第15卷 第5期 电子科学学刊 Vol. 15, No. 5
1993 年 9 月 JOURNAL OF ELECTRONICS Sept., 1993

多个序列综合问题的新模型及其应用

陆佩忠 宋国文
(成都电信技术研究所,成都 610031)
周 锦 君
(郑州信息工程学院,郑州 450002)

摘要 本文提出新的数学模型,用来刻划序列的综合问题,并将其推广,揭示了可用Gröbner基理论解决序列的综合问题,并得到有效的算法,从而成功地开辟了解决多个序列综合问题的新途经. 本文另一重要结果是给出了 J.Justesen 等构造的一类代数几何码 (JAG 码)的有效译码算法,此算法是 Euclid 算法的非平凡推广.

关键词 序列综合; 齐次理想; Gröbner 基;代数几何码;错误位置多项式

一、引 言

设 F 为任一域, $\bar{a}=(a_0,\cdots,a_N)$ 是 F 上的序列, $A(x)=a_0+a_1x+\cdots+a_Nx^N$ 是 $\bar{a}$ 的母函数表示,下面是传统的数学模型,用来刻划综合问题.

模型 I 设 σ 是由满足如下关系的元素对 $(\sigma(x),l)$ 构成的集合:

$$\sigma(x)A(x)\equiv a(x)\bmod x^{N+1},\quad \sigma(0)\neq 0 \tag{1}$$

这里 $\sigma(x)=\sum_{i=0}^{l}\sigma_ix^i$, $a(x)$ 是与 $\sigma(x)$ 有关的多项式,且 $\deg a(x)<l$. 求 σ 中使 l 达到极小的 $(\sigma(x),l)$.

由于 σ 不是一个理想,它没有理想的加法封闭性,因而难以研究其结构,不好清楚地解释欲求的 $\sigma(x)$ 在 σ 中的地位.

显然,如果 $(\sigma(x),l)\in\sigma$,则

$$\sum_{i=0}^{l}\sigma_ia_{j-i}=0,\quad j=l,\cdots,N-1,N \tag{2}$$

因而称 $(\sigma(x),l)$ 是能生成 $\bar{a}$ 的 l 级线性反馈移位寄存器,模型 I 就是级数最短的线性移位寄存的综合.

本文主要解决两个问题: (1) 给出综合问题更加合理直观的数学模型,并证明这一

1992.04.06 收到,1992.10.19 定稿.
陆佩忠 男,1961 年生,工程师,从事代数编码、代数计算、密码学等领域的研究工作. 现通信地址: 上海市江湾镇沽源路 231 号,邮政编码 200434.
宋国文 男,1942 年生,高级工程师,现从事图象压缩、处理,通信以及信源信道编码等研究工作. 现通信地址: 上海市江湾镇沽源路 231 号,邮政编码 200434.
周锦君 女,教授,现从事密码学、代数理论等领域的研究工作.

新模型具有更加广阔的实用前景。作为应用，本文成功地解决了多个序列的综合问题[1]. (2) 利用新模型解决 J. Justensen 等所构造的基于平面代数曲线的代数几何码 (JAG) 的更加有效的译码算法问题。文献 [2,3] 给出的算法复杂性是 $O(n^4)$。本文利用 Gröbner 基理论，对 JAG 码给出了类似于 Euclid 算法的译码新算法，也就是将著名的 Berlekamp-Massey 算法[1]应用到代数几何码的译码，从而解决了这个多年悬而未决的问题。

二、序列综合的新数学模型

先介绍一些概念和符号。

齐次多项式　设 $\sigma(x_1,\cdots x_n)$ 是多元多项式，且各单项次数相同，则称 $\sigma(x_1,\cdots,x_n)$ 是齐次多项式。

多项式的齐次化　设 $n\geqslant 2$，$\sigma(x_1,\cdots,x_{n-1})\in F[x_1,\cdots,x_{n-1}]$ 是 a 次多元多项式，令 $\bar\sigma(x_1,\cdots,x_n)=x_n^a\sigma(x_1/x_n,\cdots,x_{n-1}/x_n)$，则称 $\bar\sigma$ 是 σ 的齐次化多项式。例 $n=2$，设 $\sigma(x)=\sum_{i=0}^{a}\sigma_i x^i$，且 $\sigma_a\neq 0$，则 $\bar\sigma(x,y)=y^a\sigma(x/y)=\sum_{i=0}^{a}\sigma_i x^i y^{a-i}$。

齐次理想　称 $F[x_1,\cdots,x_n]$ 中的理想 I 是齐次理想，如果 I 是由有限个齐次多项式生成的。

现将序列 $\bar a$ 的母函数 $A(x)$ 齐次化，即

$$A(x,y)=\sum_{i=0}^{N}a_i x^i y^{N-i},$$

设 I 是 $F[x,y]$ 中由 x^{N+1},y^{N+1} 生成的齐次理想。

模型 II　设 $\bar\sigma$ 是由 $F[x,y]$ 中的齐次线性方程

$$\sigma(x,y)A(x,y)\equiv 0 \mod I \tag{3}$$

的解 $\sigma(x,y)$ 全体构成的理想，确定 $\bar\sigma$ 的生成元集。

下面我们要证明模型 II 的内涵包括了模型 I。

定理 1　$(\sigma(x),l)\in\sigma$，当且仅当 $\sigma(0)\neq 0$，且 $\sigma(x)$ 的齐次化

$$\sigma(x,y)=y^l\sigma(x/y)\in\bar\sigma.$$

证明　*必要性*　因为 $(\sigma(x),l)\in\sigma$，故存在 $a(x)$，使 $\deg a(x)<l$，且

$$\sigma(x)A(x)\equiv a(x)\bmod x^{N+1},$$

则 $y^{N+l}\sigma(x/y)A(x/y)=y^l\sigma(x/y)\cdot y^N A(x/y)=\sigma(x,y)\cdot A(x,y)\equiv y^{N+l}a(x/y)\bmod x^{N+1}$，由于 $\deg a(x)<l$，故 $y^{N+l}a(x/y)\equiv 0 \bmod y^{N+1}$，所以 $\sigma(x,y)A(x,y)\equiv 0 \bmod I$，即 $\sigma(x,y)\in\bar\sigma$。

充分性　若 $\sigma(0)\neq 0$，且使其齐次化 $\sigma(x,y)\in\bar\sigma$，则 $\sigma(x,y)A(x,y)\equiv 0 \bmod I$，设 $l=\deg\sigma(x,y)$，则存在 $a(x,y),b(x,y)\in F[x,y]$，其中 $\deg a(x,y)<l,\deg b(x,y)<l$，使

$$\sigma(x,y)A(x,y)=b(x,y)\cdot x^{N+1}+a(x,y)\cdot y^{N+1} \tag{4}$$

从而 $\sigma(x,1)A(x,1)=\sigma(x)A(x)\equiv a(x,1)\bmod x^{N+1}$，显然 $\deg a(x,1)\leqslant\deg a(x,y)<l$，故 $(\sigma(x),l)\in\sigma$。

定理 2 设 $\sigma(x,y)\in\bar{\sigma}$，且 $l=\deg\sigma(x,y)=\deg_y\sigma(x,y)$，则 $(\sigma(x,1),l)\in\sigma$.

证明 由于 $l=\deg\sigma(x,y)=\deg_y\sigma(x,y)$，故 $\sigma(0,1)\neq 0$. 其余证明类似于定理 1 的充分性的证明.

由定理 1 和定理 2 便知 $\sigma=\{\sigma(x,1)|\sigma(x,y)\in\bar{\sigma},\deg\sigma(x,y)=\deg_y\sigma(x,y)\}$. 下面我们要进一步确定 $\bar{\sigma}$ 的生成元，并指出模型 I 中欲求的 $\sigma(x)$ 必可在 $\bar{\sigma}$ 的某特定生成元中找到. 为此，我们引进 Gröbner 基的概念.

三、模型 II 的推广和 Gröbner 基理论

设 I 为 $F[x_1,\cdots,x_n]$ 中的齐次理想，$g_1,\cdots,g_m$ 为生成元，且 g_i 齐次. 设 $S(x_1,\cdots,x_n)$ 是任一齐次多项式. 下面的模型是模型 II 的推广.

模型 III 设 $\bar{\sigma}$ 是 $F[x_1,\cdots,x_n]$ 上齐次线性方程

$$\sigma(x_1,x_2,\cdots,x_n)S(x_1,\cdots,x_n)\equiv 0 \bmod I \tag{5}$$

的解 $\sigma(x_1,\cdots,x_n)$ 全体构成的理想，确定 $\bar{\sigma}$ 的一组生成元.

引理 1 上述理想 $\bar{\sigma}$ 是齐次的.

证明 见文献[4].

我们称 $\bar{\sigma}$ 是生成理想. 现给出多个序列的综合问题的求解. 冯贵良[1]已解决此问题，但其算法的描述和正确性的证明非常繁杂. 为简便起见，我们只给出三个序列时的情形.

多个序列的综合 设 $\bar{a}=(a_0,\cdots,a_N),\bar{b}=(b_0,\cdots,b_N),\bar{c}=(c_0,\cdots,c_N)$ 是三个 F 上的序列，求能同时生成这三个序列的级数最短的线性移位寄存器.

求解过程 (1) 记 $d_i(x_3,x_4)=a_ix_3^2+b_ix_3x_4+c_ix_4^2,\ i=0,\cdots,N$. (2) 记 $S(x_1,x_2,x_3,x_4)=\sum_{i=0}^{N}d_i(x_3,x_4)x_1^ix_2^{N-i}$. (3) 作齐次理想 $I=\langle x_1^{N+1},x_2^{N+1},x_3^3,x_4^3\rangle$. (4)利用模型 III 求出生成理想 $\bar{\sigma}$ 的生成元组.

可见，算法的关键是第 (4) 步. 为此要引进 Gröbner 基的概念. 有关这方面的详细介绍见文献[5].

设 s,t,u 是 $F[x_1,\cdots,x_n]$ 中的单项，设“$<_T$”是定义在单项集上的全序，且满足：

(T_1) $1<_T t$ 对所有单项 $t\neq 1$.

(T_2) 如果 $s<_T t$，则 $s\cdot u<_T t\cdot u$.

例 1 全次数全序 在 $F[x,y]$ 上定义

$$1<_T x<_T y<_T x^2<_T xy<_T y^2<_T x^3<_T x^2y<_T\cdots.$$

例 2 纯字典全序 在 $F[x,y]$ 上定义

$$1<_T x<_T x^2<_T\cdots<_T y<_T xy<_T x^2y<_T\cdots<_T y^2<_T xy^2<_T x^2y^2<_T\cdots.$$

对已经选定某全序后，我们引出下面符号：

$\mathrm{Coef}(g,t)$ 多项式 g 中单项 t 前的系数.

$\mathrm{LP}(f)$ 多项式 f 相对于“$<_T$”极大单项，即 f 的首项.

LC(f)　　f 的首项系数.

定义 1　设 K 是 $F[x_1,\cdots,x_n]$ 中的有限集，对于多项式 g，若存在 $f\in K$，常数 b，单项 u，使 $h=g-b\cdot u\cdot f$，且 $\mathrm{Coef}(g,u\cdot \mathrm{LP}(f))=b\cdot \mathrm{LC}(f)\neq 0$，则称 $g\bmod K$ 简约成 h. 这时记 $g\to_K h$，称 g 可用 f,b,u 简化，记 $g\to_{f,b,u}$.

可见，简化过程类似于多项式除法，将“大”的单项用一些“小”的单项和替代.

例 3　设 $K=\{f_1,f_2,f_3\}$，其中 $f_1=x^3y+xy+y+x^2+1$，$f_2=x^3y+xy+y+x^3+x+1$ $f_3=x^2y+x^3+x^2$，域 $F=F_2$，“$<_T$”是定义在 $F[x,y]$ 上的纯字典全序. 设 $g=x^4y^2+x^3y+y+x+1$，则下面的 h_1,h_2,h_3,h_4 是逐步简化得到的多项式.

$$h_1=g-xyf_1=x^2y^2+xy^2+xy+y+x+1$$
$$h_2=h_1-yf_3=xy^2+x^3y+x^2y+xy+y+x+1$$
$$h_3=h_2-xf_3=xy^2+x^2y+xy+y+x^4+x^3+x+1$$
$$h_4=h_3-f_3=xy^2+xy+y+x^4+x^2+x+1$$

因此，$g\to_K h_1\to_K h_2\to_K h_3\to_K h_4$，$g\to_{f_1,1,xy}$ 等.

定义 2　称 g 是 mod$K$ 的标准型，如果不存在 h，使 $g\to_K h$.

例 4　如例 2 中的 h_4 是 mod$K$ 的标准型. 因为 h_4 的单项都要小于 K 中多项式的首项，故不能再简化了.

定义 3　称 h 是 g mod$K$ 的标准型，如果存在一个简化过程：$g=h_0\to_K h_1\to_K\cdots\to_K h_m=h$，且 h 是 mod$K$ 的标准型.

例 5　如例 2，h_4 是 g mod$K$ 的标准型.

定义 4　称 S 为标准型算法，如果输入任意有限集 K，和多项式 g，其输出多项式 $S(K,g)$ 是 g mod$K$ 的标准型. 下面算法是标准型算法[5]，采用类似于 C 语言表示：

算法 1　Normal Form(F,g)

$h:=g$

while($\exists f\in K,b,u$，使 $h\to_{f,b,u}$)

do (取 $f\in K,b,u$，使 $h\to_{f,b,u}$，且 $u\cdot \mathrm{LP}(f)$ 极大，$h:=h-b\cdot u\cdot f$)

return h

定义 5　有限多项式集 K 是 Gröbner 基，如果对任意多项式 g，若 h_1,h_2 都是 g mod$K$ 的标准型，则 $h_1=h_2$.

例 6　例 2 中的 K 不是 Gröbner 基. 因为可设 $g=x^3y$，则 $g-f_1\triangleq h_1=xy+y$ x^2+1，$h_2\triangleq g-f_2=xy+y+x^3+x+1$，显然，$h_1,h_2$ 都是 g mod$K$ 的标准型，但 $h_1\neq h_2$

例 7　设 $K=\{x^n,y^m\}$，则 K 是 Gröbner 基. 因为，若 h_1,h_2 都是 mod$K$ 的标准型，且 $h_1\equiv h_2 \bmod K$ 则 $h_1-h_2\equiv 0 \bmod (x^n,y^m)$，若 $h_1\neq h_2$，故 h_1 或 h_2 中有单项是 x^n 或 y^m 的倍数，这与 h_1,h_2，是 mod$K$ 标准型矛盾.

定义 6　称 K 是既约 Gröbner 基，如果 K 是 Gröbner 基，且对所有 $f\in K$，f 是 mod$(K-\{f\})$ 的标准型，且 $\mathrm{LC}(f)=1$.

文献[5]给出了一个有效的算法，简称 RGB 算法. 输入有限集 $K=\{k_1,\cdots,k_n\}$，输出既约 Gröbner 基 $G=\mathrm{RGB}(K)$，使 Ideal(K) = Ideal(G).

定义 7 对任意多项式 f_1,f_2 对应一个多项式 $SP(f_1,f_2)=u_1f_1-(c_1/c_2)u_2\cdot f_2$，这里 $c_i=LC(f_i)$，u_i 使 s_iu_i 是 s_1,s_2 的最小公倍，这里 $s_i=LP(f_i)$，$i=1,2$。

下面的定理刻划了 Gröbner 基的特征。

定理 3 设 $I=Ideal(K)$，S 是任一标准型算法，则下列条件等价

(1) K 是 Gröbner 基

(2) 设 $LP(M)$ 是多项式集合 M 中多项式首项构成的集合，则 $LP(K)$ 可以生成 $LP(I)$，即 $LP(I)$ 中的单项是 $LP(K)$ 中某单项的倍数。

(3) 对任一 $f\in I$，则 $S(K,f)=0$

(4) 对任一 $f_1,f_2\in K$，存在 $h_1,\cdots,h_m$，使

$$SP(f_1,f_2)\to_K h_1\to_K\cdots\to_K h_m=0$$

(5) 对任一 $f\in I$，存在表示式 $f=\sum_{i=1}^{n}h_ik_i$，且 $LP(f)\geqslant_T \max\{LP(h_ik_i)\}$。(此时，称之为 G-表示。)

证明 见文献 [6]

定理 4 设 $G=\{g_1,\cdots,g_m\}$ 是既约 Gröbner 基，且 $LP(g_1)<_T\cdots<_T LP(g_m)$，若 $f\in Ideal(G)$，使 $LP(f)<_T LP(g_{l+1})$，则 $f\in Ideal(g_1,\cdots,g_l)$，$f=\sum_{i=1}^{l}f_ig_i$，其中 $LP(f)\geqslant_T \max_{i\leqslant l}\{LP(f_ig_i)\}$。特别当 f 是 $Ideal(G)$ 中相对于 "$<_T$" 使 $LP(f)$ 达到最小的非常量首一多项式，则 $f=g_1$。

证明 由定理 3(5) 知

$$f=\sum_{i=1}^{l}f_ig_i+\sum_{i=l+1}^{m}f_ig_i,$$

且 $LP(f)\geqslant \max_{1\leqslant i\leqslant m}\{LP(f_ig_i)\}$，故 $f_{l+1}=\cdots=f_m=0$。当 f 在 $Ideal(G)$ 中达到 $LP(f)$ 极小，故 $LP(f)<_T LP(g_2)$，所以 $f=f_1g_1$，再由 f 的非常数首一性质知 $f=g_1$。

定理 5 设 G 如定理 4，若 $f\in Ideal(G)$，使 $f\notin Ideal(g_1,\cdots,g_l)$，$LP(f)\leqslant LP(g_{l+1})$，首一，则 $f=f_{l+1}+\sum_{i=1}^{l}f_ig_i$，其中 $LP(f)>LP(g_if_i)$，$i=1,\cdots,l$。

证明 由定理 4 知，$f=\sum_{i=0}^{l+1}f'_ig_i$，且 $LP(f)\geqslant LP(f'_ig_i)$，$i=1,\cdots,l+1$，由 f 的首一性与首项条件知 $f'_{l+1}=1$。显然 $LP(f-g_{l+1})<_T LP(g_{l+1})$，再由定理 4 即可推知本定理。

四、模型 III 的求解算法和综合问题的求解

下面是比模型 III 更一般的 Syzygy 复形计算[4]。

Syzygy 问题 设 $f_1,\cdots,f_m$ 为 $F[x_1,\cdots x_n]$ 中齐次多项式，求 m 列多项式矩阵 R，使 R 的行构成方程

$$h_1f_1+\cdots+h_mf_m=0$$

$$\sigma(E_i)=0,\ i=1,\cdots,s \tag{13}$$

$$\sum_{i=1}^{n} e_i\sigma(P_i)=0 \tag{14}$$

设　　$$f_{b,i,j}=y^iz^jx^{b-(i+j)},\ 0\leqslant i\leqslant b,\ 0\leqslant j\leqslant b-i \tag{15}$$

显然，$\{f_{b,i,j}\}$ 构成 V_b 空间的基．定义

$$s_{ij}=S(r,y^iz^jx^{T-(i+j)})=\sum_{u=1}^{n} r_uf_{T,i,j}(P_u)=\sum_{u=1}^{n} e_uf_{T,i,j}(P_u) \tag{16}$$

是伴随式．设 $s(x,y,z)$ 是伴随式母函数，即

$$s(x,y,z)=\sum_{i=0}^{T}\sum_{j=0}^{T-i} s_{ij}y^iz^jx^{T-(i+j)} \tag{17}$$

现已知 $s(x,y,z)$，欲求次数最小的错误位置多项式 $\sigma(x,y,z)$，进而求出错误向量 e．

设 I 是 $F[x,y,z]$ 中由 x^{T+1},y^{T+1},z^{T+1} 生成的齐次理想，设 $H(x,y,z)=(xyz)^Ts(1/x,1/y,1/z)$ 是一个 $2T$ 次齐次多项式，是已知的．

定理 10　设 $\sigma(x,y,z)$ 是齐次错误位置多项式，则

$$\sigma(x,y,z)H(x,y,z)\equiv 0\ \mathrm{mod}I \tag{18}$$

证明　较复杂，因篇幅所限，故从略．

定理 11　设 a 次齐次多项式满足

$$\sigma(x,y,z)H(x,y,z)\equiv 0\ \mathrm{mod}I$$

且若错误个数 $s=\mathrm{weight}(e)<(T-a)m-2g+2$，则 $\sigma(x,y,z)$ 必是错误位置多项式．

证明　较复杂，从略．

由上述两定理知，可用模型 III 来刻划译码问题．用算法 2 给出译码算法，此时，$K=\{H(x,y,z),\ x^{T+1},\ y^{T+1},\ z^{T+1}\}$．算法的复杂性主要由求 K 的 Gröbner 基的复杂性决定．文献 [7] 指出，其复杂性是 $O(n^2)$．

六、结　束　语

本文用齐次多项式理论来刻划序列综合问题．这开辟了研究这类问题的新途径．我们认为这抓住了问题的实质．这一方法可望推广到一般交换 Noether 环上序列的综合，以及对其它种类的代数编码的快速译码．在密码分析中也可能有重要的应用．

参　考　文　献

[1] 冯贵良等，中国科学，A 辑，1985 年，第 8 期，第 1—12 页．
[2] J. Justesen et al., *IEEE Trans. on IT*, **IT-35**(1989)4, 811—821.
[3] A. N. Skorobogatov et al., *IEEE Trans. on IT*, **IT-36**(1990)5, 1051—1061.
[4] O. Zariski, Commutative Algebra II, Springer-Verlag, New York, (1960), pp 192—250.
[5] B. Buchberger, Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory, in Multidimensional Systems Theory, Ed. by N. K. Bose, Springer-Verlag, Berlin, (1984), pp. 184—232.
[6] H. Moller, *J. Algebra*, **100**(1986), 138—178.
[7] S. Sakata, *IEEE Trans. on IT*, **IT-37**(1991)4, 1200—1203.

SYNTHESIS OF MULTISEQUENCES AND THEIR APPLICATIONS

Lu Peizhong Song Guowen

(Chengdu Institute of Telecommunication Technique, Chengdu 610031)

Zhou Jinjun

(Zhengzhou Institute of Information Engineering, Zhengzhou 450002)

Abstract A new mathematical model, the linear homogeneous equations with polynomial coefficients for describing the synthesis problem, is presented in this paper. It gives a nature approach to generalize the linear synthesis to nonlinear case. This method is used to obtain a new solution for the multisequence synthesis. The Gröbner bases theory in polynomial ring is used to present an efficient algorithm for the mathematical model. This turns out to be a generalization of Euclid' algorithm. However, the new one has much brilliant prospects. As one of the important results, it is discovered that the new algorithm can be used to deduce an efficient decoding algorithm for a class of algebraic geometry codes constructed by Justesen, so the important open problem is solved.

Key words Synthesis of sequence; Homogeneous ideal; Gröbner base; Algebra geometry code; Error-locator polynomial