代数等式系有穷公理化的一个扩充定理*

王 驹[1] 赵希顺[2]

[1](中国科学院软件研究所 北京 100080)

[2](南京大学数学系 南京 210008)

摘要 首先介绍两个概念:主同余类的弱可定义性以及次直不可分解类的可定义性.证明了任一有穷代数 A,若 $V(A)$ 具有弱可定义的主同余类以及可定义次直不可分解类,则它的等式系是可以有穷公理化的.进一步的讨论揭示出其结果是新的,是对已有工作的有意义的扩充.

关键词 等式系,主同余类,次直不可分解类.

中图法分类号 TP301

随着近年来计算机理论研究中代数归约的应用及发展,很多原来属于代数理论的问题引起了计算机理论工作者的兴趣.其中之一即是代数的等式系的有穷公理化问题.关于它在代数归约研究中潜在的应用前景,只需指出一点就够了:它将有助于将高阶的代数语言归结为一阶语言.

任给一个有穷代数 A,比如,群、环、域、布尔代数、格、代数归约理论中的 many-sorted algebra 等等.它的等式系 $\Sigma(A)$ 指的是所有形如 $p=q$ 又满足:$A\models p=q$ 的等式全体,这里 p,q 是 A 的语言中的任意项.$\Sigma(A)$ 是可以有穷公理化的,如果存在 $\Sigma(A)$ 的一个有穷子集 Σ_1,$\Sigma_1\subseteq\Sigma(A)$,使对任一 $\Sigma(A)$ 中的公式 $p=q$,我们有 $\Sigma_1\vdash p=q$,$\vdash$ 是关系"可推出"的简写.

代数等式系有穷公理化研究几乎有大半个世纪的历史[1],很难给出一个哪怕是比较完全的综述.在否定性的研究方向(即不可有穷公理化):Lyndon 在 1954 年构造了一个仅含 7 个元素的代数,带 1 个二元运算,1 个一元运算,它的等式系是不可有穷公理化的.以后,Murskii 的三元代数(1965 年);Perkins 的六元半群(1969 年);Polin 的有穷非结合环(1976 年)等,都是这方面熟知的结果.1986 年,Bryant 定义了所谓的有穷 pointed group,也是不可有穷公理化的.Polin 的结果及 finite pointed group 的结果的重要性在于:它们与著名的 Oates-Powell[2]定理形成了十分强烈的对比.后者是说:任一有穷群的等式系都是可以有穷公理化的.这 3 类有穷代数,都归于模族类.以上事实也揭示出有穷公理化问题远比人们想象的复杂得多.

在肯定的方面,主要的工作有:Birkhoff(1941 年)证明:如果 A 有穷,且是有穷型(即只含有穷个函词),又如果只允许有穷个变元,则 A 的等式系可有穷公理化.Mckenzie(1978 年),如果 $V(A)$ 有可定主同余类,有穷型,只含有穷个次直不可分解代数,都是有穷的,则 A 的等式系可有穷公理化.K. Baker(1978 年)[1]证明:若 A 是有穷且有穷型,$V(A)$ 是分配的,则 A 的等式系可有穷公理化.1988 年,Mckenzie 把结果推广到只含有穷个次直不可分解代数的模族上[3].另外,关于具体的代数、二元代数(Lyndon,1951 年)、有限群(Oates-Powell,1965 年)、有限环(Kruse,Lvov,1973 年)等,都是可有穷公理化的.

从整个研究的发展过程来看,Baker 在分配族上的工作及 Oates-Powell 关于群的结果,被认为是主要的进展.一个几十年未解决的问题是:如何将 Baker 定理以及 Oates-Powell 定理统一到一个扩充定理中.但由于 Polin 在 1976 年的结果及 1996 年 pointed group 的给出,人们已几乎相信,这样的一个扩充不存在.

本文的结果即是在上述方向研究中的一个新结果.其意义在于:(1) 它是已知结果的真正扩充.(2) 现在已

* 本文研究得到国家自然科学基金和国家 863 高科技项目基金资助.作者王驹,1950 年生,研究员,主要研究领域为逻辑及计算机科学.赵希顺,1961 年生,在职博士生,副教授,主要研究领域为逻辑及计算机科学.

本文通讯联系人:王驹,北京 100080,中国科学院软件研究所

本文 1997-03-31 收到原稿,1998-03-30 收到修改稿

知的是,它至少分别覆盖以上两个定理的很大部份.

1　主要定理及其证明

在本节里,假定 A 是一个有穷代数,具有穷型. $V(A)$是由 A 生成的代数族,是所有满足 A 的等式系的同类型的代数的全体.

定义 1. 我们说 $V(A)$有弱可定义主同余类,如果在 A 的语言中,存在两个一阶公式 $\Gamma_1(w,v,x,y)$,$\Gamma_2(w,v,x,y)$,使得对所有的 $B\in V(A)$,对所有的 $s,t\in B,s\neq t$,我们总能找到 $a,b\in B,a\neq b$,满足:

(1) $B\models\Gamma_1(w,v,x,y)$,则 $\theta(w,v)\leqslant\theta(x,y)$.

(2) $B\models\Gamma_2(w,v,x,y)$,则 $\theta(w,v)\leqslant\theta(x,y)$.

(3) $B\models\Gamma_1(a,b,s,t)$,亦即 $a\equiv b\pmod{\theta(s,t)}$.

(4) 公式 Γ_2 定义了整个由 a,b 生成的主同余类 $\theta(a,b)$. 亦即对所有的 $c,d\in B$:$c\equiv d\pmod{\theta(a,b)}$当且仅当 $B\ \Gamma_2\models(c,d,a,b)$.

定义 2. (K. Baker) 我们说 $V(A)$有可定义的次直不可分解代数类,如果存在 A 的语言的一个公式 Φ,使得对任一与 A 同型的代数 B,下式成立:

$$B\text{ 是次直不可约的且 }B\in V(A)\text{ 当且仅当 }B\models\Phi.$$

主定理. 如果 A 有弱可定义主同余类且 $V(A)$中的次直不可约代数类是可定义的,则 A 的等式系是可有穷公理化的.

证明:先建立下列的引理.

引理 1. 存在一个一阶公式 Φ_1,它表达性质:$V(A)$" 有弱可定义主同余类 ",即,$V(A)$有弱可定义主同余类当且仅当$\forall\ B\in V(A),B\models\Phi_1$.

引理证明:考虑下面的公式:

$$\forall\ s,t[s\neq t\to\exists\ a,b[a\neq b\wedge\Gamma_1(a,b,s,t)\wedge\{\Gamma_2(a,b,a,b)\wedge\forall\ x\Gamma_2(x,x,a,b)\wedge\forall\ x,y(\Gamma_2(x,y,a,b)\to\Gamma_2(y,x,a,b))\wedge\forall\ x,y,z(\Gamma_2(x,y,a,b)\wedge\Gamma_2(y,z,a,b)\to\Gamma_2(x,z,a,b))\wedge\bigwedge_{f\in\Phi_n}^{\Phi_n\neq\varnothing}\forall\ x_1,y_1,x_2,y_2,\dots,x_n,y_n[\bigwedge_{1\leqslant i\leqslant n}\Gamma_2(x_i,y_i,a,b)\to\Gamma_2(f(\vec{x}),f(\vec{y}),a,b)]\}]].$$

这里,Φ_n 是 A 的语言中 n 元函词的全体. 注意 Φ 是一个有穷集. 显然,以上公式中在{ }内的部分定义了主同余类 $\theta(a,b)$. 将以上公式记为 Ψ_1. 容易验证:任给与 A 同型的代数 B,可以不在 $V(A)$内,如果我们有 $B\models\Psi_1$,则 B 满足定义 1 中的(1)～(4).

引理 2. 在 A 的语言中,存在一个公式 Ψ_2,对所有与 A 同型的代数 B,可以不在 $V(A)$内,有

$$B\models\Psi_2\text{ 当且仅当 }B\models\Psi_1\text{,而且 }B\text{ 是次直不可约的.}$$

证明:考虑下面的公式:

$$\Psi_1\wedge\exists\ c,d,\forall\ s,t[s\neq t\to\exists\ a,b[a\neq b\wedge\Gamma_1(a,b,s,t)\wedge\{\Gamma_2(a,b,a,b)\wedge\forall\ x\Gamma_2(x,x,a,b)\wedge\forall\ x,y(\Gamma_2(x,y,a,b)\to\Gamma_2(y,x,a,b))\wedge\forall\ x,y,z(\Gamma_2(x,y,a,b)\wedge\Gamma_2(y,z,a,b)\to\Gamma_2(x,z,a,b))\wedge\bigwedge_{f\in\Phi_n}^{\Phi_n\neq\varnothing}\forall\ x_1,y_1,x_2,y_2,\dots,x_n,y_n[\bigwedge_{1\leqslant i\leqslant n}\Gamma_2(x_i,y_i,a,b)\to\Gamma_2(f(\vec{x}),f(\vec{y}),a,b)]\wedge\Gamma_2(c,d,a,b)\wedge\forall\ x,y(\Gamma_2(x,y,c,d)\to\Gamma_2(c,d,x,y))\}]],$$

将以上公式记为 Ψ_2.

若 $B\models\Psi_2$,当然我们有 $B\models\Psi_1$,由(1),$\theta(a,b)\leqslant\theta(s,t)$,由(2),$\theta(c,d)\leqslant\theta(a,b)$,从而 $\theta(c,d)\leqslant\theta(s,t)$. s,t 是任意的,所以,$\theta(c,d)$是 $CON(B)$中唯一的最小同余类,所以 B 是次直不可约的.

反过来,若 $B\models\Psi_1$ 同时又是次直不可约的. 令 γ 是 B 的最小的同余类. 任给 $s,t\in B,s\neq t$,则 $\gamma\leqslant\theta(s,t)$. 由 Ψ_1,存在 a,b,使 $\Gamma_1(a,b,s,t)$,而 $\theta(a,b)$是可以用 Γ_2 来定义的. 由于 γ 是最小的,我们有 $\gamma\leqslant\theta(a,b)$. 于是有 c,d,使 $\theta(c,d)=\gamma$,同时,$\Gamma_2(c,d,a,b)$. 所以 Ψ_2 在 B 中成立. □

回到主定理的证明. 由以上两个引理,我们有

$$\Sigma(A)\vdash\Psi_1\wedge(\Psi_2\to\Phi).$$

由紧致性定理,存在 $\Sigma(A)$的一个有穷集 Σ_1,使

$$\Sigma_1 \vdash \Psi_1 \wedge (\Psi_2 \rightarrow \Phi).$$

我们要证:$\Sigma_1 \vdash \Sigma(A)$,即 $\Sigma(A)$可有穷公理化.只需证 $V(\Sigma_1)=V(\Sigma(A))$即可.但我们早有 $V(\Sigma(A))\subseteq V(\Sigma_1)$.此时,只需证 $V(\Sigma_1)$ 中的次直不可约代数都在 $V(A)$中.令 $B\in V(\Sigma_1)$,是次直不可约的,则 $B\models\Sigma_1$.于是 $B\models\Psi_1$,同时我们有 $B\models\Psi_2$(由引理 2).但 $B\models\Psi_2\rightarrow\Phi$,所以,$B\models\Phi$.由定理给出的条件,$B\in V(A)$.所以我们有 $V(\Sigma(A))=V(A)=V(\Sigma_1)$. □

2 讨 论

弄清楚我们的主定理有多大的覆盖面,显然是一个有意义的问题,但不是一个容易的问题.为了揭示它确实是已知结果的扩充,我们考虑两个已知的、著名的有穷公理化定理:Mckenzie 定理及 Oates-Powell 定理.二者是互相独立的.

Mckenzie 定理.如果 A 有穷且是有穷型,$V(A)$仅含有穷个有穷次直不可约代数,同时又有可定义的主同余类,则 $V(A)$的等式系是可有穷公理化的.

Oates-Powell 定理.G 是有限群,则 $V(G)$的等式系可有穷公理化.

Oates-Powell 定理显然不包括 Mckenzie 定理.反过来,$V(G)$中(一般地说)含有无穷个次直不可约群,而只在很少的情况下,$V(G)$有可定义的主同余类,因而 Mckenzie 定理及 Oates-Powell 定理是互相独立的.

命题 1. $V(A)$有可定义的主同余类,则 $V(A)$有弱可定义的主同余类.

证明:显然.

命题 2. $V(A)$含有穷个有穷次直不可约代数,则 $V(A)$有可定义次直不可约类.

证明:由 Quakenbush 的结果(见文献[1]),$V(A)$中没有无穷的次直不可约代数.令 $S_1,S_2,\ldots,S_n$ 是 $V(A)$中次直不可约代数的全体.只要证明任一 S_i 在 A 的语言中是可定义的即可.实际上,任一有穷的代数都是可定义的.令 S 是有穷的.记 $S=\{a_1,a_2,\ldots,a_k\}$,S 的运算是 $f_1,f_2,\ldots,f_m$.定义公式:

$$\Omega \equiv \exists\ x_1,x_2,\ldots,x_m[\Phi \wedge \wedge_{1\leqslant i\leqslant m}\Psi_i].$$

这里,$\Phi \equiv \wedge_{i,j\leqslant k}(x_i\neq x_j)\wedge\forall\ x(\vee_{1\leqslant i,j\leqslant k}x=x_i)$,$\Psi_i \equiv \wedge f(\vec{x})=x_j$,$\vec{x}=\{x_{i_1},x_{i_2},\ldots,x_{i_s}\}$,而且 $f_i(a_{i_1},a_{i_2},\ldots,a_{i_s})=a_j$.注意这里我们默认 x_i 对应于 a_i.

容易验证,对 A 的语言的任一代数 S',S' 当且仅当 $S'\cong S$.

由命题 1,2,主定理是 Mckenzie 定理的扩充.

为了证明主定理是 Mckenzie 定理的真实扩充,只需借助于 Oates-Powell 定理的一个特殊情形即可.

命题 3. G 是有限幂零群,则 $V(G)$有可定义主同余类.(从而有弱可定义主同余类).

证明:见文献[4].

很容易找到一个有限幂零群 G,使 $V(G)$中存在任意大的有限次直不可约群,由 Taylor 的结果[3],$V(G)$中存在任意大的无穷次直不可约群,$V(G)$显然不在 Mckenzie 定理的范围内.但是,我们有:

命题 4. $V(G)$有可定义的次直不可约类.

证明:由 Oates-Powell 定理,$V(G)$可有穷公理化,从而存在有穷个等式 $p_i=q_i$,$1\leqslant i\leqslant n$,使对任一群 F,F,$p_i=q_i$,$1\leqslant i\leqslant n$,$\forall\ i$ 当且仅当 $F\in V(G)$.由命题 3,存在一主同余类公式 $\Gamma(w,v,x,y)$,它定义 $V(G)$中的所有主同余类.考虑下面的公式:

$$\Phi \equiv \wedge_{1\leqslant i\leqslant n}(p_i=q_i)\wedge\exists\ w,v\forall\ x,y\Gamma(w,v,x,y),$$

这里,等式 $p_i=q_i$ 被当作带全称量词的语句.容易验证,Φ 定义了 $V(G)$中的次直不可约类. □

所以主定理是 Mckenzie 定理的真正扩充.

参考文献

1 Burris S, Sankappanavar H P. A Course in Universal Algebra. New York: Spring-Verlag. 1981

2 Oates S, Powell M B. Identical relations in finite groups. Journal of Algebra, 1965,(1):11~39

3 Freese R, Mckenzie R. Commutator Theory for Congruence Modular Varieties. Cambridge: Cambridge University

Press, 1987

4 Burris S Lawrence. Definable principal congruences in varieties of groups and rings. Algebra Universali, 1979,(9):152～164

An Extension Theorem on Finitely Axiomatizable Algebraic Equation Systems

WANG Ju[1]　ZHAO Xi-shun[2]

[1](*Institute of Software. The Chinese Academy of Sciences Beijing* 100080)
[2](*Department of Mathematics Nanjing University Nanjing* 210008)

Abstract First, the two notions: weakly definable principal congruence and definable subdirectly irreducible class are introduced in this paper. The authors prove that if a variety generated by a finite algebra has both weakly definable principal congruence and definable subdirectly irreducible class, its equational system is finitely axiomatizable. Further discussion shows that the results are new, and are significant generalization of the known results.

Key words Equational system, principal congruence, subdirectly irreducible