密码学进展——CHINACRYPT′2000

第六届中国密码学学术会议论文集

王萼芳　杨伟成　编

科学出版社

2000

内 容 简 介

本书是2000年5月在武汉召开的第六届中国密码学学术会议论文集。书中收集了密码学各分支的研究论文40篇，主要内容包括序列密码和线性阵列、分组密码和公钥密码、自动机密码、认证理论和秘密共享、数字签名、Bent函数和布尔函数、与密码有关的代数、逻辑、混沌理论和零知识证明以及密码的应用等。

本书可供从事密码学、数学和计算机通讯专业的科技人员以及高等院校相关专业的师生参考。

图书在版编目(CIP)数据

密码学进展——CHINACRYPT'2000：第六届中国密码学学术会议论文集/王尊芳，杨伟成编．-北京：科学出版社，2000

ISBN 7-03-008262-1

Ⅰ．密… Ⅱ．①王… ②杨… Ⅲ．密码-理论-学术会议-中国-文集 Ⅳ．TN918．1-53

中国版本图书馆CIP数据核字（2000）第01507号

科学出版社 出版

北京东黄城根北街16号

邮政编码：100717

新蕾印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

2000年5月第 一 版 开本：787×1092 1/16

2000年5月第一次印刷 印张：16

印数：1—1 000 字数：368 000

定价：25.00元

（如有印装质量问题，我社负责调换〈新欣〉）

前　言

第六届中国密码学学术会议于2000年5月在武汉召开，本书收集了在这次会议上报告的40篇论文，内容涉及序列密码和线性阵列、分组密码和公钥密码、自动机密码、认证理论和秘密共享、数字签名、Bent函数和布尔函数、与密码有关的代数、逻辑、混沌理论和零知识证明，以及密码的应用等研究课题。这些论文反映了我国密码学学术界近年来的研究动态，从中可以看到，我们的研究工作正在不断地走向深入。

本届会议共收到论文57篇，每篇收到的论文都由程序委员会中2名以上的专家主审。在1999年10月23日召开的程序委员会会议上，委员们经过认真讨论，决定了录用的论文。我们感谢所有的投稿者对会议的关心和支持。

中国船舶工业总公司第七二二研究所为本届会议提供了赞助，并为会议的召开作了大量的组织工作，在此向他们表示衷心感谢。

环 $Z/(2^e)$ 上本原序列导出序列的 0、1 分布[1)]

朱凤翔　戚文峰

（郑州信息工程大学应用数学系，郑州　450002）

摘要　本文研究环 $Z/(2^e)$ 上本原序列最高权位的 0、1 分布，证明了当 $e\geqslant 8$，次数 $n\geqslant 30$ 时，本原序列 $\boldsymbol{a}$ 的最高权位序列 $\boldsymbol{a}_{e-1}$ 在一个周期中 0（或 1）所占的比例 $\lambda(\boldsymbol{a}_{e-1})$ 满足 $43.7477\%<\lambda(\boldsymbol{a}_{e-1})<56.2523\%$。

关键词　线性递归序列　本原序列　最高权位序列

1. 引　　言

设 $f(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_0$ 是环 $Z/(2^e)$ 上首一多项式。若 $Z/(2^e)$ 上序列 $\boldsymbol{a}=(a_0,a_1,\cdots\cdots)$ 满足递归式 $a_{i+n}=-(c_0a_i+\cdots+c_{n-1}a_{i+n-1})$，$i=0,1,2,\cdots$，则称 $\boldsymbol{a}$ 为 $f(x)$ 生成的线性递归序列，记 $G(f(x))$ 为由 $f(x)$ 生成的序列全体，$G'(f(x))=\{\boldsymbol{a}\in G(f(x))\mid \boldsymbol{a}\neq \boldsymbol{0} \bmod 2\}$。$Z/(2^e)$ 上序列 $\boldsymbol{a}$ 有唯一的权位分解 $\boldsymbol{a}=\boldsymbol{a}_0+\boldsymbol{a}_1\cdot 2+\cdots+\boldsymbol{a}_{e-1}\cdot 2^{e-1}$，称 $\boldsymbol{a}_i$ 是 $\boldsymbol{a}$ 的第 i 权位，$\boldsymbol{a}_{e-1}$ 是 $\boldsymbol{a}$ 的最高权位序列。对 $Z/(2^e)$ 上 n 首一多项式 $f(x)$，若 $\mathrm{per}(f(x))=2^{e-1}(2^n-1)$，则称 $f(x)$ 是 $Z/(2^e)$ 上 n 次本原多项式，此时对 $d=1,2,\cdots,e-1$，在 $Z/(2^e)$ 上有

$$x^{2^{d-1}T}-1=2^dh_d(x)\quad \bmod f(x) \tag{1}$$

其中 $h_d(x)$ 是 $Z/(2^e)$ 上次数小于 n 的多项式且显然有 $h_d(x)\neq 0 \bmod 2$，$h_1(x)\neq 1 \bmod 2$，$h_2(x)=h_3(x)=\cdots=h_{e-1}(x) \bmod 2$，$h_2(x)=h_1(x)(1+h_1(x)) \bmod (2,f(x))$。若 $e\geqslant 3$ 且 $h_2(x)\neq 1 \bmod 2$，则称 $f(x)$ 是强本原多项式。若 $f(x)$ 是 $Z/(2^e)$ 上 n 次本原多项式，$\boldsymbol{a}\in G'(f(x))$，即 $\boldsymbol{a}_0\neq \boldsymbol{0}$，则称 $\boldsymbol{a}$ 是由 $f(x)$ 生成的 $Z/(2^e)$ 上的本原序列。由文献[2]，本原序列 $\boldsymbol{a}$ 的第 k 权位序列 $\boldsymbol{a}_k$ 的周期 $\mathrm{per}(\boldsymbol{a}_k)=2^kT$，其中 $T=2^n-1$。文献[3]给出了具有重要密码意义的保熵定理。

定理 A[3]　设 $f(x)$ 是 $Z/(2^e)$ 上本原多项式，$\boldsymbol{a},\boldsymbol{b}\in G(f(x))$，则 $\boldsymbol{a}_{e-1}=\boldsymbol{b}_{e-1}$ 当且仅当 $\boldsymbol{a}=\boldsymbol{b}$。即本原序列 $\boldsymbol{a}$ 的最高权位 $\boldsymbol{a}_{e-1}$ 包含了原序列 $\boldsymbol{a}$ 的所有信息。

文献[4,5]给出了 $\boldsymbol{a}_{e-1}$ 的 0、1 分布的二种描述，本文在文献[5]的基础上，更精确地刻划了 $\boldsymbol{a}_{e-1}$ 的 0、1 分布。

定理 B[5]　设 $f(x)$ 是 $Z/(2^e)$ 上 n 次强本原多项式，$e\geqslant 8$，$h_1(x)$ 和 $h_2(x)$ 由(1)式确定，若 $h_1(x)h_2(x)\neq 1 \bmod (2,f(x))$，$(1+h_1(x))h_2(x)\neq 1 \bmod (2,f(x))$，则对 $\boldsymbol{a}\in G'(f(x))$：

(1) 若 $n\geqslant 10$，则 $40.2505\%<\lambda(\boldsymbol{a}_{e-1})<59.7495\%$。

1) 国家自然科学基金(19771088)及河南省自然科学基金资助课题。

(2) 若 $n\geqslant 30$，则 $40.6249\%<\lambda(\boldsymbol{a}_{e-1})<59.3751\%$。

2. 最高权位序列的 0、1 分布

引理 1[5] 设 $f(x)$ 是 $Z/(2^e)$ 上 n 次本原多项式，$T=2^n-1$，$\boldsymbol{a}$ 是由 $f(x)$ 生成的 $Z/(2^e)$ 上本原序列，设 $1\leqslant d\leqslant e/2$，令 $Z/(2^d)$ 上序列 $\boldsymbol{\alpha}=h_{e-d}(x)\boldsymbol{a} \bmod 2^d$，其中 $h_{e-d}(x)$ 由(1)式确定，$n_0(\boldsymbol{\alpha})$ 表示 $\boldsymbol{\alpha}$ 在一个周期($=2^{d-1}T$)中 0 的个数，则 $\boldsymbol{a}_{e-1}$ 在一个周期中 0 所占的比例 $\lambda(\boldsymbol{a}_{e-1})$ 满足 $\frac{1}{2}-\frac{n_0(\boldsymbol{\alpha})}{2^dT}\leqslant\lambda(\boldsymbol{a}_{e-1})\leqslant\frac{1}{2}+\frac{n_0(\boldsymbol{\alpha})}{2^dT}$。

引理 2[6] 设 $\boldsymbol{a}$ 是 $Z/(2^2)$ 上 n 次本原多项式生成的本原序列，对 $i\in Z/(2^2)$，记 $n_i(\boldsymbol{a})$ 为 $\boldsymbol{a}$ 在一个周期($=2(2^n-1)$)中 i 出现的次数，则有(其中 $\delta,\varepsilon\in\{-1,0,1\}$)

n 的条件	$n_0(\boldsymbol{a})$	$n_1(\boldsymbol{a})$	$n_2(\boldsymbol{a})$	$n_3(\boldsymbol{a})$	δ,ε 的条件
$n=2m$	$2^{n-1}-\delta 2^m-2$	$2^{n-1}-\varepsilon 2^m$	$2^{n-1}+\delta 2^m$	$2^{n-1}+\varepsilon 2^m$	$\delta\varepsilon=0$
	$2^{n-1}-\delta 2^{m-1}-2$	$2^{n-1}-\varepsilon 2^{m-1}$	$2^{n-1}+\delta 2^{m-1}$	$2^{n-1}+\varepsilon 2^{m-1}$	$\delta\varepsilon\neq 0$
$n=2m+1$	$2^{n-1}-\delta 2^m-2$	$2^{n-1}-\varepsilon 2^m$	$2^{n-1}+\delta 2^m$	$2^{n-1}+\varepsilon 2^m$	$\lvert\delta\rvert=\lvert\varepsilon\rvert$
	$2^{n-1}-\delta 2^{m-1}-2$	$2^{n-1}-\varepsilon 2^{m-1}$	$2^{n-1}+\delta 2^{m-1}$	$2^{n-1}+\varepsilon 2^{m-1}$	$\lvert\delta\rvert\neq\lvert\varepsilon\rvert$

下面讨论 $Z/(2^4)$ 上本原序列一个周期中 0 的个数的上界。设 $\boldsymbol{a},\boldsymbol{b}$ 是 $Z/(2^2)$ 上周期都为 $2T$ 的序列，对 $i,j\in Z/(2^2)$，用 $n_{ij}(\boldsymbol{a},\boldsymbol{b})$ 表示在 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的一个周期中使得 $a_k=i$ 且 $b_k=j$ 的出现的次数，即 $n_{ij}(\boldsymbol{a},\boldsymbol{b})=|S_{ij}|$，其中 $S_{ij}=\{k\mid a_k=i,b_k=j,k=0,1,\ldots,2T-1\}$。

定理 1 设 $f(x)$ 是 $Z/(2^2)$ 上 n 次本原多项式，$\boldsymbol{a}=(a_0,a_1,a_2,\ldots)$，$\boldsymbol{b}=(b_0,b_1,b_2,\ldots)\in G'(f(x))$ 且 $\boldsymbol{a}\neq\boldsymbol{b} \bmod 2$。令 $\boldsymbol{c}=\boldsymbol{a}+\boldsymbol{b},\boldsymbol{d}=\boldsymbol{a}-\boldsymbol{b},\boldsymbol{u}=\boldsymbol{a}+2\boldsymbol{b},\boldsymbol{v}=2\boldsymbol{a}+\boldsymbol{b}$，显然 $\boldsymbol{c},\boldsymbol{d},\boldsymbol{u},\boldsymbol{v}$ 仍是 $Z/(2^2)$ 上由 $f(x)$ 生成的本原序列。对 $i,j\in Z/(2^2)$，简记 $n_{ij}=n_{ij}(\boldsymbol{a},\boldsymbol{b})$，令

$$D=(n_{00},n_{01},n_{02},n_{03},n_{10},n_{11},n_{12},n_{13},n_{20},n_{21},n_{22},n_{23},n_{30},n_{31},n_{32},n_{33})^t \tag{2}$$

$$B=(n_0(\boldsymbol{c}),n_1(\boldsymbol{c}),n_2(\boldsymbol{c}),n_3(\boldsymbol{c}),n_0(\boldsymbol{a}),n_1(\boldsymbol{a}),n_2(\boldsymbol{a}),n_0(\boldsymbol{b}),n_1(\boldsymbol{b}),$$
$$n_2(\boldsymbol{b}),n_0(\boldsymbol{d}),n_1(\boldsymbol{d}),n_0(\boldsymbol{u}),n_1(\boldsymbol{u}),n_0(\boldsymbol{v}),n_1(\boldsymbol{v}))^t$$

其中 t 表示转置，$n_i(\boldsymbol{c})$ 表示 $\boldsymbol{c}$ 在一个周期($=2(2^n-1)$)中 i 的个数，$i\in Z/(2^2)$，则 $D=A\cdot B$：

$$A=\begin{pmatrix}
0 & -1/8 & -1/4 & -1/8 & 1/8 & 0 & -1/8 & 1/8 & 0 & -1/8 & 1/4 & 0 & 1/4 & 0 & 1/4 & 0\\
-1/4 & 1/8 & -1/4 & -1/8 & 3/8 & 0 & 1/8 & 1/8 & 1/4 & 1/8 & 0 & -1/4 & -1/4 & 0 & 0 & 1/4\\
0 & -1/8 & 1/4 & -1/8 & 1/8 & 0 & -1/8 & 1/8 & 0 & 3/8 & -1/4 & 0 & 1/4 & 0 & -1/4 & 0\\
1/4 & 1/8 & 1/4 & 3/8 & 3/8 & 0 & 1/8 & -3/8 & -1/4 & -3/8 & 0 & 1/4 & -1/4 & 0 & 0 & -1/4\\
-1/4 & -1/8 & -1/4 & -3/8 & 1/8 & 1/4 & 1/8 & 3/8 & 0 & 1/8 & 0 & 1/4 & 0 & 1/4 & -1/4 & 0\\
0 & 1/8 & 1/4 & 1/8 & -1/8 & 1/4 & -1/8 & -1/8 & 1/4 & -1/8 & 1/4 & 0 & 0 & -1/4 & 0 & -1/4\\
-1/4 & -1/8 & -1/4 & 1/8 & 1/8 & 1/4 & 1/8 & -1/8 & 0 & 1/8 & 0 & -1/4 & 0 & 1/4 & 1/4 & 0\\
1/2 & 1/8 & 1/4 & 1/8 & -1/8 & 1/4 & -1/8 & -1/8 & -1/4 & -1/8 & -1/4 & 0 & 0 & -1/4 & 0 & 1/4\\
0 & -1/8 & 1/4 & -1/8 & 1/8 & 0 & 3/8 & 1/8 & 0 & -1/8 & -1/4 & 0 & -1/4 & 0 & 1/4 & 0\\
-1/4 & -3/8 & -1/4 & -1/8 & -1/8 & 0 & 1/8 & 1/8 & 1/4 & 1/8 & 0 & 1/4 & 1/4 & 0 & 0 & 1/4\\
0 & -1/8 & -1/4 & -1/8 & 1/8 & 0 & 3/8 & 1/8 & 0 & 3/8 & 1/4 & 0 & -1/4 & 0 & -1/4 & 0\\
1/4 & 5/8 & 1/4 & 3/8 & -1/8 & 0 & 1/8 & -3/8 & -1/4 & -3/8 & 0 & -1/4 & 1/4 & 0 & 0 & -1/4\\
1/4 & 3/8 & 1/4 & 5/8 & -3/8 & -1/4 & -3/8 & 3/8 & 0 & 1/8 & 0 & -1/4 & 0 & -1/4 & -1/4 & 0\\
1/2 & 1/8 & 1/4 & 1/8 & -1/8 & -1/4 & -1/8 & -1/8 & 1/4 & -1/8 & -1/4 & 0 & 0 & 1/4 & 0 & -1/4\\
1/4 & 3/8 & 1/4 & 1/8 & -3/8 & -1/4 & -3/8 & -1/8 & 0 & 1/8 & 0 & 1/4 & 0 & -1/4 & 1/4 & 0\\
0 & 1/8 & 1/4 & 1/8 & -1/8 & -1/4 & -1/8 & -1/8 & -1/4 & -1/8 & 1/4 & 0 & 0 & 1/4 & 0 & 1/4
\end{pmatrix}$$

证：对 $\boldsymbol{c}=\boldsymbol{a}+\boldsymbol{b}=(c_0,c_1,c_2,\cdots)$，考虑 n_{ij} 与 $n_k(\boldsymbol{c})$ 之间的关系，$(i,j,k\in Z/(2^2))$。因为 $c_k=0$ 当且仅当 $(a_k,b_k)=(0,0)$ 或 $(1,3)$ 或 $(2,2)$ 或 $(3,1)$，所以 $n_{00}+n_{13}+n_{22}+n_{31}=n_0(\boldsymbol{c})$。同理有

$$n_{01}+n_{10}+n_{23}+n_{32}=n_1(\boldsymbol{c}) \qquad n_{02}+n_{11}+n_{33}+n_{20}=n_2(\boldsymbol{c})$$

$$n_{03}+n_{12}+n_{21}+n_{30}=n_3(\boldsymbol{c})$$

类似地，对 $\boldsymbol{d}=\boldsymbol{a}-\boldsymbol{b},\boldsymbol{u}=\boldsymbol{a}+2\boldsymbol{b},\boldsymbol{v}=2\boldsymbol{a}+\boldsymbol{b}$，也可建立 n_{ij} 与 $n_k(\boldsymbol{d}),n_k(\boldsymbol{u}),n_k(\boldsymbol{v})$ 之间的关系，从而得到由下列 24 个方程构成的方程组：

$$\begin{array}{lll}
n_{00}+n_{13}+n_{22}+n_{31}=n_0(\boldsymbol{c}) & n_{00}+n_{01}+n_{02}+n_{03}=n_0(\boldsymbol{a}) & n_{00}+n_{10}+n_{20}+n_{30}=n_0(\boldsymbol{b}) \\
n_{01}+n_{10}+n_{23}+n_{32}=n_1(\boldsymbol{c}) & n_{10}+n_{11}+n_{12}+n_{13}=n_1(\boldsymbol{a}) & n_{01}+n_{11}+n_{21}+n_{31}=n_1(\boldsymbol{b}) \\
n_{02}+n_{11}+n_{20}+n_{33}=n_2(\boldsymbol{c}) & n_{20}+n_{21}+n_{22}+n_{23}=n_2(\boldsymbol{a}) & n_{02}+n_{12}+n_{22}+n_{32}=n_2(\boldsymbol{b}) \\
n_{03}+n_{12}+n_{21}+n_{30}=n_3(\boldsymbol{c}) & n_{30}+n_{31}+n_{32}+n_{33}=n_3(\boldsymbol{a}) & n_{03}+n_{13}+n_{23}+n_{33}=n_3(\boldsymbol{b}) \\
n_{00}+n_{11}+n_{22}+n_{33}=n_0(\boldsymbol{d}) & n_{00}+n_{02}+n_{21}+n_{23}=n_0(\boldsymbol{u}) & n_{00}+n_{12}+n_{20}+n_{32}=n_0(\boldsymbol{v}) \\
n_{10}+n_{03}+n_{21}+n_{32}=n_1(\boldsymbol{d}) & n_{10}+n_{12}+n_{31}+n_{33}=n_1(\boldsymbol{u}) & n_{01}+n_{13}+n_{21}+n_{33}=n_1(\boldsymbol{v}) \\
n_{02}+n_{13}+n_{20}+n_{31}=n_2(\boldsymbol{d}) & n_{01}+n_{03}+n_{20}+n_{22}=n_2(\boldsymbol{u}) & n_{02}+n_{10}+n_{22}+n_{30}=n_2(\boldsymbol{v}) \\
n_{01}+n_{12}+n_{23}+n_{30}=n_3(\boldsymbol{d}) & n_{30}+n_{11}+n_{13}+n_{32}=n_3(\boldsymbol{u}) & n_{03}+n_{11}+n_{23}+n_{31}=n_3(\boldsymbol{v})
\end{array}$$

该方程组系数矩阵的秩为 16，选取下列 16 个线性无关的方程构成线性方程组：

$$\begin{array}{lll}
n_{00}+n_{13}+n_{22}+n_{31}=n_0(\boldsymbol{c}) & n_{20}+n_{21}+n_{22}+n_{23}=n_2(\boldsymbol{a}) & n_{03}+n_{10}+n_{21}+n_{32}=n_1(\boldsymbol{d}) \\
n_{01}+n_{10}+n_{23}+n_{32}=n_1(\boldsymbol{c}) & n_{00}+n_{10}+n_{20}+n_{30}=n_0(\boldsymbol{b}) & n_{00}+n_{02}+n_{21}+n_{23}=n_0(\boldsymbol{u}) \\
n_{02}+n_{11}+n_{20}+n_{33}=n_2(\boldsymbol{c}) & n_{01}+n_{11}+n_{21}+n_{31}=n_1(\boldsymbol{b}) & n_{10}+n_{12}+n_{31}+n_{33}=n_1(\boldsymbol{u}) \\
n_{03}+n_{12}+n_{21}+n_{30}=n_3(\boldsymbol{c}) & n_{02}+n_{12}+n_{22}+n_{32}=n_2(\boldsymbol{b}) & n_{00}+n_{12}+n_{20}+n_{32}=n_0(\boldsymbol{v}) \\
n_{00}+n_{01}+n_{02}+n_{03}=n_0(\boldsymbol{a}) & n_{00}+n_{11}+n_{22}+n_{33}=n_0(\boldsymbol{d}) & n_{01}+n_{13}+n_{21}+n_{33}=n_1(\boldsymbol{v}) \\
n_{10}+n_{11}+n_{12}+n_{13}=n_1(\boldsymbol{a}) & &
\end{array}$$

按(2)式中向量 D 中的 n_{ij} 顺序，该线性方程组的系数矩阵为

$$C=\begin{pmatrix}
1&0&0&0&0&0&0&1&0&0&1&0&0&1&0&0\\
0&1&0&0&1&0&0&0&0&0&0&1&0&0&1&0\\
0&0&1&0&0&1&0&0&1&0&0&0&0&0&0&1\\
0&0&0&1&0&0&1&0&0&1&0&0&1&0&0&0\\
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0\\
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0\\
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0\\
1&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&0&0&1&0&1\\
1&0&0&0&0&0&1&0&1&0&0&0&0&0&1&0\\
0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&1
\end{pmatrix}$$

计算可得 C 逆 $C^{-1}=A$，则有 $D=A\cdot B$。

定理 2 设 $f(x)$ 是 $Z/(2^4)$ 上 n 次强本原多项式，$\boldsymbol{a}$ 为 $f(x)$ 生成的 $Z/(2^4)$ 上本原序列，记 $Z/(2^2)$ 上序列 $\boldsymbol{b}=h_2(x)\boldsymbol{a} \bmod 2^2$，$\boldsymbol{d}=\boldsymbol{a} \bmod 2^2$，即 $\boldsymbol{d}=\boldsymbol{a}_0+\boldsymbol{a}_1\cdot 2$。令 $n_{ij}=n_{ij}(\boldsymbol{d},\boldsymbol{b})$，其中 $i,j\in Z/(2^2)$，则 $\boldsymbol{a}$ 在一个周期($=2^3(2^n-1)$)内 0 的个数满足 $n_0(\boldsymbol{a})\leqslant 4n_{00}+2n_{02}+n_{01}+n_{03}$。

证：令 $T=2^n-1$，由(1)式，$x^{2T}-1=2^2h_2(x) \bmod f(x)$，作用于序列 $\boldsymbol{a}=\boldsymbol{a}_0+\boldsymbol{a}_1\cdot 2+\boldsymbol{a}_2\cdot 2^2+\boldsymbol{a}_3\cdot 2^3$，并由 $\mathrm{per}(\boldsymbol{a}_i)=2^iT$ 得，在 $Z/(2^2)$ 上

$$(x^{2T}-1)(\boldsymbol{a}_2+\boldsymbol{a}_3\cdot 2)=h_2(x)(\boldsymbol{a}_0+\boldsymbol{a}_1\cdot 2) \tag{3}$$

令 $\boldsymbol{c}=\boldsymbol{a}_2+\boldsymbol{a}_3\cdot 2=(c_0,c_1,c_2,\cdots)$ 和 $\boldsymbol{b}=h_2(x)(\boldsymbol{a}_0+\boldsymbol{a}_1\cdot 2)=(b_0,b_1,b_2,\cdots)$ 是 $Z/(2^2)$ 的序列，$L=2T$，则由(3)式得

$$c_{i+kL}=c_i+kb_i \bmod 2^2 \qquad k=0,1,2,3 \tag{4}$$

当 i 取 $0,1,\ldots,L-1$，k 取 $0,1,2,3$ 时，c_{i+kL} 恰好取遍 $\boldsymbol{c}$ 的第一个周期，考虑序列 $\boldsymbol{a}$ 在一个周期中所有可能为 0 的 a_i，对某固定的 i，$0\leqslant i\leqslant L-1$，设 $a_i=0 \bmod 2^2$，由(4)式得：

(1) 若 $b_i=0$，则当 $c_i=0$ 时，$\{c_i,c_{i+L},c_{i+2L},c_{i+3L}\}$ 中元素全为 0；否则全不为 0。

(2) 若 $b_i=2$，则当 $c_i=0$ 或 2 时，$\{c_i,c_{i+L},c_{i+2L},c_{i+3L}\}$ 中恰有二个元素为 0；否则当 $c_i=1$ 或 3 时，$\{c_i,c_{i+L},c_{i+2L},c_{i+3L}\}$ 中元素全不为 0。

(3) 若 $b_i\neq 0 \bmod 2$，则 $\{c_i,c_{i+L},c_{i+2L},c_{i+3L}\}$ 中恰有一个元素为 0。

综上 $n_0(\boldsymbol{a})\leqslant 4n_{00}+2n_{02}+n_{01}+n_{03}$。

推论 1 设 $f(x)$ 是 $Z/(2^4)$ 上 n 次强本原多项式，$\alpha=(\alpha_0,\alpha_1,\alpha_2,\cdots)\in G'(f(x))$，则 α 在一个周期($=2^3(2^n-1)$)中 0 的个数 $n_0(\alpha)\leqslant 2^n+12\cdot 2^{n/2}-8$。

证：令 $Z/(2^2)$ 上序列 $\boldsymbol{b}=h_2(x)\alpha \bmod 2^2$，$\boldsymbol{a}=\alpha \bmod 2^2$。由 $f(x)$ 强本原性，得 $h_2(x)\neq 1 \bmod 2$，有 $\boldsymbol{b}\neq\boldsymbol{a} \bmod 2$。设 $\boldsymbol{c}=\boldsymbol{a}+\boldsymbol{b}$，$\boldsymbol{d}=\boldsymbol{a}-\boldsymbol{b}$，$\boldsymbol{u}=\boldsymbol{a}+2\boldsymbol{b}$，$\boldsymbol{v}=2\boldsymbol{a}+\boldsymbol{b}$，显然 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c},\boldsymbol{d},\boldsymbol{u},\boldsymbol{v}$ 都是 $Z(2^2)$ 上本原序列。而对 $Z/(2^2)$ 上任一本原序列 $\boldsymbol{w}$，由引理 2

$$n_0(\boldsymbol{w})+n_2(\boldsymbol{w})=2\cdot(2^{n-1}-1)=2^n-2 \qquad n_1(\boldsymbol{w})+n_3(\boldsymbol{w})=2\cdot 2^{n-1}=2^n$$

$$2^{n-1}-2^{n/2}-2\leqslant n_0(\boldsymbol{w})\leqslant 2^{n-1}+2^{n/2}-2$$

$$2^{n-1}-2^{n/2}\leqslant n_i(\boldsymbol{w})\leqslant 2^{n-1}+2^{n/2},\quad i\in Z/(2^2) \qquad i\neq 0$$

令 $n_{ij}=n_{ij}(\boldsymbol{a},\boldsymbol{b})$，则由定理 1 并代入相应的值得

$$\begin{aligned}
n_{00}=&-n_1(\boldsymbol{c})/8-n_2(\boldsymbol{c})/4-n_3(\boldsymbol{c})/8+n_0(\boldsymbol{a})/8-n_2(\boldsymbol{a})/8+n_0(\boldsymbol{b})/8-\\
&n_2(\boldsymbol{b})/8+n_0(\boldsymbol{d})/4+n_0(\boldsymbol{u})/4+n_0(\boldsymbol{v})/4\leqslant 2^{n-3}+3\times 2^{n/2-1}-2\\
n_{01}=&-n_0(\boldsymbol{c})/4+n_1(\boldsymbol{c})/8-n_2(\boldsymbol{c})/4-n_3(\boldsymbol{c})/8+3n_0(\boldsymbol{a})/8+n_2(\boldsymbol{a})/8+n_0(\boldsymbol{b})/8\\
&+n_1(\boldsymbol{b})/4+n_2(\boldsymbol{b})/8-n_1(\boldsymbol{d})/4-n_0(\boldsymbol{u})/4+n_1(\boldsymbol{v})/4\leqslant 2^{n-3}+3\times 2^{n/2-1}\\
n_{02}=&-n_1(\boldsymbol{c})/8+n_2(\boldsymbol{c})/4-n_3(\boldsymbol{c})/8+n_0(\boldsymbol{a})/8-n_2(\boldsymbol{a})/8+n_0(\boldsymbol{b})/8+3n_2(\boldsymbol{b})/8\\
&-n_0(\boldsymbol{d})/4+n_0(\boldsymbol{u})/4-n_0(\boldsymbol{v})/4\leqslant 2^{n-3}+3\times 2^{n/2-1}\\
n_{03}=&n_0(\boldsymbol{c})/4+n_1(\boldsymbol{c})/8+n_2(\boldsymbol{c})/4+3n_3(\boldsymbol{c})/8+3n_0(\boldsymbol{a})/8+n_2(\boldsymbol{a})/8-3n_0(\boldsymbol{b})/8\\
&-n_1(\boldsymbol{b})/4-3n_2(\boldsymbol{b})/8+n_1(\boldsymbol{d})/4-n_0(\boldsymbol{u})/4-n_1(\boldsymbol{v})/4\leqslant 2^{n-3}+3\times 2^{n/2-1}
\end{aligned}$$

再由定理 1 得

$$n_0(\alpha)\leqslant 4n_{00}+2n_{02}+n_{01}+n_{03}\leqslant 2^n+12\times 2^{n/2}-8$$

定理 3 设 $f(x)$ 是 $Z/(2^e)$ 上 n 次强本原多项式，$e\geqslant 8$，对 $\boldsymbol{a}\in G'(f(x))$，则

(1) 当 $n\geqslant 10$ 时，$41.4467\%<\lambda(\boldsymbol{a}_{e-1})<58.5533\%$。

(2) 当 $n\geqslant 30$ 时，$43.7477\%<\lambda(\boldsymbol{a}_{e-1})<56.2523\%$。

证：令 $Z/(2^4)$ 上序列 $\alpha=h_4(x)\ \boldsymbol{a} \bmod 2^4$，容易验证，$n\geqslant 10$ 时，$\frac{2^n+12\cdot 2^{n/2}-8}{2^4(2^n-1)}$ 关于 n 是单调下降的，得(1)$n\geqslant 10$ 时

$$\frac{n_0(\alpha)}{2^4(2^n-1)}\leqslant\frac{2^n+12\cdot 2^{n/2}-8}{2^4(2^n-1)}<0.085533$$

(2) $n\geqslant 30$ 时

$$\frac{n_0(\alpha)}{2^4(2^n-1)}\leqslant\frac{2^n+12\cdot 2^{n/2}-8}{2^4(2^n-1)}<0.062523$$

再由引理 1 得到该结论。

定理 1 中 $\lambda(\boldsymbol{a}_{e-1})$ 的估计与文献[5]中相比，区间缩小了很多，并去掉了 $f(x)$ 的所有附加条件，但仍未能最终接近理想的 50%。从上述讨论中可以看出，如果有办法对定理 2 中 $n_0(\boldsymbol{a})$ 的上界估计得更准确些，那么 $\lambda(\boldsymbol{a}_{e-1})$ 的估计就会更接近 50%；另一方面若能把定理 1 和 2 中解方程的思想转化成另一种逻辑证明方法，将直接影响对 $\lambda(\boldsymbol{a}_{e-1})$ 的估计。

参 考 文 献

[1] Ward M. ,The arithmetical theory of linear recurring sequences,Trans. Amer. Math. Soc. 35(6),1933,600—628.

[2] Dai Zongduo,Binary sequences derived from ML-sequences over rings I:periods and minimal polynomials,Journal of Cryptology,1992 5(2),193—207.

[3] Huang Minqiang,Dai Zongduo,Projective maps of linear recurring sequences with maximal p-adic periods,Fibonacci Quart. ,1992,30(2),139—143.

[4] 戚文峰、周锦君，环 $Z/(2^e)$ 上本原序列最高权位的 0、1 分布，中国科学，A 辑，27(4)，1997，311—316。

[5] 戚文峰、周锦君，环 $Z/(2^e)$ 上本原序列最高权位的 0、1 分布(Ⅱ)，科学通报，42(18)，1997，1938—1940。

[6] Kuzmin A. S. ,The distribution of elements on cycles of linear recurrents over rings of residues,Russian Mathmatical Survey,1992,47(6),219—221.

[7] Qi Wenfeng, Yang Junhui and Zhou Jinjun, ML-Sequences over rings $Z/(2^e)$, Advances in Cryptology——ASIACRYPT'98,LNCS. 1514,Springer-Verlag,Berlin Heidelberg,1998,315—326.

[8] 戚文峰、周锦君，$Z/(2^e)$ 上压缩序列 $\boldsymbol{a}_{e-1}+\eta(\boldsymbol{a}_0,\boldsymbol{a}_1,\cdots,\boldsymbol{a}_{e-2})$ 的 0、1 分布，密码学进展——ChinaCrypt'98，科学出版社，1998，30—33。

Distribution of 0 and 1 in Sequences Derived from primitive Sequences over $Z/(2^e)$

Zhu Fengxiang　　Qi Wenfeng

(Department of Applied Mathematics,Zhengzhou Information Engineering University,Zhengzhou 450002,PRC)

Abstract In the paper we study the distribution of 0 and 1 in the the highest level of primitive sequences. It is proved that the proportion $\lambda(\boldsymbol{a}_{e-1})$ of 0(or 1) in one period of $\boldsymbol{a}_{e-1}$ satisfies $43.7477\%<\lambda(\boldsymbol{a}_{e-1})<56.2523\%$ for $e\geqslant 8$ and $n\geqslant 30$.

Key words Linear recurring sequence　Primitive sequence　Highest level sequence

交换环上线性递归阵列的代数表示

陆 佩 忠

(复旦大学计算机系,上海 200433)

摘要 设 R 是交换 Noether 环,$R[X]$是 R 上 n 个变元的多项式环,其中 $X=(x_1,\cdots,x_n)$,I 是 $R[X]$的理想,$\mathrm{Zer}(I)$是 R 上的以 I 中的每个多项式为线性递归关系的 n 维阵列组成的集合。本文利用同调代数的观点,给出 $\mathrm{Zer}(I)$中阵列的代数表示,这些表示是域上序列的迹、母函数、状态矩阵等表示在形式和作用范围等方面的综合和推广。利用 Gröbner 基理论,本文给出构造 $\mathrm{Zer}(I)$生成元的算法。

关键词 逆幂级数 状态转移矩阵 线性递归阵列 Gröbner 基

1. 引 言

本文中的 R 是交换环 Noether 环,$R[X]=R[x_1,\cdots,x_n]$是 R 上 n 个变元的多项式环。Z_+是非负整数集合。如果 I 是 $R[X]$的理想,且 $R[X]/I$ 是有限生成 R-模,则称 I 是零维理想。

域上序列的迹表示、母函数表示、状态矩阵表示等是研究的线性递归序列的重要的工具。而要研究 R 上的 n 维线性递归阵列同样需要把阵列表示出来的代数工具。由于域与交换环,一维序列与 n 维阵列都有很大的不同,欲把域上序列的研究工具推广应用到环上 n 维阵列上是有很大的难度的,现有的结果不多。当 R 是域、I 是 $R[x,y]$上的零维理想时,刘木兰和胡磊[5]给出了 Zer (I)中阵列的迹表示。同样在 R 是域、I 是 $R[x,y]$上的零维理想时,Fornasini 等[4]在研究自动控制中 2-D 有限维行为的状态空间实现问题时,给出了 $\mathrm{Zer}(I)$中阵列的状态转移矩阵表示。

本文利用同调代数的观点,对一般交换环 R,证明 $\mathrm{Zer}(I)$与 $\mathrm{Hom}_R(R[X]/I,R)$的 $R[X]$-模同构,并给出阵列的代数表示。这样的表示是域上序列的迹表示在形式和作用范围等方面的提炼、综合和推广。运用新的代数表示,并利用 Gröbner 基理论,我们可以轻松地给出构造 $\mathrm{Zer}(I)$生成元的算法。同时,对 $R[X]$一般的零维理想 I 所对应的 $\mathrm{Zer}(I)$中的环上阵列,我们给出状态转移矩阵表示,该结果大大地推广了 Fornasini 等人的结果。

2. 阵列的逆幂级数表示

形式幂级数环 $R[[X^{-1}]]=R[[x_1^{-1},\cdots,x_n^{-1}]]$在如下定义的数乘下构成 $R[X]$-模:对任意 $f(X)=\sum_i f_iX^i\in R[X]$

$$f(X)\cdot\Big(\sum_{j\in Z_+^n}a_jX^{-j}\Big)=\sum_{j\in Z_+^n}\Big(\sum_i f_ia_{i+j}\Big)X^{-j} \tag{1}$$

把 R 上的 n-维阵列 $(a_j)_{j\in Z_+^n}$ 看成 $R[[X^{-1}]]$ 中的一个元素 $\sum_{j\in Z_+^n}a_jX^{-j}$。记 $\mathscr{M}=R[[X^{-1}]]$。

对 $\mathscr{M}$ 中的任意一个阵列 α，如果存在一个非零多项式 $f\in R[X]$，使得

$$f\cdot\alpha=0$$

则称 α 是一个线性递归阵列(简称为 LRA)。

若 I 为 $R[X]$的理想，M 是 $\mathscr{M}_R$ 的 $R[X]$-子模，则定义

$$\mathrm{Zer}_{\mathscr{M}}(I)=\{\xi\in\mathscr{M}_R\mid f\cdot\xi=0,\text{对任意 } f\in I\} \tag{2}$$

在上下文明确时，简记 $\mathrm{Zer}(I)=\mathrm{Zer}_{\mathscr{M}}(I)$。

3. 阵列的同态表示

下面的引理在本文中起关键作用。

引理 1 I 是 R 的一个理想，M 是一个 R-模则

$$\mathrm{Hom}_R(R/I,M)\cong\mathrm{Ann}_M(I)$$

其中

$$\mathrm{Ann}_M(I)=\{\alpha\in M\mid \text{对任意 } f\in I,f\cdot\alpha=0\}$$

设 M 是 R-模，则称 R-模 $M^*=\mathrm{Hom}_R(M,R)$是 M 的对偶。

引理 2 若 M 是自由 R-模，则 M 可已嵌入到 M^* 中。若 M 是有限生成自由 R-模，则 M^* 与 M 同构。

引理 3 设 M 是 $R[X]$-模，因而是当然的 R-模。对任意 $f\in R[X]$，和 $\alpha\in M^*=\mathrm{Hom}_R(M,R)$，定义 $f\cdot\alpha\in M^*$，使得$(f\alpha)(m)=\alpha(f\cdot m)$，其中 $m\in M$，则在上述的数乘定义下 M^*是 $R[X]$-模。

引理 4[3](136页) 设 R,S,T,U 是有单位的环，$M={}_RM_S$，$N={}_SN_T$，$P={}_UP_T$ 是相应环的左右双模，则

$$\mathrm{Hom}_T(M\otimes N,P)\cong\mathrm{Hom}_S(M,\mathrm{Hom}_T(N,P))$$

是 U-R-双模同构。

命题 1 设 R 是任意交换环，则 $\mathrm{Hom}_R(R[X],R)\cong R[[X^{-1}]]$是 $R[X]$-模同构。

定理 1 对 R 上的任意一个阵列 $\alpha=\sum_{i\in Z_+^n}a_iX^{-i}$，存在唯一的一个 $R[X]$到 R 的同态 ϕ，使得

$$\alpha=\sum_{i\in Z_+^n}\phi(X^i)X^{-i}$$

4. *LRA* 的同态表示

下面的定理将在本文以后内容中起重要作用。

定理 2(基本对偶定理) 设 R 是交换环，N 是 $R[X]$-模，则有如下 $R[X]$-模同构

$$\mathrm{Hom}_{R[X]}(N,R[[X^{-1}]]) \cong \mathrm{Hom}_R(N,R)$$

证明：由命题 1，有正合 $R[X]$-模序列

$$0 \to R[[X^{-1}]] \to \mathrm{Hom}_R(R[X],R) \to 0$$

于是由 $\mathrm{Hom}(N,-)$函子的左正合性知

$$\mathrm{Hom}_{R[X]}(N,R[[X^{-1}]]) \cong \mathrm{Hom}_{R[X]}(N,\mathrm{Hom}_R(R[X],R))$$

下面证明

$$\mathrm{Hom}_R(N,R) \cong \mathrm{Hom}_R(N \otimes_{R[X]} R[X],R)$$

设映射

$$\theta:\begin{cases}\mathrm{Hom}_R(N,R) \to \mathrm{Hom}_R(N \otimes_{R[X]} R[X],R)\\ \alpha \to \theta(\alpha)\end{cases}$$

使得

$$\theta(\alpha):\begin{cases}N \otimes_{R[X]} R[X] \to R\\ n \otimes f \to \alpha(fn)\end{cases}$$

显然 θ 是 $R[X]$-单同态。由对任意 $\beta \in \mathrm{Hom}_R(N \otimes_{R[X]} R[X],R)$，定义 $\alpha: N \to R$，使得 $\alpha(n)=\beta(n \otimes 1)$，则 α 显然是 R-同态，故 $\alpha \in \mathrm{Hom}_R(N,R)$，且 $\theta(\alpha)(n \otimes f)=\alpha(nf)=\beta(nf \otimes 1)=\beta(n \otimes f)$，所以 $\theta(\alpha)=\beta$，即 θ 是映上的，故进而 θ 是 $R[X]$-同构。

再利用引理 4 得

$$\begin{aligned}N' &= \mathrm{Hom}_{R[X]}(N,R[[X^{-1}]])\\ &\cong \mathrm{Hom}_{R[X]}(N,\mathrm{Hom}_R(R[X],R))\\ &\cong \mathrm{Hom}_R(N \otimes_{R[X]} R[X],R)\\ &\cong \mathrm{Hom}_R(N,R)\end{aligned}$$

对任意 $R[X]$-模 N，记 $N'=\mathrm{Hom}_{R[X]}(N,R[[X^{-1}]])$。

定理 3 设 I 是 $R[X]$的理想，则

$$\mathrm{Zer}_{\mathscr{A}}(I) \cong \mathrm{Hom}_R(R[X]/I,R)。$$

证明：由引理 1 知

$$\mathrm{Zer}_{\mathscr{A}}(I) \cong \mathrm{Hom}_{R[X]}(R[X]/I,R[[X^{-1}]])$$

是 $R[X]$-模同构，因而也是 R-模同构。于是由定理 2 推知

$$\mathrm{Zer}_{\mathscr{A}}(I) \cong \mathrm{Hom}_R(R[X]/I,R)。$$

推论 1[6] 若 F 是域，I 是 $F[X]$的零维理想，则

$$\dim_F \mathrm{Zer}_{\mathscr{A}}(I) = \dim_F F[X]/I$$

5. $\mathrm{Zer}_{\mathscr{A}}(I)$的生成元集的构造

定理 4 设 R 是交换环，I 是 $R[X]$的理想，若 G^* 是 $\mathrm{Hom}_R(R[X]/I,R)$的 R-生成元集（$R[X]$-生成元集），则如下定义的映射 ξ 是 $\mathrm{Hom}_R(R[X]/I,R)$到 $\mathrm{Zer}_{\mathscr{A}}(I)$上的 $R[X]$-同构，其中

$$\xi(g^*) = \sum_{j \in Z_+^n} g^*(\overline{X}^j)X^{-j}, g^* \in G^* A \tag{3}$$

$\overline{X^j}$ 是 X^j 在 $F[X]/I$ 中的标准同态像。

下设 F 是一个域，I 是 $F[X]$的零维理想，我们要构造 F-$F[X]$-双模 $\mathrm{Zer}_{\mathcal{M}}(I)$的 F-基。实际上，我们只要构造出 $F[X]/I$ 的基 G，然后利用同构便得到 $\mathrm{Zer}_{\mathcal{M}}(I)$的基。利用 Gröbner 基理论中的常规的算法方便地实现对 $F[X]/I$ 的基的构造。

引理 5[1](58页，*Prop.* 2.1.6) 设 I 是 $F[x_1,\cdots,x_n]$的零维理想，$G=\{g_1,\cdots,g_t\}$是 I 的极小 Gröbner 基，令 $T=\{X^v \mid v\in Z_+^n, lp(g_i)\nmid X^v, i=1,\cdots,t\}$，则 T 是 $F[x_1,\cdots,x_n]/I$ 的 F-向量空间的基。

例 1 设 $F=F_2, I=\langle x^3+1,(x+1)(y^2+1),y^3+x^2y+xy\rangle$是 $F[X]$的理想，求$\mathrm{Zer}(I)$的基。

解：$G=\{x^3+1,(x+1)(y^2+1),y^3+x^2y+xy\}$是 I 的极小 GB 基。由公式(3)知 $\dim_F F[x,y]/I=7$，并容易求出 $F[x,y]/I$ 的基 $T=\{1,x,x^2,y,xy,x^2y,y^2\}$。$T^*=\{t^* \mid t\in T\}$是 T 的对偶基。

设序列的排序如下表第一行：

$X^i=$	1	x	y	x^2	xy	y^2	x^3	x^2y	xy^2	y^3	x^4	x^3y	x^2y^2	$\cdots$
$\overline{X^i}=$	1	x	y	x^2	xy	y^2	1	x^2y	y^2+x+1	x^2y+xy	x	y	y^2+x^2+1	$\cdots$

其中$\overline{X^i}$是 X^i 在 GB 基 G 约化下的标准型，现利用公式

$$\xi(t)=(t^*(\overline{X^i}))_{i\in Z_+^2} \quad t\in T$$

得到

$$\begin{aligned}
\xi(1)&=(1,0,0,0,0,0,1,0,1,0,0,0,1,\cdots)\\
\xi(x)&=(0,1,0,0,0,0,0,0,1,0,1,0,0,\cdots)\\
\xi(x^2)&=(0,0,0,1,0,0,0,0,1,0,0,0,1,\cdots)\\
\xi(y)&=(0,0,1,0,0,0,0,0,0,0,0,1,0,\cdots)\\
\xi(xy)&=(0,0,0,0,1,0,0,0,0,1,0,0,0,\cdots)\\
\xi(x^2y)&=(0,0,0,0,0,0,0,1,0,1,0,0,0,\cdots)\\
\xi(y^2)&=(0,0,0,0,0,1,0,0,1,0,0,0,1,\cdots)
\end{aligned}$$

6. *LRA* 的状态转移矩阵表示

命题 2 设 I 是 $R[X]$的理想，使得 $R[X]/I$ 是有限生成自由 R-模，且秩是 v，则存在两两交换的 v 阶方阵 $M_i\in R^{v\times v}, i=1,\ldots,n$，和行向量 $c\in R^v$，使得对任意同态 $\alpha\in \mathrm{Hom}_R(R[X]/I,R)$，存在唯一的向量 $d_\alpha\in R^v$ 满足

$$\alpha(\overline{X^i})=cM^id_\alpha^T \qquad i\in Z_+^n$$

其中 $i=(i_1,\ldots,i_n), M^i=M_1^{i_1}\cdots M_n^{i_n}, d_\alpha^T$ 是向量 d_α 的转置。

推论 2 设 R 是交换环，I 是 $R[X]$的理想，且 $R[X]/I$ 是秩为 v 的自由 R-模，则存在两两交换的 v 阶方阵 $M_i\in R^{v\times v}, i=1,\ldots,n$，和行向量 $c\in R^v$，使得对任意一个阵列 $a=(a_i)_{i\in Z_+^n}\in \mathrm{Zer}_{\mathcal{M}}(I)$，存在唯一的向量 $d_\alpha\in R^v$ 满足

$$a_i=cM_1^{i_1}\cdots M_n^{i_n}d_\alpha^T \qquad i\in Z_+^n$$

其中 $i=(i_1,\cdots,i_n)$

推论 3[4] 设 F 是域，设 I 是 $F[x,y]$的零维理想，且 $\dim_F F[x,y]/I=v$，则存在两个相互交换的 v 阶方阵 $M_i\in F^{v\times v}$，$i=1,2$，和行向量 $c\in F^v$，使得对任意一个阵列 $a=(a_i)_{i\in Z_+^n}\in \mathrm{Zer}_{\mathscr{A}}(I)$，存在唯一的向量 $d_a\in F^v$，满足

$$a_{s,t}=cM_1^s\cdot M_2^t d_a^T \qquad (s,t)\in Z_+^n$$

下面的定理刻画了零维理想，表明只有零维理想所对应的阵列才能有矩阵表示。

定理 5 I 是 $R[X]$的零维理想的充分必要条件，存在整数 $v>0$，和 n 个两两交换的 v 阶方阵 $M_i\in R^{v\times v}$，$i=1,\ldots,n$，和一个行向量 $c\in R^v$，使得对任意一个阵列 $a=(a_i)_{i\in Z_+^n}\in \mathrm{Zer}_{\mathscr{A}}(I)$，存在唯一的向量 $d_a\in R^v$ 满足

$$a_i=cM_1^{i_1}\cdots M_n^{i_n}d_a^T \qquad i\in Z_+^n \tag{4}$$

其中 $i=(i_1,\ldots,i_n)$。

参 考 文 献

[1] W. W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, Amer. Math. Society, 1994.

[2] M. F. Atiyah, I. G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley Publishing Company, 1969.

[3] N. Jacobson, Basic Algebra I, W. H. Freeman and Company, 1980.

[4] E. Fornasini, P. Rocha, S. Zampieri, State space realization of 2-D finitedimensional behaviours, SIAM J. Control and Optimization, Vol. 31, No. 6, Nov. 1993, 1502—1517.

[5] 刘木兰、胡磊，双周期阵列的迹表示，科学通报，Vol. 41, No. 5, 1996。

[6] S. Sakata, General theory of doubly periodic arrays over an arbitrary finite field and its applications, IEEE Transactions on Information Theory, Vol. IT-24, No. 6, 1978.

Representations of Linear Recurring Arrays over Commutative Rings

Lu Peizhong

(*Department of Computer Sciences Fudan University, Shanghai* 200433, *PRC*)

Abstract Let R be a commutative Noetherian ring. We present a series of representations of linear recurring arrays over R, which turn out to be the essential tools in the study of linear recurring arrays.

Key words Inverse power series State transition matrix Linear recurring array Gröbner basis

QF 环上零维理想是线性递归阵列的零化理想的判别[1)]

陆 佩 忠

(复旦大学计算机科学系信息论室,上海 200433)

刘 木 兰

(中国科学院系统科学研究所,北京 100082)

摘要 设 R 是 Quasi-Frobenius 环(简记 QF 环),$R[X]$是 R 上 n 个变元的多项式环,其中 $X=(x_1,\cdots,x_n)$。I 是 $R[X]$的任意一个零维理想。本文给出判别 I 恰是一个 R 上的一个线性递归阵列的特征理想的方法。

关键词 QF 环 Gröbner 基 线性递归阵列 零化理想

1. 引 言

线性递归序列的研究已有悠久的历史,由于密码学、编码学和系统科学等理论的应用背景,域上的线性递归阵列(LRA)的研究已有丰硕的成果。近年来,Galois 环上的 LRA 的研究已引起了广泛的兴趣[7]。Gröbner 基理论对研究环上的 LRA 提供了十分有力的工具。本文将用 Gröbner 基理论研究环上 LRA 的零化理想。我们的目的是给出判断 $R[X]$的理想 I 是否恰是一个线性递归阵列的零化理想的方法。我们的结果推广了 Obsert[8]和 M. Heiligman[3]等许多人的关于域上 LRA 零化理想判别的工作。

设 R 是有单位元的变换环。称 R 是一个 Quasi-Frobenious 环,简记 QF 环。如果 R 是 Artin 环,且对 R 的任意一个理想 I,有 $\mathrm{Ann}_R(\mathrm{Ann}_R(I))=I$。容易验证 Galois 环 $GR(q^n,p^n)$是 QF 环,更一般的局部 Artin 主理想环是 QF 环。

本文中,我们始终用 R 表示一个 QF 环。设 $\mathscr{M}=R[[X^{-1}]]=R[[x_1^{-1},\cdots,x_n^{-1}]]$是形式幂级数环,也称之为 R 上的全体阵列组成的 R-模。$\mathscr{M}_R$ 在如下定义的数乘下构成 $R[X]$-模,即对任意 $R[X]$中的单项 $X^i=x_1^{i_1}\cdots x_n^{i_n}$,和 R 中的元素 a,定义

$$aX^i\cdot\Big(\sum_{j\in Z_+^n}a_jX^{-j}\Big)=\sum_{j\in Z_+^n}(aa_j)X^{i-j}=\sum_{j\in Z_+^n}aa_{j+i}X^{-j} \tag{1}$$

其中当 $i\not\leq j$ 时,$X^{i-j}\triangleq 0$,并由此线性扩展到多项式环,即对任意 $f(X)=\sum_i f_iX^i\in R[X]$,$\alpha=\sum_{j\in Z_+^n}a_jX^{-j}\in R[[X^{-1}]]$

$$f(X)\cdot\alpha=\sum_{j\in Z_+^n}\Big(\sum_i f_ia_{i+j}\Big)X^{-j} \tag{2}$$

则 $R[[X^{-1}]]$是 $R[X]$-模。设

1) 本文得到中国博士后基金的资助。

$$\mathscr{A} = \{\alpha \in \mathscr{M} \mid \text{存在首一多项式 } f_s(x_s) \in R[x_s], \text{使得 } f_s(x_s)\alpha = 0, s = 1, \cdots, n\} \tag{3}$$

$\mathscr{A}$ 中的每个元素称之为 LRA。显然 $\mathscr{A}_R$ 也是 $R[X]$-模。

若 I 为 $R[X]$的理想，M 是 $\mathscr{M}$ 的 $R[X]$-子模，则定义

$$\mathrm{Zer}_{\mathscr{M}}(I) = \{\xi \in \mathscr{M} \mid f \cdot \xi = 0, \text{对任意 } f \in I\} \tag{4}$$

$$\mathrm{Ann}_{R[X]}(M) = \{f \in R[X] \mid f \cdot \xi = 0, \text{对任意 } \xi \in M\} \tag{5}$$

在上下文明确时，简记 $\mathrm{Zer}_{\mathscr{M}}(I)=\mathrm{Zer}(I)$，$\mathrm{Ann}_{R[X]}(M)=\mathrm{Ann}(M)$。

本文研究 $R[X]$的任意一个零维理想 I，是否存在 $\alpha\in\mathscr{A}$，使得 $I=\mathrm{Ann}(\alpha)$，即 I 恰是 α 的零化理想。同时研究何时存在 $\alpha\in\mathscr{A}$ 使得 $\mathrm{Ann}(I)=R[X]\alpha$。

2. 阵列的零化理想与不可约理想

下面讨论 LRA 特征理想的判别问题，我们需要下面的结果。

零化定理[6] 设 R 是 QF 环，I 是 $R[X]$的任意一个理想，则

$$\mathrm{Ann}_{R[X]}(\mathrm{Zer}_{\mathscr{M}}(I)) = I \tag{6}$$

强逆系定理[6] 设 R 是 QF 环，M 是 $R[[X^{-1}]]$的 $R[X]$-子模，且是有限生成 R-模，则

$$\mathrm{Zer}_{\mathscr{M}}(\mathrm{Ann}_{R[X]}(M)) = M \tag{7}$$

引理 1 设 R 是 Noether 环，I 是 $R[X]$的零维理想。则 $\mathrm{Zer}_{\mathscr{M}}(I)$是有限生成 R-模。

引理 2 设 R 是 Noether 环，I 是 $R[X]$的零维理想。若 M 是 $R[[X^{-1}]]$的 $R[X]$-子模，使得 $I=\mathrm{Ann}_{R[X]}(M)$，则 M 是有限生成 R-模。

定理 1 设 R 是 QF 环，I 是 $R[X]$的一个零维准素理想，则 I 是 $R[[X^{-1}]]$中某阵列 ζ 的特征理想当且仅当 I 是不可约理想。

证明：充分性：由于 I 是零维理想，故由引理 1 知 $\mathrm{Zer}_{\mathscr{M}}(I)$是有限生成 R-模，也当然是有限生成 $R[X]$-模。不妨设

$$\mathrm{Zer}_{\mathscr{M}}(I) = R[X] \cdot \alpha_1 + R[X] \cdot \alpha_2$$

其中 $\alpha_1, \alpha_2 \in R[[X^{-1}]]$，令 $I_i=\mathrm{Ann}_{R[X]}(\alpha_i)$，$i=1,2$，则由零点定理知

$$I = \mathrm{Ann}_{R[X]}(\mathrm{Zer}_{\mathscr{M}}(I)) = \mathrm{Ann}_{R[X]}(R[X]\alpha_1 + R[X]\alpha_2) = \mathrm{Ann}_{R[X]}(\alpha_1) \cap \mathrm{Ann}_{R[X]}(\alpha_2)$$

所以

$$I = I_1 \cap I_2$$

由于 I 是不可约理想，故 $I=I_1=\mathrm{Ann}_{R[X]}(\alpha_1)$或 $I=I_2=\mathrm{Ann}_{R[X]}(\alpha_2)$。充分性得证。

必要性：设 $I=\mathrm{Ann}_{R[X]}(\zeta)$，其中 $\zeta\in R[[X^{-1}]]$，ζ 是一个 LRA。

若 $I=I_1\cap I_2$，设 $M_1=\mathrm{Zer}(I_1)$，$M_2=\mathrm{Zer}(I_2)$是 $\mathscr{M}$ 的两个 $R[X]$-子模，则由零点定理推知，$I_i=\mathrm{Ann}_{R[X]}(M_i)$。所以

$$I = I_1 \cap I_2 = \mathrm{Ann}(M_1) \cap \mathrm{Ann}(M_2) = \mathrm{Ann}(M_1 + M_2) = \mathrm{Ann}(\zeta)$$

由于 I 是零维的，故 I_i 也是零维的。由引理 2，$R[X]\zeta$，M_1，M_2 都是有限生成 R-模，故由强逆系定理

$$M_1 + M_2 = \mathrm{Zer}(\mathrm{Ann}(M_1 + M_2)) = \mathrm{Zer}(\mathrm{Ann}(\zeta)) = R[X] \cdot \zeta$$

所以存在 $\alpha_i \in M_i$，使得 $\alpha_1+\alpha_2=\zeta$。由于 $I_i \supset I$，所以 $R[X]\cdot\zeta=\mathrm{Zer}(I)\supset\mathrm{Zer}(I_i)=M_i$，所以，存在 $f_1, f_2 \in R[X]$，使得 $\alpha_1=f_1\zeta$，$\alpha_2=f_2\zeta$。于是 $(1-f_1-f_2)\zeta=0$，这样 $1-f_1-f_2\in \mathrm{Ann}_{R[X]}(\zeta)=I$。于是 $\overline{f}_2=\overline{1}-\overline{f}_2$，其中 $\overline{f}$ 是 f 在 $R[X]/I$ 中的像。由于 I 是零维准素理想，因此包含 I 的素理想一定是极大理想，故 $P=\sqrt{I}$ 是唯一的包含 I 的素理想。所以 $R[X]/I$ 是局部环。故 $\overline{f}_1$ 在 $R[X]/I$ 中或可逆，或幂零。所以 $\overline{f}_1$，$\overline{1}-\overline{f}_1$ 中必有一个是可逆元。若 $\overline{f}_1$ 可逆，则

$$I=\mathrm{Ann}(\zeta)=\mathrm{Ann}(\overline{f}_1^{-1}\alpha_1)=\mathrm{Ann}(\alpha_1)\supseteq I_1\supseteq I$$

所以 $I=I_1$。同样，若 $\overline{f}_2$ 可逆，则 $I=I_2$。于是，我们证明了 I 是不可约理想。 ■

定理 1 把循环性的判别转化成对不可约理想的判别，这是实现解决只用 I 本身刻画 $\mathrm{Zer}_{\mathscr{M}}(I)$ 的循环性问题的关键一步。自然，我们还需要进一步刻画不可约理想。

引理 3 设 R 是 QF 环，I 是 $R[X]$ 的零维理想，若 $I=I_1\cap\cdots\cap I_s$ 是 I 的极小准素分解，$P_i=\sqrt{I_i}$，则

(1) P_i 是极大理想，$i=1,\cdots,s$。

(2) $I_i, i=1,\cdots,s$ 两两互素。

引理 4[5](引理3.19,190页) 设 R 是 Noether 局部环，P 是 R 的极大理想，Q 是 R 的 P-准素理想，则 Q 是不可约理想当且仅当 $\dim_{R/P}(Q:P)/Q=1$。

引理 5 设 R 是一个交换 Noether 环，I 是 R 的准素理想，且 $P=\sqrt{I}$，则 $I:P\neq I$。

命题 1 设 R 是一个 Noether 环，P 是 R 的极大理想，I 是 R 的一个 P-准素理想，则 I 是不可约理想当且仅当 $\dim_{\frac{R}{P}}\frac{I:P}{I}=1$。

证明："⇐"：显然，$\frac{I:P}{I}$ 是一个 R/P-模。因为 $\dim_{\frac{R}{P}}\frac{I:P}{I}=1$，故有 R/P-模同构：$\frac{I:P}{I}\cong\frac{R}{P}$。设 $S=R\backslash P$，于是 $S^{-1}I$ 是环 $S^{-1}R$ 的一个 $S^{-1}P$-准素理想。$\frac{S^{-1}I:S^{-1}P}{S^{-1}I}$ 是域 $\frac{S^{-1}R}{S^{-1}P}$ 上的一个向量空间，且满足

$$S^{-1}\left(\frac{I:P}{I}\right)\cong\frac{S^{-1}I:S^{-1}P}{S^{-1}I}\cong S^{-1}\left(\frac{R}{P}\right)\cong\frac{S^{-1}R}{S^{-1}P}$$

于是

$$\dim_{\frac{S^{-1}R}{S^{-1}P}}\frac{S^{-1}I:S^{-1}P}{S^{-1}I}=1$$

从而，由引理 4 知，$S^{-1}I$ 是 R_P 的一个不可约理想。如果存在 R 的理想 I_1, I_2，使得 $I=I_1\cap I_2$，则 $S^{-1}I=S^{-1}I_1\cap S^{-1}I_2$。因为 $S^{-1}I$ 是不可约的，故 $S^{-1}I=S^{-1}I_1$ 或 $S^{-1}I=S^{-1}I_2$。不妨设 $S^{-1}I=S^{-1}I_1$，显然 $I\subset I_1$。如果 $a\in I_1$，则 $\frac{a}{1}\in S^{-1}I_1=S^{-1}I$，从而存在 $b\in I$ 和 $u\in S$，使得 $\frac{b}{u}=\frac{a}{1}$。于是存在 $v\in S$，使得 $v(au-b)=0$。所以 $vua\in I$。如果 $a\notin I$，由 I 是 P-准素理想，所以 $vu\in P$，但这与 $vu\in S$ 相矛盾。所以只能 $a\in I$。于是证明了 $I_1\subseteq I$，进而得到 $I_1=I$，所以证明了 I 是不可约理想。

"⇒"：由引理 5，$\dim_{\frac{R}{m}}\frac{I:m}{I}>0$。如果 $\dim_{\frac{R}{m}}\frac{I:m}{I}>1$，则存在 $(I:m)/I$ 的 1 维子空间 V_1, V_2 使得 $V_1\cap V_2=0$。由于 $(I:m)/I$ 的 R/m-子空间必然是 R-子模，两者数乘的定义是