无误差多项式矩阵计算

蒋昌俊
闫春钢
编著

123··

安徽科学技术出版社

无误差多项式矩阵计算

蒋昌俊　闻春钢　编著
吴哲辉　主审

安徽科学技术出版社

(皖)新登字02号

责任编辑：杨家骊
责任校对：杨小红

无误差多项式矩阵计算
蒋昌俊　阎春钢　编著
•
安徽科学技术出版社出版
（合肥市九州大厦八楼）
邮政编码：230063
安徽省新华书店经销　　安徽少管所印刷厂印刷
•
开本：787×1092　1/32　印张：7.75　字数：163000
1993年11月第一版　　1993年11月第一次印刷
印数：1000
ISBN7—5337—0936—5／N·11　　定价：6.40元

前　言

无误差计算属于计算机科学中最近才发展起来的一个分支——计算机代数. 它的处理方法与过去用计算机进行数值计算而采取的近似计算是根本不同的. 我国在计算机代数方面的研究工作刚刚开始，有关资料很少，正式出版的著作仅见到《计算机代数》(裘仁保编著，国防科学技术大学出版社，1989)一书，每年发表的文章也不过数篇. 有关工作者深感资料匮乏，不利于开展研究. 为此，我们编写了本书，希望为国内从事计算机代数研究的同行提供一点帮助.

本书主要讨论多项式矩阵方面的无误差计算方法，前五章主要取材于 Error-Free Polynomial Matrix Computation (E. V. Krishnamurthy 著)一书，后两章主要是我们近几年的工作.

我们在编写过程中，中国 Petri 网研究会副理事长、中国袖珍机用户协会常务理事、山东省计算机学会理事、山东矿业学院应用数学与软件工程系主任吴哲辉教授曾给予热情帮助与指导，并审阅了全部稿件，付出了辛勤的劳动. 在此，谨表示衷心的感谢. 本书的出版，得到了国家自然科学基金的资助.

蒋昌俊　闻春钢

1992年10月

符号简介

A^-	矩阵 A 的一个 g-逆
A^{-1}	矩阵 A 的逆
A_L^-	矩阵 A 的一个最小平方 g-逆
A_M^-	矩阵 A 的一个极小范数 g-逆
A_R^-	矩阵 A 的一个自反 g-逆
A^T	矩阵 A 的转置
A^+	矩阵 A 的 Moore-Penrose 逆
$A(x)$	一元多项式矩阵 A
$A(x_1, x_2, \cdots, x_n)$	多元多项式矩阵 A
$A \cong B$	A 同构(或等价)于 B
(A, P)	具有元素 A 和运算 P 的代数系统
$a \to b$	a 到 b 的赋值
$a \mid b$	a 除 b
$[a/b]$	a/b 商的整数部分
$\lvert a \rvert_m$	a 被 m 除的非负余数
$a \equiv_m b$ 或 $a \equiv \lvert b \rvert_m$ 或 $a = b \bmod m$	a 与 b 模 m 同余
$a(x) \bmod m(x)$	$a(x)$ 被 $m(x)$ 除的余式
$a(x)^{-1}$	域 F 上 $a(x)$ 的逆变换
$\mathrm{adj}A$	矩阵 A 的伴随阵
D	整区
$\deg a(x)$	$a(x)$ 的次数
$\det A$	矩阵 A 的行列式
DFT	离散傅立叶变换

F	域
FFT	快速傅立叶变换
F_N	N 阶法瑞函数的集合
$F[x]$	域 F 上的有理函数
$F[[x]]$	域 F 上的形式幂级数
$F((x))$	域 F 上幂级数有理函数
$F\langle x\rangle$	域 F 上广义形式幂级数
$F_p(x)$	有限域$(Z_p, +, \cdot)$上的有理多项式的集合
$F_p((x))$	$(Z_p, +, \cdot)$上的幂级数有理函数
$F[x_1, x_2, \cdots, x_n]$	域 F 上的多元多项式
$F(x_1, x_2, \cdots, x_n)$	域 F 上的多元有理多项式
$F[[x_1, x_2, \cdots, x_n]]$	域 F 上的多元形式幂级数
$F((x_1, x_2, \cdots, x_n))$	域 F 上的多元幂级数有理函数
$F\langle x_1, x_2, \cdots, x_n\rangle$	域 F 上的多元广义幂级数
$F_p(x_1, x_2, \cdots, x_n)$	有限域$(Z_p, +, \cdot)$上的多元有理多项式
$F_p((x_1, x_2, \cdots, x_n))$	有限域$(Z_p, +, \cdot)$上的幂级数有理函数
G	群
$\gcd(a, b)$	a 和 b 的最大公约数
$H(P, r, \alpha)$	有理数 α 的汉塞尔码
$H(P, r, \alpha(x))$	有限域$(Z_p, +, \cdot)$上的有理多项式 $\alpha(x)$ 的汉塞尔码
$H(P, r, \alpha(x_1, \cdots x_n))$	有限域$(Z_p, +, \cdot)$上的多元有理多项式$\alpha(x_1, x_2, \cdots, x_n)$的汉塞尔码
Z	整数集
$Z[x]$	Z 上的多项式
$Z[x_1, x_2, \cdots, x_n]$	Z 上的多元多项式
$Z/(m)$	整数模 m 的商环
Z_p	整数模 p 的剩余类$\{0, 1, 2, \cdots, p-1\}$
$Z_p[x]$	有限域$(Z_p, +, \cdot)$上的多项式
$Z_p[[x]]$	有限域$(Z_p, +, \cdot)$上的幂级数

$Z_p[x_1, x_2, \cdots, x_n]$	有限域$(Z_p, +, \cdot)$上的多元多项式
$Z_p[[x_1, x_2, \cdots, x_n]]$	有限域$(Z_p, +, \cdot)$上的多元幂级数
$\mathrm{lcm}(a, b)$	a和b的最小公倍数
N	非负整数集
NTT	数论变换
$o(r)$	次数$\geqslant r$的项的舍位
$\mathrm{ord}_a(x)$	$a(x)$的阶
$P(L/M, F_p(x))$	满足分子次数$\leqslant L$和分母次数$\leqslant M$的有限域$(Z_p, +, \cdot)$上关于x的Padé有理多项式
$P(L/M, N, x)$	满足系数$\leqslant N$和分子次数$\leqslant L$及分母次数$\leqslant M$的整数集上关于x的Padé有理多项式
$P(L_1, \cdots, L_n/M_1, \cdots, M_n, F_p(x_1, \cdots, x_n))$	有限域$(Z_p, +, \cdot)$上多元Padé有理多项式，这里x_i的分子多项式次数$\leqslant L_i$及分母多项式次数$\leqslant M_i$
$P(L_1, \cdots, L_n/M_1, \cdots, M_n, N, x_1, \cdots, x_n)$	整数集上多元Padé有理多项式，这里系数$\leqslant N$和x_i的分子多项式次数$\leqslant L_i$，分母多项式次数$\leqslant M_i$
Q	有理数集合
$Q(D)$	D的商域
Q_p	p-进制数的集合
$Q(x)$	有理数域Q上有理多项式
$Q(x_1, x_2, \cdots, x_n)$	有理数域Q上多元有理多项式
R	环
$R[x]$	环R上多项式
$R[x]_{m(x)}$	模$m(x)$的多项式环
$R[x]/m(x)$	模$m(x)$的多项式商环
$R[[x]]$	环R上的幂级数
$R[[x]]_m$	次数为m的舍位幂级数环
$R[[x]]/(x^m)$	幂级数模x^m的商环
$R[x_1, x_2, \cdots, x_n]$	n个变量$x_1, x_2, \cdots, x_n$的多项式环

S_m	$\{-(m-1)/2, \cdots, -1, 0, 1, \cdots (m-1)/2\}$ 对称剩余集
$v(A)$	将 $m \times n$ 矩阵 A 所有 m 行首尾相连，第一行在最左边，最后一行在最右边所形成的 $mn \times 1$ 行向量的转置所得到的列向量
$\in$	属于
$\notin$	不属于
$\phi(\cdot)$	范数
$\phi(m)$	欧拉函数
$\prod_{i=1}^{n}$	求积符号
$\sum_{i=1}^{n}$	求和符号
ω	本原根
$\otimes$	矩阵的张量积(或直积，Kronecker 积)
$*$	卷积

目　录

第一章 基本概念

本章将介绍在抽象代数和计算多项式矩阵代数之间起桥梁作用的某些基本概念. 所用的背景材料大都属于抽象代数范畴. 我们假设读者熟悉这些内容. 这些结果在代数及相关的通用教课书中都可以找到. 读者可参看 Albert(1956), Berlekamp (1968), Childs (1979), Jacobson (1976), Lipson (1981), Zariski and Samuel(1975)等撰写的著作. 下面我们将很快地复习一下这些结果, 并不加证明地陈述一些定理. 读者可从上面列出的教课书中找到详细的证明.

§1 群、环、整区和域

1.1 群

一个含有元素 a, b, c … 的集合 G 称为关于某个二元运算, 譬如乘法(记为·)构成一个群:

(i) 对 $\forall a, b \in G$, 都有 $a \cdot b \in G$(封闭性);

(ii) 对 $\forall a, b, c \in G$, 有 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$(结合律);

(iii) G 中有一元 e, 使对 $\forall a \in G$, 总有 $a \cdot e = e \cdot a = a$, 这个 e 叫做 G 的单位元;

(iv) 对 $\forall a \in G$, 在 G 中能找到一个元 b, 使 $b \cdot a = e = a \cdot b$, 这个元 b 叫做 a 的逆元, 记作 $b = a^{-1}$.

因为在有些群中，运算“·”不一定是可换的，而在有些群中，“·”是可换的，所以定义中并没有规定 $a\cdot b=b\cdot a$. 如果 $\forall a, b\in G$，都有 $a\cdot b=b\cdot a$，则称 G 是可换群或称 Abel 群.

例　考虑模 p 整数集 Z_p，这里 p 是一个素数，在 Z_p 中，加法(+)按照在整数集 Z 中执行加法所得的结果再除 p 后所得的余数，就是其运算的结果(用模 p 或 mod p). 注意 $(Z_p, +)$ 是一个以 0 为单位元的 Abel 群，而且对 $\forall a\in\{0,1,\cdots,p-1\}$，则 $p-a$ 是它的加法逆元.

1.2　环

一个环 $(R, +, \times)$ 是这样一个集合，对于两种二元运算 $+$，$\times$ 封闭，使得 $(R, +)$ 是一个 Abel 群，对 $\times$ 满足结合律且有一个单位元(表示为 1)，对 $\forall a, b, c\in R$，“+”与“×”联合运算时满足两个分配律：

$$a\times(b+c)=(a\times b)+(a\times c)$$
$$(a+b)\times c=(a\times c)+(b\times c)$$

我们将加法的单位元表示为 0，a 对加法的逆元表示为 $-a$.

1.2.1　可换性

一个环称为可换的，如果对所有的 $a, b\in R$，都有 $a\times b=b\times a$.

1.2.2　零因子

R 中的一个非零元素 a 称为零因子，如果存在 $b\neq 0$，$b\in R$，使得 $a\times b=0$(对称地 b 也是一个零因子).

1.2.3　单位

R 中的非零元素 u 称为一个单位，如果它是可逆的，即存在 $v\in R$，使得 $u\times v=1$. 我们记 $v=u^{-1}$.

1.2.4 除环

一个环 R 称为除环 R^*，如果 $R^*=(R-\{0\})$ 关于 $\times$ 是一个群.

例 考虑模 m 的整数集 Z_m，这里 m 是一个正整数，在 Z_m 中，加法(+)和乘法(×)按照在整数集 Z 中执行加法和乘法.但所有数 y 由 y 除以 m 后所得的余数代替($y \bmod m$). 这是一个对加法以 0 为单位元，对乘法以 1 为单位元的可换环. 特别地，考虑 Z_6，我们有 $2\times3=0$ 因此 Z_6 是一个具有零因子环，而且 1 和 5 都是单位，因为它们是可逆的，且 $1^{-1}=1$，$5^{-1}=5$.

1.3 整区

一个整区 D 是一个不具有零因子($a\times b=0$ 意味着 $a=0$ 或 $b=0$)的可换环，意味着对 $\forall a, b, c\in D$，$a\times b=a\times c$ 且 $a\neq0$ 必有 $b=c$，或者说满足消去律.

1.3.1 可除性

在 D 中，我们说 a 可以由 b 整除(或 b 整除 a，表示为 $b|a$)，指的是如果存在元素 $c\in D$，使得 $a=b\times c$，我们也说 a 是 b 的倍数和 b 是 a 的因子.

1.3.2 单位

如果 u 在 D 中整除 D 的单位元 1，则 u 称为 D 的一个单位. 如果在 D 中 u 有一个逆元，则 u 是 D 的一个可逆元(单位). 一个单位的逆元也是一个单位.

1.3.3 相伴的

两个元素 $a, b\in D^*$(这里 $D^*=(D-\{0\})$)，被称为相伴的，指的是如果 $a=u\times b$，其中 u 是 D 的一个单位. 这种相伴性是 D^* 上的一个等价关系.

1.3.4 因子

b 的一个因子 a 被称为 b 的一个真因子，指的是如果 a 既不是一个单位也不是与 b 相伴的.

1.3.5 素数

整区 D 的一个量 p 称为素数或不可约量，指的是如果 $p \neq 0$ 是 D 的一个非单位且在 D 中 p 的因子只有单位和 p 的相伴元. 一个素数的每个相伴元是一个素数.

1.3.6 合数

D 的一个合数 $a(\neq 0)$ 是一个既非素数也非 D 的单位.

1.3.7 最大公因子

对于 a, $b \in D$, 元素 $c \in D$ 被称为 a 和 b 的最大公因子(gcd)，指的是如果 $c \mid a$, $c \mid b$ 且 c 是 a 和 b 的任何其它公因子的倍数.

1.3.8 最小公倍数

对于 a $b \in D$, 元素 $c \in D$ 称为 a 和 b 的最小公倍数(lcm)，指的是如果 $a \mid c$, $b \mid c$ 且 c 是 a 和 b 的任何其它公倍数的因子.

1.3.9 互素

我们称两个元素 a, $b \in D$ 是互素的，指的是如果 $\gcd(a, b) = 1$.

例 整数集 Z 连同加法(+)和乘法(×)构成一个整区.

(i) 1 和 −1 都是单位;

(ii) 3 是 9 和 12 的最大公因子;

(iii) −3 也是 9 和 12 的最大公因子;

(iv) 3 和 −3 是相伴的;

(v) 3 和 14 是互素的;

(vi) 19 和 −19 都是素数;

(vii) 18 是一个合数.

现在自然要问是否 D 的每一个合数 a 都可以写成 D 中有限个素数积的形式 $a=p_1\times p_2\times\cdots\times p_k$.

1.4 唯一分解区

一个整区 D 称为唯一分解区，指的是如果对所有的 $a\in D^*$，a 或者是一个单位或者 a 可以表示为有限个素数的积(即：$a=p_1\times p_2\times\cdots\times p_k$)，使得这些素因子在相伴和重排意义下是唯一的(即，如果 $a=p_1\times p_2\times\cdots\times p_k$ 和 $a=q_1\times q_2\times\cdots\times q_m$，这里 p_i $(1\leqslant i\leqslant k)$，和 $q_j(1\leqslant j\leqslant m)$都是素数，则 $k=m$ 且存在 q_j 的一个重排使得 p_i 是 q_i 的一个相伴元$(1\leqslant i\leqslant k)$).

1.4.1 定理

如果 D 是唯一分解区且 a，$b\in D$ 都是非零因子，则 $\gcd(a,b)$存在且唯一.

以上定理保证了最大公因子的存在且唯一.

1.4.2 D 中唯一最大公因子的选择

在 D 中，两元素 c 和 d 是相伴的当且仅当存在可逆元 u，使得 $c\times u=d$(通常表示为 cu). 如果 c 是 a 和 b 的最大公因子，则 c 的任何相伴元 $d=cu$ 也是 a、b 的最大公因子. 相反地，如果 c 和 d 都是 a 和 b 的最大公因子，则 c 必定是 d 的一个相伴元.

为了使最大公因子唯一，我们必须增加另外一个条件. 由于相伴性(或相伴关系)是一个等价关系，对 $\forall a\in D^*$，它将 D^* 划分为相伴元的等价类. 若我们用 $[a]=\{ua\mid u\in U(D)\}$ 表示这种等价类，这里 $U(D)$为 D 的可逆元构成的群，在这种等价类中，我们可以通过约定，在每一类中选出一个特定的代表，我们

把任何一个元素表示为：

$$a=\triangle(a)u(a)$$

这里 $\triangle(a)$ 表示包含 a 的相伴类的特定代表，$u(a)$ 表示对应的单位，这样我们就能选择 $\triangle(a)$ 为唯一的特定代表.

例 (i) 在 Z 中我们有

$$\triangle(a)=|a|,\ u(a)=\mathrm{sgn}(a),$$

$$\mathrm{sgn}(a)=\begin{cases}-1 & a<0\\ +1 & a\geqslant 0\end{cases}$$

(ii) 在任何一般整区 D 中，我们选择单位元为 $[u]$ 的特定代表，这里 u 是一个单位.

1.4.3 最小公倍数的唯一性

任何两个元素 a、$b\in D$，当它们的最小公倍数存在时，可以通过唯一的最大公约数来确定. 因为

$$\mathrm{lcm}(a,\ b)=\frac{a\cdot b}{\gcd(a,\ b)}$$

1.5 欧几里德整区

一个整区 D 称为欧几里德整区，指的是如果存在一个映射（也称欧几里德度函数）v: $D-\{0\}\to N$（非负整数集），具有下列性质：

(i) 对所有 a、$b\in D-\{0\}$，$v(ab)\geqslant v(a)$；

(ii) 对所有 a、$b\in D$ 且 $b\neq 0$，存在元素 q、$r\in D$，使得 $a=bq+r$，这里 $r=0$ 或 $v(r)<v(b)$；

(iii) 任何欧几里德整区是这样一个整区，每对不全为零的元素 $(a,\ b)$，都有一个最大公因子 $g(\gcd)$，它可表示为

$$g=sa+tb\quad (s,\ t\in D)$$

例 1 在 Z 中，$\gcd(8, 20)=4$，我们有

$$4=s(8)+t(20)$$

这里 $s=-2$，$t=1$.

1.5.1 求最大公因子的推广的欧几里德算法(EEA)

求最大公因子 $g=\gcd(a, b)$ 的推广的欧几里德算法（第1章§5，Gregory 和 Krishnamurthy[1984]）以及计算 $s, t\in D$，使得 $g=sa+tb$（需要详细地讨论请参看 Knuth [1981]，Lipson[1981]）. 我们分别就 $D=Z$（整数集）及一般的 D 的情况进行讨论：

在 $D=Z$（整数集）的情况下，为了求一对整数 s 和 t，满足

$$sa+tb=g$$

我们重复应用欧几里德辗转除法如下：

令

$$r_1=a+b(-q_1)$$

$$r_2=b+r_1(-q_2)=a(-q_2)+b(1+q_1q_2)$$

$$r_3=r_1+r_2(-q_3)=a(1+q_2q_3)+b(-q_1-q_3-q_1q_2q_3)$$

$$\vdots$$

$$r_n=r_{n-2}+r_{n-1}(-q_n)=sa+tb$$

$$0=r_{n-1}+r_n(-q_{n+1})=xa+yb$$

上面计算能够被表达为如下的表格形式：

	a	1	0
	b	0	1
q_1	r_1	1	$-q_1$
q_2	r_2	$-q_2$	$1+q_1q_2$
q_3	r_3	$1+q_2q_3$	$-q_1-q_3-q_1q_2q_3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
q_n	r_n	s	t
q_{n+1}	0	x	y