(y),$$

对此公式使用运算2时，得

$$\overline{\mathscr{A}}(y)V(\exists x)\overline{\mathscr{A}}(x)VA(y).$$

这个公式是基本正规的，因而公理$(\forall x)A(x)\to A(y)$是正规的公式。

谓词演算第二个公理的正规性类似地证明。

现在看第Ⅵ组公理。显然公理Ⅵ—1　$x=x$是原始真式。对于Ⅵ—2，x和y分别用Σ^*中的字z_1和z_2代替，得$z_1=z_2\to(A(z_1)\to A(z_2))$。若$z_1$和$z_2$是不同的，则表达式$z_1=z_2$是假的，那么上述公式必为真。若$z_1=z_2$，则有

$$z_1=z_1\to(A(z_1)\to A(z_1)).$$

蕴涵式的第二项是命题演算的可推出公式，它是永真的，因此整个公式是命题代数永真公式。Ⅵ-2原始真式。

第Ⅶ组公理的正规性证明，同Ⅵ组相似。

最后，在受约字公理算术中，有如下形式的可推出公式：

$$f_i(x_1,\cdots,x_n,\Lambda)=g(x_1,x_2,\cdots,x_n)$$

$$f_i(x_1,\cdots,x_n,\lambda(y))=h_i(x_1,\cdots,x_n,y,f_i(x_1,\cdots,x_n,y)),$$

其中$f(x_1,\cdots,x_n,y),g(x_1,\cdots,x_n),h_i(x_1,\cdots,x_n,y,z)$—递归项。这些等式的字解释是等式的

两边分别用字代入，两边都得到Σ^*中的相同的字，即由Λ开始的作用的λ-函数相同和作用次数相同。因此，所有这样形式的公式是原始真式。

所有的公理都是正规的，使用定理1得出S中的可推出公式是正规公式。〔证毕〕

定理3 公式$\overline{\Lambda=\Lambda}$在$S$中不可推出的。

证明 用反证法。设$\overline{\Lambda=\Lambda}$是可推出的，则根据定理2，$\overline{\Lambda=\Lambda}$是正规的公式，同时也是狭义正规的公式。但基本命题$\Lambda=\Lambda$应有真值为$T$，故$\overline{\Lambda=\Lambda}$应为$F$。这样$\overline{\Lambda=\Lambda}$不可能是狭义正规的，矛盾。这样$\overline{\Lambda=\Lambda}$不可能在$S$中可推出。〔证毕〕

推论 S是无矛盾的。

根据定理3，$\overline{\Lambda=\Lambda}$是$S$中的不可推出公式。即在$S$中存在着不可推出公式，这样$S$是无矛盾的。

参考文献

(1) 王浩，数理逻辑通俗讲话，科学出版社，1980.

(2) 侯广坤，关于描述计算机科学数学对象的形式系统的构造，中山大学学报(自然科学版)，1982，2.

(3) 侯广坤，数理逻辑基础原理，海洋出版社.

(4) П.С. Новиков, элементы Математической Логики, изд. «Наука» москва, 1974.

(5) Eonar Manna, Mathematical Theory of Computation, 1974.

(6) Мальцев А.И., Алгоритмы и Рекурсивные функции, изд.«Наука» москва, 1965.

(7) Kleen, *Introduction to metamethematics*, 1953.

(8) Luckham D, C., Park. D.M.R., Paterson M.S., On Formalised Computer Programs, *J. Computer aud System Sci.*, (1970), 4, 220—249.

On the Consistency of the Formal System Describing Mathematical Objects of Computer Science

Hou Guangkun

Abstract

The main purpose of this paper is to prove the consistency of S by means of proving that the formula $\overline{\Lambda=\Lambda}$ in S can not be inferred in S. This paper Proves tnat all inferable formulas in S are regular formulas and the rules of inference in S keep formulas regutarly. Suppose that $\overline{\Lambda=\Lambda}$ can be inferred, then it is basie regular, therefore it should be a prmitive true formula. But $\overline{\Lambda=\Lambda}$ is pimitive fault, it leads to a contradietion.