第17卷第3期 数学研究与评论 Vol. 17 No. 3
1997年8月 JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION Aug. 1997

有限可换主理想环上模理论可判定性及其复杂性*

薛 锐
(山西师范大学计算中心, 临汾041004)

摘 要 本文利用初等等价的工具, 引用 Ehenfeucht Game 理论, 证明了有限可换主理想环上模的理论是可判定的, 并且判定过程的计算复杂性上界为2^{cn^2}.

关键词 n-初等等价, Ehrenfeucht Game, 可判定性, 复杂性
分类号 AMS(1991) 03C, 68Q/CCL O141.3, O141.4

设R是有限可换主理想环, 在语言$\mathbf{L}$中讨论$\mathbf{R}$-模的初等理论, 语言$\mathbf{L}=\{+,\cdot,1=,f_\lambda\}$, 其中$\lambda\in R$, f_λ是一元函数, R-模理论T_R的公理为模的公理

定义1 设$n,k\in N$, A,B是两个结构, 说A,B是n-初等等价的, 如果对任意$\overline{a_k}\in A^k$, $\overline{b_k}\in B^k$, 对任意量词深度$\le n$的公式$F(\overline{x_k})$满足$(A,\overline{a_k})\vDash F(\overline{x_k})\Leftrightarrow(B,\overline{b_k})\vDash F(\overline{x_k})$.

把n-初等等价的两个结构A,B记为: $(A,\overline{a_k})\equiv(B,\overline{b_k})$. 为了研究$R$-模理论, 先观察$R$-模的一些结果, R可分解成素数幂阶的环的直和$R=\bigoplus_p R_p$, p是素数, $R_p=\{x\mid x\in R$, 存在$n\ge 1$使$p^n x=0\}$, 这里R_p的特征$\mathrm{char}(R_p)=p^s$, $s\in N$, 并且R_p也是主理想环. 下面讨论T_{R_p}.

引理1 p是素数, 任意R_p-模是形如$R_p/pR_p, R_p/p^2R_p,\cdots, R_p/p^sR_p$诸子模的直和

证明 设M为R_p-模, $S=\{R_p x\mid x\in M\ \mathrm{ann}(x)=0\}$..

若$S\neq\varnothing$, 令$A=\{\sum_{\text{有限}} R_p x\mid R_p x\in S\}$, Zorn引理保证了$A$中存在关于序$\supseteq$的极大元$F_0=\bigoplus_x R_p x$, 由于$\mathrm{ann}(x)=0$, 所以$R_p x\cong R_p$, 由$R_p$是自内射模, 故知$F_0$也是内射模, 由内射模的性质, 可知存在$M$的子模$M_1$, 使得$M=F_0\oplus M_1$.

若$S=\varnothing$, 则取$F_0=0, M_1=M$.. 现在考虑M_1, $\forall x\in M_1$, 则$\mathrm{ann}(x)\neq 0$, 否则$F_0+R_p x=F_0\oplus R_p x$与$F_0$的极大性矛盾. 于是$p^{s-1}R_p\subseteq\mathrm{ann}(x)$, 故可视$R_p$-模$M_1$为$R_p/p^{s-1}R_p$-模. 同上可取到$F_1$为$R_p/p^{s-1}R_p$的直和, 使$M_1=F_1\oplus M_2$; 如此下去, 最终可得: $M=F_0\oplus F_1\oplus\cdots\oplus F_{s-1}$, 其中$F_i\cong\bigoplus R_p/p^{s-i}R_p$, $i=0,1,\cdots,s-1$.

定理2 设$R=R_{p_1}\oplus R_{p_2}\oplus\cdots\oplus R_{p_t}$, 则任意$R$-模$M$, 可分解为形如$R_{p_i}/p_i^{s_i-j}R_{p_i}$的直和$(1\le i\le t)$, $p^{s_i}=\mathrm{char}(R_{p_i})$, $1\le j\le s_i$.

证明 由引理1可得.

定理3 设R_{p_r}-模M_k是$M=\overset{m}{\oplus}R_l$的子模, 且由M的k个元素生成的子模, 任取$a\in M_k$, 则$p_r x=a$在M_k中至多有p_r^k多个解, 其中$R_l=R_{p_r}/p_r^l R_{p_r}$$(0\le l\le r)$.

* 1994年6月20日收到. 山西省自然科学基金资助.

证明 先证明在$M=\overset{m}{\oplus}R_l$中$p_rx=a$至多有p_r^m多个解 $a=(a_1,a_2,\cdots,a_m)$. 设方程$px_i=a_i$如果有解x_0,则$x_0+p_r^{l-1}R_{p_r}/p_r^lR_{p_r}$中元素都是$p_rx_i=a_i$的解,亦即有$p_r$个解 于是$p_rx=a$在$M$ 中至多有p_r^m多个解 由于$a\in M_k$而M_k由k个元素生成因而$p_rx=a$在M_k中至多有p_r^k多个解

为了证明T_R的可判定性,现利用Ehrenfeucht Game理论进行讨论 Ehrenfeucht Game是对两个结构M,N,有两个players: player Ⅰ和player Ⅱ,他们各走n步,第一步player Ⅰ在M(或N)中选定一个元素a_1,player Ⅱ则在N(或M)中选定一元素b_1;第二步同样先由Ⅰ选定a_2(或b_2),再由Ⅱ选定b_2(或a_2);如此下去,直到第n步,这样就选定了一个序列$\langle a_1,b_1\rangle$,$\langle a_2,b_2\rangle$,$\cdots$,$\langle a_n,b_n\rangle$. 若子结构$\mathrm{Str}\langle a_1,a_2,\cdots,a_n\rangle$及$\mathrm{Str}\langle b_1,b_2,\cdots,b_n\rangle$在对$a_l\leftrightarrow b_l$下为局部同构的,则说player Ⅱ在此Ehrenfeucht Game中有必胜策略 记此Game为$G_n(M,N)$.

定理4 设$M=\overset{m}{\oplus}R_p$任意给定正整数$n\leq m$,记$N=\overset{n}{\oplus}R_p$,则$G_n(M,N)$. 对player Ⅱ有必胜策略

证明 (1) 对于player Ⅰ选定的M中元素a_1,$a_1=(a_{11},a_{12},\cdots,a_{1m})$,知$N$中必有$b_1$,使$b_1$的阶数与$a_1$的阶数相同,player Ⅱ选定$b_1$.

(2) 假设player Ⅰ已选定$a_1,a_2,\cdots,a_k$,player Ⅱ已选定$b_1,b_2,\cdots,b_k$,满足$a_i\in M$,$b_i\in N$,并且存在$M_k=\mathrm{Str}\langle a_1,a_2,\cdots,a_k\rangle$到$N_k=\mathrm{Str}\langle b_1,b_2,\cdots,b_k\rangle$的同构$f$,使$f:a_i\leftrightarrow b_i$, $i=1,2,\cdots,k$.

(3) 对于player Ⅰ任意选定的$a_{k+1}\in M$,a_{k+1}为p^t阶的元素,则$p^ta_{k+1}\in M_k$,设μ是使$p^\mu a_{k+1}\in M_k$的最小数,则对任意元素$x\in M_{k+1}=\mathrm{Str}\langle a_1,a_2,\cdots,a_{k+1}\rangle$. x可以分解为$x=g+qa_{k+1}$其中$g\in M_k$,$q\in\{0,1,2,\cdots,p^{\mu-1}\}$. 易证此分解是由$x$唯一确定的

$\mu=0$时,$a_{k+1}\in M_k$即$M_{k+1}=M_k$,选取$f(a_{k+1})=b_{k+1}\in N_k$作为player Ⅱ的选择

$\mu\neq 0$时,令$b=f(p^\mu a_{k+1})\in N_k$,那么方程$px=b$在模$N$中有$p^n$多个解,由定理3可知$px=b$在$N_k$中至多有$p^k$个解,因而至少有$p^n-p^k(k<n)$个解不在$N_k$中,因此可以取到$c_1\in N-N_k$,使$pc_1=b$,同时可以取到$c_2,c_3,\cdots,c_\mu$满足$pc_\mu=c_{\mu-1}$,$pc_{\mu-1}=c_{\mu-2}$,$\cdots$,$pc_2=c_1$,这时$c_2,c_3,\cdots,c_\mu$都不是$N_k$中元素 否则若$c_\mu\in N_k\Rightarrow c_{\mu-1}\in N_k\Rightarrow\cdots\Rightarrow c_1\in N_k$与$c_1$的取法不合. 取$b_{k+1}=c_\mu$,$N_{k+1}=\mathrm{Str}\langle b_1,b_2,\cdots,b_k,b_{k+1}\rangle$,由$b_{k+1}$取法可知,$p^\mu b_{k+1}=pc_1=b\in N_k$. 当$\nu<\mu$时,$p^\nu b_{k+1}\notin N_k$,因为$p^\nu b_{k+1}=p^\nu c_\mu=c_{\mu-\nu}\notin N_k$. N_{k+1}中任意元素y,$y=g+gb_{k+1}$,$q\in N_k$,$0\leq q\leq p^\mu-1$. y的这种分解是唯一的,从而可知$M_{k+1}=M_k\oplus p^\mu R_pa_{k+1}$,$N_{k+1}=N_k\oplus p^\mu R_pb_{k+1}$. 同构$f:M_k\to N_k$: $a_i\leftrightarrow b_i$ $(i=1,2,\cdots,k)$可以扩充为$\bar{f}:a_i\leftrightarrow b_i$ $(i=1,2,\cdots,k,k+1)$是M_{k+1}到N_{k+1}的同构 同样,对player Ⅰ任意选定的$b'_{k+1}\in N$,player Ⅱ可以找到$a'_{k+1}\in M$,使得$\bar{f}:a_i\to b_i$, $a'_{k+1}\to b'_{k+1}$, $(i=1,2,\cdots,k)$成为$\mathrm{Str}\langle a_1,a_2,\cdots,a_k,a_{k+1}\rangle$到$\mathrm{Str}\langle b_1,b_2,\cdots,b_k,b_{k+1}\rangle$的同构

由上述(1)、(2)、(3)可知player Ⅱ在Ehrenfeucht Game $G_n(M,N)$中有必胜策略 证毕

引理5 A,B是两个模型,$n,k\in\mathbf{N}$,$\bar{a}_k\in A^k$,$\bar{b}_k\in B^k$,则$(A,\bar{a}_k)\underset{n+1}{\equiv}(B,\bar{b}_k)$充要条件是下述同时成立:

1) 对A中任意元素,a_{k+1},有$b_{k+1}\in B$,使得$(A,\bar{a}_{k+1})\underset{n}{\equiv}(B,\bar{b}_{k+1})$

2) 对B中任意元素b_{k+1},有$a_{k+1}\in A$,使得$(A,\bar{a}_{k+1})\underset{n}{\equiv}(B,\bar{b}_{k+1})$.

此引理属于[1].

推论1 令 R_p-模 $M=\overset{m}{\oplus}R_p$, 对任意 $n\leq m$, $N=\overset{n}{\oplus}R_p$, 则 M, N 是 n-初等等价的.

证明 由定理4及引理5可得.

用 $T_n(K)$ 来表示语言 $\mathbf{L}$ 的量词深度 $\leq n$ 的语句集, 这些语句在模型类 K 中被满足. 令

$$M_\mu(p)=\{\overset{m}{\oplus}p^\mu R_p \mid m\in N\},\ N_\mu(p)=\{\overset{v}{\oplus}p^\mu R_p \mid v\leq n\}.$$

推论2 $T_n(M_\mu(p))=T_n(N_\mu(p))$.

定理6 设 M_1, M_2, N 是 R-模, 若 player Ⅱ 在 Ehrenfeucht Game $G_n(M_1, M_2)$ 中有必胜策略, 则在 $G_n(M_1\oplus N, M_2\oplus N)$ 中也有必胜策略.

证明 设 player Ⅱ 在 Game $G_n(M_1, M_2)$ 中有必胜策略, 用归纳法证明 player Ⅱ 在 $G_n(M_1\oplus N, M_2\oplus N)$ 中也有必胜策略, 设在第 l 次选择后, 有对应

$$f: a_1+c_1\leftrightarrow b_1+c_1',\ a_2+c_2\leftrightarrow b_2+c_2',\ \cdots,\ a_l+c_l\leftrightarrow b_l+c_l',$$

使得

$$\mathrm{Str}\langle a_1+c_1, a_2+c_2, \cdots, a_l+c_l\rangle\overset{f}{\cong}\mathrm{Str}\langle b_1+c_1', b_2+c_2', \cdots, b_l+c_l'\rangle$$

对于 $M_1\oplus N$ 中任意元素 $a_{l+1}+c_{l+1}$, 由假设存在 M_2 中元素 b_{l+1}, 使

$$\mathrm{Str}\langle a_1, a_2, \cdots, a_l, a_{l+1}\rangle\overset{g}{\cong}\mathrm{Str}\langle b_1, b_2, \cdots, b_l, b_{l+1}\rangle$$

$g(a_i)=b_i$, $i=1, 2, \cdots, l+1$, player Ⅱ 选取 $b_{l+1}+c_{l+1}$, $c_{l+1}'=c_{l+1}$, 则

$$\mathrm{Str}\langle a_1+c_1, a_2+c_2, \cdots, a_{l+1}+c_{l+1}\rangle\overset{f'}{\cong}\mathrm{Str}\langle b_1+c_1', b_2+c_2', \cdots, b_{l+1}+c_{l+1}\rangle,$$
$$f'(a_i+c_i)=b_i+c_i',\quad i=1, 2, \cdots, l+1.$$

由归纳法可知, player Ⅱ 在 Game $G_n(M_1\oplus N, M_2\oplus N)$ 中有必胜策略. 证毕.

令 $M(p)=\{\sum^{\text{有限}}A_\mu \mid \in M_\mu(p), \mu\in N\};\ N(p)=\{\sum^{n}B_\mu \mid B_\mu\in N_\mu(p), \mu\in N\}$.

由定理6有下述结论:

推论3 $T_n(M(p))=T_n(N(p))$.

定理7 有限可换主理想环 $R=\overset{t}{\underset{i=1}{\oplus}}R_{p_i}$, 则 $M(p_i)$ 是 R_{p_i}-模类, 并且 $T_n(M)=T_n(N)$. 其中 $M=\{\overset{t}{\underset{i=1}{\oplus}}A_i \mid A_i\in M(p_i)\};\ N=\{\overset{t}{\underset{j=1}{\oplus}}B_j \mid B_j\in N(p_j)\}$

利用定理6及推论2可以证明推论3. 同理可以证明定理7.

定理8 判定 R-模语言 $\mathbf{L}$ 中任意量词深度 n 语句的可满足性至多需 2^{cn^2} (c 是大于零的实数)

证明 由于 $\mathbf{L}$ 中任一语句化成前束标准只需多项式时间, 不妨假设 $\varphi=Q_1x_1Q_2x_2\cdots Q_nx_n\psi(x_1x_2\cdots x_n)$ 具有前束形, $\psi(x_1x_2\cdots x_n)$ 不含量词, $Q_i\in\{\forall, \exists\}$. 由定理7知, $\varphi\in T_R\Leftrightarrow\varphi\in T_n(M)=T_n(N)$.

由于任意模 $\mathfrak{A}\in N_\mu(p_j)$, 有 $|\mathfrak{A}|\leq p_j^{\mu n}$; 因而任意模 $\mathfrak{A}\in N(p_j)$, 有 $|\mathfrak{A}|\leq p_j^{(1+2+\cdots+t)n}$; 从而任意模 $\mathfrak{A}\in N$, 有 $|\mathfrak{A}|\leq\prod_j p_j^{r_in}\leq 2^{d_1n}$ (d_1 只与 $\mathrm{char}(R)$ 有关).

于是要判定是否 $\varphi\in T_n(N)$ 至多需要 $|N|2^{d_1n}$ 步, 又有 $|N|=n^{d_2}$ (d_2 只与 $\mathrm{char}(R)$ 有关); 因而有判定 $\varphi\in T_n(N)$ 至多需要 $n^{d_2}\cdot 2^{d_1n}\leq 2^{cn}$.

定理9 T_R 是可判定的, 判定的计算复杂性上界 $\leq 2^{cn^2}$ 图灵步.

证明 构造多带图灵机, 注意到 R 的有限性, R 中元素与 N 中元素乘法至多需 $2^{d_1 n |R|}$ 步, 加法至多需 $2^{d_1 n} \cdot 2^{d_1 n}$ 步, 因此消去一个 Q_i 至多需要 $2^{d_1 n |R|} + 2^{2d_1 n} \leq 2^{cn}$ 步 ($c > 0$). 因此, 对长度 n 的语句判定, 至多需 $(2^{cn})^n = 2^{cn^2}$ 步.

参 考 文 献

[1] J. Ferrante, C. W. Rackoff, *The Computational Complexity of Logic Theories*, LNM 718, 1979.

[2] 王世强, 模型论基础, 科学出版社, 1987.

The Decidability and Complexity for Theories of Modules on Finitely PI Rings

Xue Rui

(Computer Center, Shanxi Teachers' University, Linfen 041004)

Abstract

By making use of Ehrenfeucht Game theory, we give a successful procedure to decide the theories of modules on finitely principal ideal (PI) rings, and also the decision process upper bounds 2^{cn^2}.

Keywords n-elementary equivalent, Ehrenfeucht Game, decidability, computational complexity.