本资源来自数缘社区

http://maths.utime.cn:81

欢迎来到数缘社区。本社区是一个高等数学及密码学的技术性论坛，由山东大学数学院研究生创办。在这里您可以尽情的遨游数学的海洋。作为站长，我诚挚的邀请您加入，希望大家能一起支持发展我们的论坛，充实每个版块。把您宝贵的资料与大家一起分享！

数学电子书库

每天都有来源于各类网站的与数学相关的新内容供大家浏览和下载，您既可以点击左键弹出网页在线阅读，又可以点右键选择下载。现在书库中藏书 1000 余本。如果本站没有您急需的电子书，可以发帖说明，我们有专人负责为您寻找您需要的电子书。

密码学论文库

国内首创信息安全专业的密码学论文库，主要收集欧密会（Eurocrypt）、美密会（Crypto）、亚密会（Asiacrypt）等国内外知名论文。现在论文库中收藏论文 4000 余篇（包括论文库版块 700 余篇、论坛顶部菜单“密码学会议论文集”3000 余篇）。如果本站没有您急需的密码学论文，可以发帖说明，我们有专人负责为您寻找您需要的论文。

提示：本站已经收集到 1981－2003 年欧密会、美密会全部论文以及 1997 年－2003 年五大会议全部论文（欧密会、美密会、亚密会、PKC、FSE）。

数学综合讨论区

论坛管理团队及部分会员来源于山东大学数学院七大专业（基础数学、应用数学、运筹学、控制论、计算数学、统计学、信息安全），在数学方面均为思维活跃、成绩优秀的研究生，相信会给您的数学学习带来很大的帮助。

密码学与网络安全

山东大学数学院的信息安全专业师资雄厚，前景广阔，具有密码理论、密码技术与网络安全技术三个研究方向。有一大批博士、硕士及本科生活跃于本论坛。本版块适合从事密码学或网络安全方面学习研究的朋友访问。

网络公式编辑器

数缘社区公式编辑器采用 Latex 语言，适用于任何支持图片格式的论坛或网页。在本论坛编辑好公式后，您可以将自动生成的公式图片的链接直接复制到你要发的帖子里以图片的形式发表。

如果您觉得本站对您的学习和成长有所帮助，请把它添加到您的收藏夹。如果您对本论坛有任何的意见或者建议，请来论坛留下您宝贵的意见。

附录 A：本站电子书库藏书目录

http://maths.utime.cn:81/bbs/dispbbs.asp?boardID=18&ID=2285

附录 B：版权问题

XIANXING YIWEI JICUNQI-XULIE

线性移位寄存器序列

丁 石 孙

上海科学技术出版社

科技新书目：1-8-1-0-5
统一书号：13119·973
定　　价：(0.30)0.40元

线性移位寄存器序列

丁石孙

上海科学技术出版社

线性移位寄存器序列

丁 石 孙

上海科学技术出版社出版

（上海瑞金二路450号）

新华书店上海发行所发行　无锡县人民印刷厂印刷

开本787×1092 1/32　印张3.875　字数83,000

1982年 2月第1版　1982年 2月第1次印刷

印数 1—4,200

统一书号：13119·979　　定价：(科五) 0.50 元

前　言

关于线性移位寄存器序列，现在已经有了一个相当完整的理论。这个理论是代数学，特别是线性代数与有限域理论的一个极好的应用。因此，它是应用代数学的一个很有趣的部分，不但有关的工程技术人员需要了解它，就是对于代数工作者，也是有吸引力的。

随着电子通讯技术的发展，线性移位寄存器序列逐步受到了人们的重视，有关的文献已有不少。作为书的形式对它进行系统讨论的首先是 S. Golomb 的«Shift Register Sequences» (Holden-Dag, San Francisco, U. S. A. 1967)。在万哲先编著的«代数和编码»(科学出版社，1976)中，对它也作了比较详细的讨论。这两本书收集的材料是丰富的，对于要了解这方面知识的同志是很有用的。不过对线性移位寄存器序列的讨论，在这两本书中，只是其中的一部分，它们都还讨论了许多其它的问题。因此，用不大的篇幅专门对线性移位寄存器序列作一系统的介绍，对某些读者还是很有必要的。

在线性移位寄存器序列的研究中，需要作进一步讨论并且还没有完全解决的问题是不少的，但作为一本介绍基本知识的书，我们不打算涉及这些问题。为了进一步研究解决有关的问题，本书将提供必要的准备。本书在处理上突出了线性代数的方法，这样会使整个理论显得更单纯些。

本书分成四章。第一章介绍线性移位寄存器序列的数学描述及其基本性质。第二章讨论最常用的极大周期序列（即

伪随机序列）的性质. 第三章讨论线性移位寄存器序列的综合问题，介绍了 J. L. Massey 在文章 Shift-Register Synthesis and BCH Decoding, IEEE Trans. on Information Theory 15(1969)122～127 中给出的迭代算法. 第四章介绍线性自动机的基本概念. 这是讨论线性移位寄存器序列的一个自然的继续与必要的推广. 在讨论中，我们用到了矩阵的有理标准形，但在一般的代数教本中有理标准形谈得较少，因此，我们写了一个附录. 此外，还把 Wayne Stahnke 所作的本原多项式的表(1973)作为另一个附录收在书中.

我们假定读者有一定的代数知识. 这些知识可参看《高等代数》(北京大学数学力学系几何与代数教研室代数小组编，人民教育出版社，1978 年)与《代数和编码》(万哲先著)中的有关章节.

在本书的准备过程中，作者得到了万哲先、聂灵沼、代宗锋、冯绪宁、刘木兰等同志的帮助，在此表示衷心感谢.

丁石孙　1980 年 8 月于北京大学

目　录

第一章　线性递推序列

§1　引言

近二十年来，利用反馈移位寄存器来产生0,1序列得到了广泛的应用，因此，对这样的0,1序列的性质的研究日益受到人们重视，它们通常称为移位寄存器序列．我们知道，n位反馈移位寄存器的逻辑功能可以用图1-1来表示．图中x_i表示寄存器$\square$所处的状态，通常用0与1来代表两个可能的状态，并且把0与1看成特征为2的素域$GF(2)$的两个元素．$f(x_0, x_1, \cdots, x_{n-1})$刻划了移位寄存器的逻辑线路的功能，它可以看成一个定义在$GF(2)$上并且在$GF(2)$中取值的n元函数．当$f(x_0, x_1, \cdots, x_{n-1})$可以表成一线性齐次函数时，即

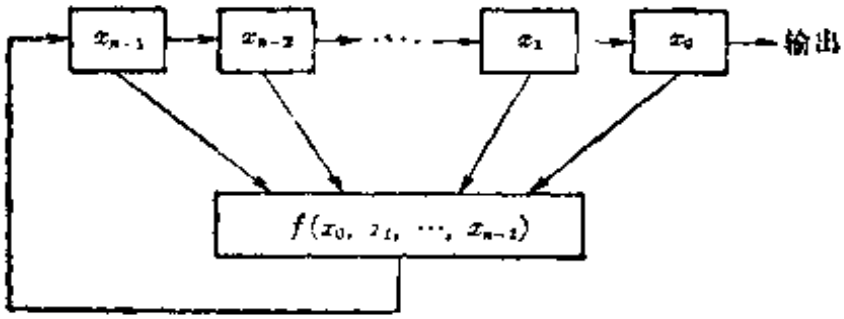
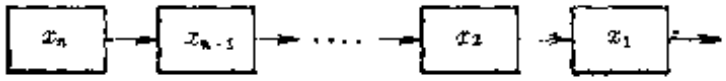


图　1-1

$$f(x_0, x_1, \cdots, x_{n-1}) = \sum_{i=0}^{n-1} c_i x_i, \quad c_i \in GF(2),$$

相应的反馈移位寄存器就称为线性的（以下简称线性移位寄存器）。

每加一个移位脉冲，寄存器中每一位的内容都向右移一位，最右边一位的内容移出来作为输出，而$f(x_0, x_1, \cdots, x_{n-1})$反馈到最左边的一位．比如说，在第一次移位脉冲之后，移位寄存器的状态变成：



其中

$$x_n = f(x_0, x_1, \cdots, x_{n-1}).$$

不断加上移位脉冲，一个 n 位线性移位寄存器的输出就成一个序列

$$x_0, x_1, x_2, \cdots, x_n, \cdots. \tag{1}$$

显然，这个序列适合关系式

$$x_{n+k} = \sum_{i=0}^{n-1} c_i x_{k+i} \quad (k = 0, 1, 2, \cdots). \tag{2}$$

这样由线性移位寄存器产生的序列就称为线性移位寄存器序列．它就是我们要讨论的主要对象．函数

$$f(x_0, x_1, \cdots, x_{n-1}) = \sum_{i=0}^{n-1} c_i x_i \tag{3}$$

完全刻划了一个线性移位寄存器的反馈功能，它通常称为线性移位寄存器的反馈函数(或反馈逻辑)．线性移位寄存器序列(1)中任意 n 位连续的项

$$x_k, x_{k+1}, \cdots, x_{k+n-1}$$

都表示线性移位寄存器在某一时刻的内部状态，因之，我们把这样得到的 n 元数组

$$(x_k, x_{k+1}, \cdots, x_{k+n-1}) \quad (k = 0, 1, 2, \cdots)$$

称为序列(1)的状态，而$(x_0, x_1, \cdots, x_{n-1})$称为初始状态．不难看出，初始状态与反馈函数完全决定一个线性移位寄存器

序列，弄清三者间的相互关系是我们讨论中的一个重要问题.

在这一章，我们将给出线性移位寄存器序列的一个适当的数学定义，随后逐步引入一些必要的数学工具. 利用这些数学工具我们将得出线性移位寄存器序列的一些基本性质.

应该指出：在实际使用中，线性移位寄存器序列都是有限长的. 但是在不同的情况下，使用的序列的长度不同，而且随着科学技术的发展，使用序列的长度不断增加. 为了便于作数学上统一的讨论与研究，以下我们总是把线性移位寄存器序列看成无限长的.

§2 线性递推序列的定义

作为线性移位寄存器序列的数学抽象，在这一节，我们引入线性递推序列的概念，同时也引入有关的符号. 虽然线性递推序列的概念可以在任意的有限域（甚至于在任意域）中定义，但是为了讨论起来更具体些，我们把讨论限制在特征为2的素域 $GF(2)$ 中进行. 当然，这也是考虑到 $GF(2)$ 在应用中所具有的特殊重要性. 事实上，这样作并不损害讨论方法的普遍性，读者将会发现，把本章的结果推广到任意有限域上去，只是一个不难的练习. 为了书写简单，以下我们用 F 代表域 $GF(2)$.

由 F 中的元素组成的无限序列

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots)\quad (a_i\in F)$$

称为 F 上的无限序列. 以下我们用黑体小写拉丁字母代表 F 上的无限序列.

在 F 上的无限序列之间可以定义加法与数量乘法. 设

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots),$$
$$\mathbf{b}=(b_0,\ b_1,\ b_2,\ \cdots)$$

是任意两个 F 上的无限序列，$c\in F$，我们定义

$$\mathbf{a}+\mathbf{b}=(a_0+b_0,\ a_1+b_1,\ a_2+b_2,\ \cdots),$$

$$c\mathbf{a}=(ca_0,\ ca_1,\ ca_2,\ \cdots).$$

不难验证，F 上无限序列的全体在这两个运算之下成为域 F 上的一个线性空间．把这个线性空间记为 $V(F)$．

显然，$V(F)$中的零元素就是全零序列$(0,\ 0,\ 0,\ \cdots)$，这个序列我们有时就简单地记为 $\mathbf{0}$．

$V(F)$中的无限序列

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots)$$

称为**一线性递推序列**，如果序列中的项 $a_0,\ a_1,\ a_2,\ \cdots$适合一线性递推关系式

$$a_{k+n}=\sum_{i=0}^{n-1}c_ia_{k+i}\quad(k=0,\ 1,\ 2,\ \cdots).\tag{1}$$

例如，无限序列

$$(0,\ 1,\ 1,\ 0,\ 1,\ 1,\ \cdots)$$

即由 0，1，1 无限重复组成的序列，适合关系式

$$a_{k+2}=a_k+a_{k+1}\quad(k=0,\ 1,\ 2,\ \cdots),$$

因之，它是一线性递推序列．

很明显，线性递推序列不过是线性移位寄存器序列的一个数学的说法．

为了以下讨论方便，我们把线性递推序列的定义换一种说法：在线性空间 $V(F)$中，我们定义一**左移变换** L．对于 $V(F)$中的无限序列

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots),$$

定义

$$L\mathbf{a}=(a_1,\ a_2,\ a_3,\ \cdots),$$

这就是说，L 的作用是把 $\mathbf{a}$ 的分量全向左移一位，把第一位去掉．容易验证，L 是 $V(F)$的一个线性变换．显然，

$$L^2\mathbf{a}=L(L\mathbf{a})=(a_2,\ a_3,\ \cdots).$$

一般地，对任意的正整数 r，有

$$L^r\mathbf{a}=(a_r,\ a_{r+1},\ \cdots).$$

利用左移变换 L，关系式(1)可以改写为

$$L^n\mathbf{a}=\sum_{i=0}^{n-1}c_iL^i\mathbf{a},$$

或者

$$\left(L^n-\sum_{i=0}^{n-1}c_iL^i\right)\mathbf{a}=\mathbf{0}. \tag{2}$$

取一文字 λ，作 λ 的多项式环 $F[\lambda]$. 我们知道，对于 $F[\lambda]$ 中的任一多项式

$$f(\lambda)=c_n\lambda^n+c_{n-1}\lambda^{n-1}+\cdots+c_0,$$

有

$$f(L)=c_nL^n+c_{n-1}L^{n-1}+\cdots+c_0I,$$

这里 I 代表 $V(F)$ 的单位变换. $f(L)$ 也是 $V(F)$ 的一个线性变换.

根据(2)，线性递推序列的定义可以改为：对于 $V(F)$ 中的无限序列 $\mathbf{a}$，如果有 $F[\lambda]$ 中的一个非零多项式 $f(\lambda)$ 使

$$f(L)\mathbf{a}=\mathbf{0},$$

那么 $\mathbf{a}$ 就称为一线性递推序列.

多项式环 $F[\lambda]$ 的性质我们是比较清楚的，这样一个定义的好处就在于使我们能够把线性递推序列的许多讨论归结为多项式的讨论.

对于 $F[\lambda]$ 中的任一多项式 $f(\lambda)$，我们用记号 $G(f(\lambda))$ (或 $G(f)$)表示 $V(F)$ 中所有适合条件

$$f(L)\mathbf{a}=\mathbf{0}$$

的无限序列 $\mathbf{a}$ 组成的集合. 因为 $f(L)$ 是一线性变换，所以容易验证，$G(f)$ 是 $V(F)$ 的一个线性子空间.

由 $f(L)\mathbf{a}=\mathbf{0}$，显然有

$$f(L)(L\mathbf{a}) - Lf(L)\mathbf{a} = \mathbf{0}.$$

这就表明，$G(f)$不但是一个子空间，而且是线性变换 L 的一个不变子空间.

设 $$f(\lambda) = \lambda^n + c_{n-1}\lambda^{n-1} + \cdots + c_0$$

是一 n 次多项式(因为 F 只有两个元素，所以总可以认为最高次项的系数是 1). 正如上面指出的，$f(L)\mathbf{a} = \mathbf{0}$ 不过是递推关系式(1)的另一种写法，因之对于 $G(f)$ 中的序列

$$\mathbf{a} = (a_0, a_1, \cdots, a_{n-1}, a_n, \cdots),$$

只要给定了前 n 个分量 $(a_0, a_1, \cdots, a_{n-1})$，其余的分量，从 a_n 开始就逐个的、唯一的被决定了. 而前 n 个分量却可以任意取值. 我们知道，域 F 上的 n 元数组共有 2^n 个，这也就是空间 $G(f)$ 中序列的个数. 这就证明了

定理 1 设 $f(\lambda) \in F[\lambda]$ 是一 n 次多项式，于是 $G(f)$ 是 $V(F)$ 中一 n 维线性子空间，它含有 2^n 个序列.

在 $G(f)$ 的定义中，我们没有考虑 $f(\lambda)$ 是零多项式的情形. 假设 $f(\lambda)$ 是零多项式，$f(L)$ 就是零变换，于是 $V(F)$ 中的任意序列 $\mathbf{a}$ 都适合条件 $f(L)\mathbf{a} = \mathbf{0}$，也就是说，$G(\mathbf{0}) = V(F)$. 这种情形没有讨论的必要.

从以上分析可以看出，给了一个非零多项式 $f(\lambda)$，就相当于给了一个线性移位寄存器，而一个线性移位寄存器随着初始状态的不同，输出的序列也不同. 子空间 $G(f)$ 正是表示了一个线性移位寄存器所能产生的序列的全体.

下面看几个例子：

设 $f(\lambda) = \lambda$. $G(f)$ 中的序列

$$\mathbf{a} = (a_0, a_1, \cdots)$$

适合条件 $L\mathbf{a} = \mathbf{0}$，即

$$(a_1, a_2, \cdots) = \mathbf{0}.$$

这就是说，$G(f)$由

$$(a_0, 0, 0, \cdots)$$

这样的无限序列组成，其中 a_0 可以是 0 也可以是 1.

设 $f(\lambda)=\lambda^n(n\geqslant 1)$. $G(f)$ 中的序列 $\mathbf{a}$ 适合条件 $L^n\mathbf{a}=\mathbf{0}$，即

$$(a_n, a_{n+1}, \cdots)=\mathbf{0}.$$

这就是说，$G(f)$是由

$$(a_0, \cdots, a_{n-1}, 0, 0, \cdots)$$

这样的无限序列组成，其中 $a_0, \cdots, a_{n-1}$ 可以任意取值. 这样的序列显然共有 2^n 个.

不难看出，形式为 λ^n 的多项式相当于无反馈的移位寄存器.

设 $f(\lambda)=\lambda^2+\lambda+1$. $f(\lambda)$是一个二次多项式，因之，$G(f)$中无限序列的前两位可以任意取值，显然总共有 4 种取法，即(0, 0), (1, 0), (0, 1), (1, 1). 有了前两位，从第三位开始就可以由关系式 $f(L)\mathbf{a}=\mathbf{0}$ 来逐个地决定. 简单的计算就可以得出 $G(f)$的四个序列为：

$$(0, 0, 0, 0, 0, 0, \cdots),$$
$$(1, 0, 1, 1, 0, 1, \cdots),$$
$$(0, 1, 1, 0, 1, 1, \cdots),$$
$$(1, 1, 0, 1, 1, 0, \cdots).$$

§3 极小多项式与周期

设 $\mathbf{a}$ 是一线性递推序列(以下，线性递推序列将简称 *LR* 序列). 按定义，有一非零多项式 $f(\lambda)$使

$$f(L)\mathbf{a}=\mathbf{0}.$$

事实上，对于固定的序列 $\mathbf{a}$，具有这种性质的多项式不是唯一

的. 例如,对于 LR 序列

$$(0, 1, 1, 0, 1, 1, \cdots),$$

多项式 $\lambda^2+\lambda+1$ 具有上述性质，同时，多项式 λ^3+1 也具有上述性质.

既然这样的多项式不止一个，那么它们之间有什么联系呢？下面就先来解决这个问题.

对于 LR 序列 $\mathbf{a}$,我们定义

$$A(\mathbf{a})=\{f(\lambda)\in F[\lambda]\mid f(L)\mathbf{a}=\mathbf{0}\}.$$

这就是说,$A(\mathbf{a})$是所有适合条件

$$f(L)\mathbf{a}=\mathbf{0}$$

的多项式 $f(\lambda)$组成的集合.

因为 $\mathbf{a}$ 是 LR 序列,所以 $A(\mathbf{a})$一定包含非零多项式. 多项式集合 $A(\mathbf{a})$具有下面两条性质:

1) 如果 $f(\lambda)$、$g(\lambda)\in A(\mathbf{a})$,那么 $f(\lambda)\pm g(\lambda)$也在 $A(\mathbf{a})$中.

由 $f(\lambda)$、$g(\lambda)\in A(\mathbf{a})$,有

$$f(L)\mathbf{a}=\mathbf{0} \text{ 与 } g(L)\mathbf{a}=\mathbf{0},$$

从而 $$(f(L)\pm g(L))\mathbf{a}=f(L)\mathbf{a}\pm g(L)\mathbf{a}=\mathbf{0}.$$

这就是说,$f(\lambda)\pm g(x)\in A(\mathbf{a})$.

2) 如果 $f(\lambda)\in A(\mathbf{a})$、$h(\lambda)\in F[\lambda]$，那么 $h(\lambda)f(\lambda)$也在 $A(\mathbf{a})$中.

由 $f(L)\mathbf{a}=\mathbf{0}$, 有

$$(h(L)f(L))\mathbf{a}=h(L)f(L)\mathbf{a}=h(L)\mathbf{0}=\mathbf{0}.$$

这就是说, $h(\lambda)f(\lambda)\in A(\mathbf{a})$.

根据 $A(\mathbf{a})$的性质我们可以证明:

定理 2 对于每个 LR 序列 $\mathbf{a}$ 都有唯一的非零多项式 $m(\lambda)$,具有性质:

1) $m(L)\mathbf{a}=\mathbf{0}$;

2) 对于 $f(\lambda)\in F[\lambda]$，$f(L)\mathbf{a}=\mathbf{0}$ 的充分必要条件是 $m(\lambda)|f(\lambda)$.

证明：在 $A(\mathbf{a})$ 的非零多项式中总有一个次数最低的，设 $m(\lambda)$ 是 $A(\mathbf{a})$ 中一个次数最低的. 我们来证明，这样选定的 $m(\lambda)$ 就具有定理中所要求的性质. 因为 $m(\lambda)\in A(\mathbf{a})$，所以性质 1) 是显然的. 由 $A(\mathbf{a})$ 的性质，对于性质 2)，只需要证明 $m(\lambda)$ 除得尽 $A(\mathbf{a})$ 中所有的多项式. 设 $f(\lambda)\in A(\mathbf{a})$，由带余除法，有

$$f(\lambda)=q(\lambda)m(\lambda)+r(\lambda),$$

其中 $r(\lambda)=0$ 或者比 $m(\lambda)$ 有更低的次数. 如果 $r(\lambda)\neq 0$，那么根据 $A(\mathbf{a})$ 的性质：

$$r(\lambda)=f(\lambda)-q(\lambda)m(\lambda)\in A(\mathbf{a}),$$

这与 $m(\lambda)$ 的选择相矛盾. 因之，一定有 $r(\lambda)=0$，即

$$m(\lambda)|f(\lambda).$$

如果还有一个这样的多项式 $m_1(\lambda)$，那么 $m(\lambda)|m_1(\lambda)$ 同时 $m_1(\lambda)|m(\lambda)$，而它们的首项系数都是 1，即得 $m(\lambda)=m_1(\lambda)$. ∎

定理 2 中所说的多项式 $m(\lambda)$ 称为 LR 序列 $\mathbf{a}$ 的**极小多项式**.

在上节，对于 $F[\lambda]$ 中任一非零多项式 $f(\lambda)$，我们定义了 $G(f)$. $G(f)$ 中的 LR 序列不一定都以 $f(\lambda)$ 作为它们的极小多项式，但是由定理 2 可知：

推论 1 设 $f(\lambda)\neq 0$，$\mathbf{a}\in G(f)$，于是 LR 序列 $\mathbf{a}$ 的极小多项式一定是 $f(\lambda)$ 的因子.

因为不可约多项式的因子只有 1 和它本身，而以 1 作为极小多项式的 LR 序列只有零序列，所以有

推论 2 如果 $f(\lambda)$ 不可约，那么 $G(f)$ 中除去零序列外，每个 LR 序列都以 $f(\lambda)$ 为它的极小多项式.

在上一节的最后，我们看到 $G(\lambda^2+\lambda+1)$ 中有 4 个序列，而 $\lambda^2+\lambda+1$ 是不可约多项式. 因之除去零序列外，其余 3 个序列全以 $\lambda^2+\lambda+1$ 为极小多项式.

虽然 $G(f)$ 中的 LR 序列并不都以 $f(\lambda)$ 为极小多项式，但是有

定理 3 设 $f(\lambda)$ 是一非零多项式，$G(f)$ 中一定有一个以 $f(\lambda)$ 作为极小多项式的序列.

证明：设 $f(\lambda)$ 的次数为 n，由 § 2 的定理 1，$G(f)$ 是 n 维的，而且 $G(f)$ 中 LR 序列的前 n 位分量可以任意取值. 因之，$G(f)$ 有一个序列 $\mathbf{a}$，它的前 n 位分量是

$$\underbrace{(0,\ 0,\ \cdots,\ 0}_{n-1\text{个}},\ 1),$$

即
$$\mathbf{a}=(0,\ 0,\ \cdots,\ 0,\ 1,\ *,\ *,\ \cdots)$$

(这里用 * 表示 $\mathbf{a}$ 的 n 位以后的分量，它们的数值在以下讨论中无关紧要). 下面来证明：序列 $\mathbf{a}$ 的极小多项式就是 $f(\lambda)$.

因为 $G(f)$ 是左移变换 L 的不变子空间，所以由 $\mathbf{a}\in G(f)$ 可知道，序列

$$\begin{aligned}
\mathbf{a}&=(0,\ 0,\ \cdots,\ 0,\ 1,\ *,\ *,\ \cdots),\\
L\mathbf{a}&=(0,\ 0,\ \cdots,\ 1,\ *,\ *,\ *,\ \cdots),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,\\
L^{n-2}\mathbf{a}&=(0,\ 1,\ \cdots,\ *,\ *,\ *,\ *,\ \cdots),\\
L^{n-1}\mathbf{a}&=(1,\ *,\ \cdots,\ *,\ *,\ *,\ *,\ \cdots)
\end{aligned}$$

都属于 $G(f)$，这 n 个序列显然是线性无关的. 这就是说，不存在 n 个不全为零的数 $c_0,\ c_1,\ \cdots,\ c_{n-1}$，使

$$c_0\mathbf{a}+c_1L\mathbf{a}+\cdots+c_{n-1}L^{n-1}\mathbf{a}$$

$$= (c_0 + c_1 L + \cdots + c_{n-1} L^{n-1})\mathbf{a} - \mathbf{0}.$$

换句话说，不存在一个次数小于 n 的多项式 $g(\lambda)$，使

$$g(L)\mathbf{a} = \mathbf{0}.$$

因为 $\mathbf{a} \in G(f)$，所以

$$f(L)\mathbf{a} = \mathbf{0}.$$

从而 $f(\lambda)$ 是次数最低的非零多项式，使

$$f(L)\mathbf{a} = \mathbf{0}.$$

由定理 2，$f(\lambda)$ 就是 $\mathbf{a}$ 的极小多项式. ∎

定理的证明是从 $\mathbf{a}$, $L\mathbf{a}$, …, $L^{n-1}\mathbf{a}$ 的线性无关性来证 $\mathbf{a}$ 的极小多项式是 n 次多项式 $f(\lambda)$. 不难看出，这个推理过程反过来也是对的. 也就是可以证明：如果 LR 序列 $\mathbf{a}$ 的极小多项式是 n 次的，那么序列 $\mathbf{a}$, $L\mathbf{a}$, …, $L^{n-1}\mathbf{a}$ 一定线性无关.

因为 $G(f)$ 是 n 维的，所以线性无关的序列 $\mathbf{a}$, $L\mathbf{a}$, …, $L^{n-1}\mathbf{a}$ 构成 $G(f)$ 的一组基. 于是我们有

推论 1 设 $f(\lambda)$ 是一个 n 次多项式，$\mathbf{a} \in G(f)$ 的极小多项式就是 $f(\lambda)$，于是 $G(f)$ 中每个序列都可以唯一地表示成 $g(L)\mathbf{a}$ 的形式，其中 $g(\lambda)$ 是次数小于 n 的多项式.

这个推论说明：如果 $f(\lambda)$ 的次数是 n，那么在 $G(f)$ 的序列与次数小于 n 的多项式之间可以建立一个 1-1 对应.

推论 2 设 $f(\lambda)$ 是一非零多项式，$\mathbf{a} \in G(f)$ 的极小多项式就是 $f(\lambda)$，于是 $G(f)$ 中的序列 $\mathbf{b} = g(L)\mathbf{a}$ 的极小多项式是

$$\frac{f(\lambda)}{(f(\lambda),\ g(\lambda))}.$$

证明：令

$$(f(\lambda),\ g(\lambda)) = d(\lambda),$$

$$f(\lambda) = f_1(\lambda)d(\lambda),$$

$$g(\lambda) = g_1(\lambda)d(\lambda),$$

而 $\mathbf{b}=g(L)\mathbf{a}$ 的极小多项式为 $m(\lambda)$. 显然

$$f_1(L)\mathbf{b}=f_1(L)g(L)\mathbf{a}=f_1(L)g_1(L)d(L)\mathbf{a}$$
$$=g_1(L)f(L)\mathbf{a}=\mathbf{0}.$$

由定理 2, $m(\lambda)\mid f_1(\lambda)$.

由 $m(L)\mathbf{b}=\mathbf{0}$, 有

$$m(L)g(L)\mathbf{a}=m(L)g_1(L)d(L)\mathbf{a}=\mathbf{0},$$

因为 $f(\lambda)$ 是 a 的极小多项式, 所以

$$f(\lambda)\mid m(\lambda)g_1(\lambda)d(\lambda),$$

即

$$f_1(\lambda)\mid m(\lambda)g_1(\lambda).$$

我们知道, $(f_1(\lambda),\ g_1(\lambda))=1$, 由此即得

$$f_1(\lambda)\mid m(\lambda).$$

这就证明了: 序列 $\mathbf{b}=g(L)\mathbf{a}$ 的极小多项式是

$$f_1(\lambda)=\frac{f(\lambda)}{(f(\lambda),\ g(\lambda))}.\ \blacksquare$$

推论 2 表明: $G(f)$ 中的序列 $g(L)\mathbf{a}$ 以 $f(\lambda)$ 为极小多项式的充分必要条件是

$$(f(\lambda),\ g(\lambda))=1.$$

在代数中, 我们用 $\phi(f(\lambda))$ 代表次数小于 $f(\lambda)$ 且与 $f(\lambda)$ 互素的多项式的个数. 因之有

推论 3 设 $f(\lambda)$ 是一个非零多项式, 于是 $G(f)$ 中以 $f(\lambda)$ 作为极小多项式的序列的个数为 $\phi(f(\lambda))$.

在上一节的最后, 作为例子, 我们写出了 $G(\lambda^2+\lambda+1)$ 中的 4 个序列, 这 4 个序列都具有周期重复的性质. 例如序列

$$(1,\ 1,\ 0,\ 1,\ 1,\ 0,\ \cdots)$$

就是由 $(1,\ 1,\ 0)$ 无限重复组成的. 这样的无限序列通常称为**周期序列**. 下面就来讨论 LR 序列与周期序列的关系:

一般地说, 一个无限序列

$$(a_0, a_1, a_2, \cdots)$$

称为周期序列，如果有一正整数 l，使关系式

$$a_{l+k}=a_k \quad (k=0, 1, 2, \cdots) \tag{1}$$

成立. 关系式(1)当然也可以写成

$$L^l\mathbf{a}=\mathbf{a} \quad 或 \quad (L^l+I)\mathbf{a}=\mathbf{0}. \tag{2}$$

上面的序列(1, 1, 0, 1, 1, 0, …)就适合关系式

$$L^3\mathbf{a}=\mathbf{a}.$$

显然，关系式(2)是一种特殊的线性递推关系式，因之，周期序列都是 LR 序列.

在进一步讨论之前，我们首先指出：对于一个周期序列，关系式(1)或(2)中的正整数 l 不是唯一的. 事实上，由

$$L^l\mathbf{a}=\mathbf{a}$$

立即推出 $$L^{2l}\mathbf{a}=L^l(L^l\mathbf{a})=L^l\mathbf{a}=\mathbf{a}.$$

这就是说，在(2)中用 $2l$ 代替 l 也是可以的. 这就相当于无限序列

$$(1, 1, 0, 1, 1, 0, \cdots)$$

既可以看成是由(1, 1, 0)无限重复所组成，也可以看成是由(1, 1, 0, 1, 1, 0)无限重复所组成.

定理 4 对于任意一个周期序列 $\mathbf{a}$，都有一个最小的正整数 p，适合条件：

1) $L^p\mathbf{a}=\mathbf{a}$;

2) 对任意正整数 l，$L^l\mathbf{a}=\mathbf{a}$ 的充分必要条件为 $p|l$.

证明：既然 $\mathbf{a}$ 是一周期序列，就有正整数使(2)式成立；根据正整数的性质，在所有使(2)式成立的正整数中总有一个最小的，我们把它记为 p. 于是

$$L^p\mathbf{a}=\mathbf{a}$$

显然成立. 如果正整数 l 是 p 的倍数，那么

$$L^l\mathbf{a}=\mathbf{a}$$

是明显的. 反过来,如果有 $L^l\mathbf{a}=\mathbf{a}$, 我们来证 $p|l$. 由整数的带余除法,有

$$l=qp+r,\quad \text{其中}\ 0\leqslant r<p.$$

即是
$$\mathbf{a}=L^l\mathbf{a}=L^{qp+r}\mathbf{a}=L^r(L^{qp}\mathbf{a})=L^r\mathbf{a},$$

由 $r<p$ 可知 $r=0$, 即 $p|l$. ∎

定理 4 中所说的最小正整数 p 称为周期序列 $\mathbf{a}$ 的周期.

设 $\mathbf{a}$ 是一 LR 序列,它的极小多项式是 $m(\lambda)$. 根据周期序列的定义与 LR 序列的性质可以知道, $\mathbf{a}$ 是一个周期序列的充分必要条件是: 在 $A(\mathbf{a})$ 中有一形式为 λ^l+1 的多项式,或者说,有一形式为 λ^l+1 的多项式是 $m(\lambda)$ 的倍式. 我们知道,在有限域上,任意一个常数项不为零的多项式都是一个形式为 λ^l+1 的多项式的因子, 而且这样的多项式也有周期的概念. 总结以上的讨论,我们有

定理 5 设 $\mathbf{a}$ 是一 LR 序列, 它的极小多项式是 $m(\lambda)$. 如果 $m(0)\neq 0$, 那么 $\mathbf{a}$ 就是周期序列, 而且序列 $\mathbf{a}$ 的周期就等于多项式 $m(\lambda)$ 的周期.

定理 5 说明了 LR 序列与周期序列的关系, 并且把确定一个周期的 LR 序列的周期的问题归结到求它的极小多项式的周期的问题.

应该看到: 定理 5 的逆命题也是成立的, 即: 如果 $\mathbf{a}$ 是一个周期序列, 那么 $\mathbf{a}$ 的极小多项式 $m(\lambda)$ 的常数项一定不为零. 事实上,对于周期序列 $\mathbf{a}$, $A(\mathbf{a})$ 中一定有形式为

$$\lambda^l+1$$

的多项式,也就是说, $m(\lambda)|\lambda^l+1$, 从而 $m(0)\neq 0$.

至于极小多项式的常数项为零的 LR 序列与周期序列的差别,在下一节将会谈到.

§4 $G(f)$的分解

设 $\mathbf{a}$、$\mathbf{b}$ 是两个 LR 序列，我们很自然地会问：序列 $\mathbf{a}+\mathbf{b}$ 是否也是 LR 序列？如果是 LR 序列，它们的极小多项式之间有什么关系？为了弄清楚这些问题，我们来讨论 $G(f)$ 作为 $V(F)$ 的子空间的分解问题.

关于 $G(f)$ 的分解，有以下的基本事实：

引理 对于任意的非零多项式 $f(\lambda)$、$g(\lambda)$，

1) $G(f)\subset G(g)$ 的充分必要条件是

$$f(\lambda)\mid g(\lambda);$$

2) $G(f)\cap G(g)=G(d)$，其中

$$d(\lambda)=(f(\lambda),\ g(\lambda));$$

3) $G(f)+G(g)=G(h)$，其中

$$h(\lambda)=[f(\lambda),\ g(\lambda)].$$

证明：

1) 如果 $f(\lambda)\mid g(\lambda)$，即 $g(\lambda)=f_1(\lambda)f(\lambda)$，那么由 $f(L)\mathbf{a}=\mathbf{0}$ 立即推出 $g(L)\mathbf{a}=f_1(L)f(L)\mathbf{a}=\mathbf{0}$.
这就是说：$G(f)\subset G(g)$.

反过来，设 $G(f)\subset G(g)$. 在 $G(f)$ 中取一个以 $f(\lambda)$ 作为极小多项式的序列 $\mathbf{a}$（根据定理 3），于是 $\mathbf{a}\in G(g)$，即 $g(L)\mathbf{a}=\mathbf{0}$，由定理 2，就有 $f(\lambda)\mid g(\lambda)$.

2) 由 1)，$G(d)\subset G(f)$，$G(d)\subset G(g)$，从而 $G(d)\subset G(f)\cap G(g)$.

设 $\mathbf{a}\in G(f)\cap G(g)$，即

$$f(L)\mathbf{a}=\mathbf{0},\ g(L)\mathbf{a}=\mathbf{0}.$$

因为 $d(\lambda)=(f(\lambda),\ g(\lambda))$，所以有多项式 $u(\lambda)$ 与 $v(\lambda)$，使

$$d(\lambda)=u(\lambda)f(\lambda)+v(\lambda)g(\lambda).$$

于是 $$d(L)\mathbf{a}=u(L)f(L)\mathbf{a}+v(L)g(L)\mathbf{a}=\mathbf{0}.$$

因而 $\mathfrak{a}\in G(d)$，这就证明了

$$G(f)\cap G(g)\subset G(d).$$

综合这两个包含关系，即得

$$G(f)\cap G(g)=G(d).$$

3) 由 1)，$G(f)\subset G(h)$，$G(g)\subset G(h)$，从而

$$G(f)+G(g)\subset G(h).$$

为了证明它们相等，只要证明它们的维数相等就可以了．根据线性代数中的维数公式，

$G(f)+G(g)$的维数

$=G(f)$的维数$+G(g)$的维数$-G(f)\cap G(g)$的维数

$=G(f)$的维数$+G(g)$的维数$-G(d)$的维数

$=f(\lambda)$的次数$+g(\lambda)$的次数$-d(\lambda)$的次数

$=h(\lambda)$的次数$=G(h)$的维数．

这里用到了

$$[f(\lambda),\ g(\lambda)]=\frac{f(\lambda)g(\lambda)}{(f(\lambda),\ g(\lambda))}$$

这个事实．∎

引理揭示了空间 $G(f)$ 的分解与多项式 $f(\lambda)$ 的因式分解之间的紧密联系，由此立即得出

定理 6 设 $f(\lambda)$ 是一非零多项式，如果

$$f(\lambda)=f_1(\lambda)^{r_1}f_2(\lambda)^{r_2}\cdots f_s(\lambda)^{r_s},$$

其中 $f_1(\lambda)$，$f_2(\lambda)$，…，$f_s(\lambda)$ 是不同的不可约多项式，$r_i\geqslant 1$ $(i=1,\ 2,\ \cdots,\ s)$．那么就有空间的直和分解

$$G(f)=G(f_1^{r_1})\dotplus G(f_2^{r_2})\dotplus\cdots\dotplus G(f_s^{r_s}).$$

证明：我们对 $f(\lambda)$ 的不同的不可约因式的个数 s 用数学归纳法：

当 $s=1$ 时，定理显然成立．

设 $s=m-1$ 时，结论已成立，我们来证 $s=m$ 的情形：

设　　$f(\lambda)=f_1(\lambda)^{r_1}f_2(\lambda)^{r_2}\cdots f_m(\lambda)^{r_m}$.

令　　$g(\lambda)=f_2(\lambda)^{r_2}\cdots f_m(\lambda)^{r_m}$,

显然　　$f(\lambda)=f_1(\lambda)^{r_1}g(\lambda)$, $(f_1(\lambda)^{r_1}, g(\lambda))=1$.

根据引理中的 2) 和 3)，有

$$G(f)=G(f_1^{r_1})-G(g),$$
$$G(f_1^{r_1})\cap G(g)=\{0\}.$$

也就是说，有直和分解

$$G(f)=G(f_1^{r_1})\dotplus G(g).$$

根据归纳法假定，

$$G(g)=G(f_2^{r_2})\dotplus\cdots\dotplus G(f_m^{r_m}),$$

代入上式，即得

$$G(f)=G(f_1^{r_1})\dotplus G(f_2^{r_2})\dotplus\cdots\dotplus G(f_m^{r_m}).$$

因之，定理普遍成立. ∎

定理 6 表明，任意一个线性移位寄存器都可以由一些比较简单的，即反馈函数为不可约多项式的方幂的线性移位寄存器通过加法器来合成. 对某些问题的研究，归结到这类比较简单的线性移位寄存器，是有方便之处的. 譬如说，$G(f_i^{r_i})$ 中的 LR 序列的极小多项式一定是 $f_i(\lambda)^{r_i}$ 的因子，因而总是不可约多项式 $f_i(\lambda)$ 的方幂. 由定理 6 就可以知道，任意一个 LR 序列都可以分解成一些极小多项式为不可约多项式的方幂的序列之和.

关于两个 LR 序列之和的极小多项式，我们有

定理 7　设 LR 序列 $\mathbf{a}$、$\mathbf{b}$ 的极小多项式分别是 $f(\lambda)$、$g(\lambda)$. 如果 $(f(\lambda), g(\lambda))=1$，那么 $\mathbf{a}+\mathbf{b}$ 的极小多项式就是 $f(\lambda)g(\lambda)$.

证明：显然有

$$f(L)g(L)(\mathbf{a}+\mathbf{b})=\mathbf{0}.$$

下面只需证明：如果有 $h(\lambda)$，使

$$h(L)(\mathbf{a}+\mathbf{b})=\mathbf{0},$$

则 $$f(\lambda)g(\lambda)\mid h(\lambda).$$

由 $$h(L)(\mathbf{a}+\mathbf{b})=\mathbf{0},$$

有 $$f(L)h(L)(\mathbf{a}+\mathbf{b})=\mathbf{0},$$

即 $$f(L)h(L)\mathbf{b}=\mathbf{0}.$$

因为 $\mathbf{b}$ 的极小多项式是 $g(\lambda)$，所以

$$g(\lambda)\mid f(\lambda)h(\lambda).$$

由 $(f(\lambda), g(\lambda))=1$ 可知

$$g(\lambda)\mid h(\lambda).$$

同理可证 $f(\lambda)\mid h(\lambda)$. 再由 $(f(\lambda), g(\lambda))=1$, 即得

$$f(\lambda)g(\lambda)\mid h(\lambda).$$ 证毕

到这里，我们就弄清楚了 LR 序列相加与分解的情况. 譬如说，如果 s_1 与 s_2 是两个线性移位寄存器，它们的反馈函数分别是 $f(\lambda)$ 与 $g(\lambda)$，那么把它们的输出端联到一个加法器上，如图 1-2 所示. 这样输出的序列还是一个 LR 序列，而且这样一个装置的功能就相当于一个以

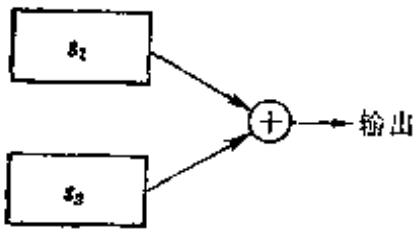


图 1-2

$$h(\lambda)=[f(\lambda), g(\lambda)]$$

为反馈函数的线性移位寄存器.

最后，利用以上结果，我们来分析一下 LR 序列与周期序列的差异.

设 LR 序列 $\mathbf{a}$ 的极小多项式为 $m(\lambda)$. 按定理 5，当 $m(0)\neq 0$ 时，$\mathbf{a}$ 是一周期序列，下面来看 $m(0)=0$ 的情形. 令

$$m(\lambda)=\lambda^s m_1(\lambda),\quad s>0,$$

其中 $m_1(0)\neq 0$. 显然, $(\lambda^s, m_1(\lambda))=1$, 于是有直和分解

$$G(m(\lambda))=G(\lambda^s)\dotplus G(m_1(\lambda)).$$

因之,

$$\mathbf{a}=\mathbf{b}+\mathbf{c},$$

其中 $\mathbf{b}\in G(\lambda^s)$, $\mathbf{c}\in G(m_1(\lambda))$. 因为 $\mathbf{a}$ 的极小多项式是 $m(\lambda)$, 所以根据定理 7, $\mathbf{c}$ 的极小多项式是 $m_1(\lambda)$, 因而 $\mathbf{c}$ 是一周期序列. 至于序列 $\mathbf{b}$, 它的极小多项式是 λ^s, 在 § 2 最后的例子中看到, 它的形式为

$$\mathbf{b}=(b_0, \cdots, b_{s-1}, 0, 0, \cdots).$$

这就说明, 序列 $\mathbf{a}$ 从第 $s+1$ 项开始与周期序列 $\mathbf{c}$ 就完全一样了. 因之, 我们可以说, 对于任意一个 LR 序列 $\mathbf{a}$, 总有一个整数 $s\geqslant 0$, 使序列 $L^s\mathbf{a}$ 是周期的.

联系到反馈移位寄存器, 当反馈函数是

$$m(\lambda)=\lambda^s m_1(\lambda), \quad s>0$$

的形式时, 寄存器的最右边的 s 位的内容实际上没有参与反馈, 因而, 略去前 s 位, 它可以看成是一个反馈函数为 $m_1(\lambda)$ 的反馈移位寄存器. 基于这个理由, 在以下的讨论中, 我们一般地总是把这种情形除外.

§ 5 状态转移矩阵

在这一节, 我们要给出处理 LR 序列的另外一种方法, 在解决某些问题时, 这种方法有它的优点.

在 § 1 中, 我们已经介绍过状态的概念. 对于一个 n 位的线性移位寄存器, 它在每一时刻的内部状态可以看作域 F 上的一个 n 维向量, 而反馈函数就是刻划了从每一时刻的状态到下一时刻的状态的转移规律, 或者用线性代数的语言说: 反馈函数定义了 n 维向量空间上的一个线性变换. 下面就从这个观点来讨论 LR 序列.

设　　$f(\lambda)=\lambda^n+c_{n-1}\lambda^{n-1}+\cdots+c_0$

是 $F[\lambda]$ 中一 n 次多项式. 对于 $G(f)$ 中的 LR 序列

$$\mathbf{a}=(a_0,\ a_1,\ \cdots,\ a_{n-1},\ \cdots),$$

我们称连续的 n 项 $(a_k,\ a_{k+1},\ \cdots,\ a_{k+n-1})$ 为 $\mathbf{a}$ 的一个状态，而 $(a_0,\ a_1,\ \cdots,\ a_{n-1})$ 称为 $\mathbf{a}$ 的初始状态，初始状态记为

$$S_0\mathbf{a}=(a_0,\ a_1,\ \cdots,\ a_{n-1}).$$

我们用 $V_n(F)$ 代表域 F 上全体 n 元数组构成的 n 维向量空间. $G(f)$ 中序列的状态可以看作 $V_n(F)$ 中的向量. 取一序列的初始状态，即 S_0，可以看作由 $G(f)$ 到 $V_n(F)$ 的一个线性变换. 因为 $G(f)$ 中的序列完全被它的初始状态决定，而初始状态的取法不受任何限制，所以 S_0 是线性空间 $G(f)$ 到 $V_n(F)$ 的一个同构映射.

在 $G(f)$ 中，对于每个序列，从状态

$$(a_k,\ a_{k+1},\ \cdots,\ a_{k+n-1})$$

到下一状态

$$(a_{k+1},\ a_{k+2},\ \cdots,\ a_{k+n})$$

的转移可以看成是 $V_n(F)$ 上的一个线性变换. 我们知道：

$$a_{k+n}=c_{n-1}a_{k+n-1}-c_{n-2}a_{k+n-2}+\cdots+c_0a_k,$$

于是状态转移变换用矩阵写出来就是

$$(a_{k+1},\ a_{k+2},\ \cdots,\ a_{k+n})$$

$$=(a_k,\ a_{k+1},\ \cdots,\ a_{k+n-1})\begin{pmatrix}0&0&0&\cdots&0&c_0\\1&0&0&\cdots&0&c_1\\0&1&0&\cdots&0&c_2\\&&&\cdots\cdots&&\\0&0&0&\cdots&1&c_{n-1}\end{pmatrix}.$$

矩阵

$$T=\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & 0 & \cdots & 0 & c_2 \\ & & \cdots\cdots & & & \\ 0 & 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix}$$

就称为 $G(f)$(也就是线性移位寄存器)的状态转移矩阵. 显然,矩阵 T 完全刻划了 $G(f)$ 中序列的情况. 事实上,从任意一个 n 维向量

$$\alpha=(a_0,\ a_1,\ \cdots,\ a_{n-1})$$

出发,作向量序列

$$\begin{aligned} \alpha &= (a_0,\ a_1,\ \cdots,\ a_{n-1}), \\ \alpha T &= (a_1,\ a_2,\ \cdots,\ a_n), \\ \alpha T^2 &= (a_2,\ a_3,\ \cdots,\ a_{n+1}), \\ &\cdots\cdots\cdots\cdots \end{aligned}$$

我们就得出了 $G(f)$ 中以 α 作为初始状态的那个 LR 序列.

我们知道,矩阵 T 是一个有理块,它的极小多项式就是它的特征多项式 $|\lambda I-T|=f(\lambda)$,而且当 T 为可逆,即 $c_0\neq 0$ 时,T 的阶就等于它的极小多项式 $f(\lambda)$ 的周期(参看附录). 以下我们假定 $c_0\neq 0$, 即矩阵 T 是可逆的. 相对于矩阵 T, 在 $V_n(F)$ 中, 所谓向量 α 的极小多项式是指次数最低的一个多项式 $m(\lambda)$,使

$$\alpha m(T)=0.$$

我们来定义向量的周期. 所谓向量 α (相对于矩阵 T)的周期是指最小的正整数 p,使

$$\alpha T^p=\alpha,$$

或者

$$\alpha(T^p+I)=0.$$

对于 LR 序列,我们有极小多项式与周期的概念,下面我

们指出，这两套概念实际上是一致的.

前面已经指出了 S_0 是线性空间 $G(f)$ 到 $V_n(F)$ 的一个同构映射，通过同构映射 S_0，我们很容易建立矩阵 T 与左移变换 L 的联系：对于

$$\mathbf{a}\in G(f), \text{有 } S_0L\mathbf{a}=(S_0\mathbf{a})T. \tag{1}$$

事实上，等式左端为

$$S_0L\mathbf{a}=S_0(a_1,\ a_2,\ \cdots)=(a_1,\ a_2,\ \cdots,\ a_n);$$

而右端为

$$\begin{aligned}(S_0\mathbf{a})T&=(a_0,\ a_1,\ \cdots,\ a_{n-1})T\\&=(a_1,\ a_2,\ \cdots,\ a_n).\end{aligned}$$

这就证明了(1). 由(1)，我们立即可以证明

引理 对于任意的 $\mathbf{a}\in G(f)$ 及任意的多项式 $g(\lambda)\in F[\lambda]$，有

$$S_0g(L)\mathbf{a}=(S_0\mathbf{a})g(T).$$

证明：因为 S_0 是线性空间之间的同构映射，所以只须证明对于任意的正整数 t，有

$$S_0L^t\mathbf{a}=(S_0\mathbf{a})T^t.$$

我们对 t 用数学归纳法：当 $t=1$ 时，要证的等式就是(1). 假设 $t=r-1$ 时，上式已成立，即

$$S_0L^{r-1}\mathbf{a}=(S_0\mathbf{a})T^{r-1}.$$

我们来证 $t=r$ 的情形：

$$\begin{aligned}S_0L^r\mathbf{a}&=S_0L^{r-1}L\mathbf{a}\\&=(S_0L\mathbf{a})T^{r-1}\\&=((S_0\mathbf{a})T)T^{r-1}\\&=(S_0\mathbf{a})T^r.\end{aligned}$$

由数学归纳法，上式普遍成立. ∎

定理 8 设 $f(\lambda)$ 是一 n 次多项式，T 为对应的状态转移矩阵. 对于任意的 $\mathbf{a}\in G(f)$，$S_0\mathbf{a}$（相对于 T）的极小多项式与

周期就是 LR 序列 $\mathfrak{a}$ 的极小多项式与周期.

证明：对于 LR 序列 $\mathfrak{a}$，在 §2 中我们定义过 $A(\mathfrak{a})$. 相仿地，对于 $V_n(F)$ 中向量 α，可以定义

$$A(\alpha)=\{g(\lambda)\in F[\lambda]\mid \alpha g(T)=0\}.$$

引理表明，对于 $\mathfrak{a}\in G(f)$，有

$$A(\mathfrak{a})=A(S_0\mathfrak{a}),$$

即这两个多项式集合是一样的. 因为极小多项式与周期都是被这个多项式集合所决定，所以自然就得出定理的结论. ∎

有了定理 8，关于 LR 序列的许多问题的讨论就可以归结为某一线性变换的讨论了. 因为对于有限维线性空间上的线性变换，我们有较多的了解，所以这就为研究 LR 序列提供了一个有力的工具.

关于状态的周期，以下的事实是常用到的.

定理 9 当 $c_0\neq 0$ 时，如果状态 α 的周期是 p，那么下列状态

$$\alpha,\ \alpha T,\ \cdots,\ \alpha T^{p-1}$$

必两两不同.

证明：用反证法：假如它们不是两两不同，那么就有 $0<i<j<p$，使

$$\alpha T^i=\alpha T^j.$$

当 $c_0\neq 0$ 时，矩阵 T 可逆，两边乘 T^{-i}，得

$$\alpha=\alpha T^{j-i}.$$

显然 $j-i<p$，这与 α 的周期是 p 相矛盾的. ∎

下面简单说一下极小多项式的求法.

设 α 是一 n 维向量，T 是状态转移矩阵. 如果

$$m(\lambda)=\lambda^r+b_{r-1}\lambda^{r-1}+\cdots+b_0$$

是 α（相对于 T）的极小多项式，那么根据极小多项式的定义，

就是说

1) $\alpha T^r + b_{r-1}\alpha T^{r-1} + \cdots + b_0\alpha = 0$，即 α, αT, $\cdots$, αT^r 线性相关；

2) 对于 $0 \leqslant s < r$, α, αT, $\cdots$, αT^s 必线性无关.

由此可见，使向量组

$$\alpha,\ \alpha T,\ \cdots,\ \alpha T^r$$

线性相关的最小正整数 r 就是 α 的极小多项式的次数. 对于这样的最小正整数 r，向量组

$$\alpha,\ \alpha T,\ \cdots,\ \alpha T^{r-1}$$

必线性无关，而 αT^r 可以由它们线性表出. 由此不难推出，对于 $l \geqslant r$，向量 αT^l 都可以由 α, αT, $\cdots$, αT^{r-1} 这 r 个向量线性表出. 因之，r 就是向量序列

$$\alpha,\ \alpha T,\ \alpha T^2,\ \cdots$$

的秩. 因为 T 的极小多项式是 n 次的，所以向量组

$$\alpha,\ \alpha T,\ \cdots,\ \alpha T^n$$

必线性相关，从而 r 也就是这个向量组的秩. 我们知道，用初等变换可以求向量组的秩. 实际上，初等变换也就给出了一个求极小多项式的现实可行的算法. 具体步骤就不细说了，读者不妨自己补出来.

最后我们指出，这里矩阵的用法与一般线性代数中稍有不同. 在 $V_n(F)$ 中，如果把状态转移

$$\alpha \mapsto \alpha T$$

看作一个线性变换 $\mathbf{T}$，那么线性变换 $\mathbf{T}$ 在基

$$\varepsilon_1 = (1,\ 0,\ 0,\ \cdots,\ 0)$$
$$\varepsilon_2 = (0,\ 1,\ 0,\ \cdots,\ 0)$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\varepsilon_n = (0,\ 0,\ 0,\ \cdots,\ 1)$$

下的矩阵应该是 T'，即 T 的转置，而不是 T．用 T 代替 T' 并不影响对问题的讨论，而直接通过矩阵的运算建立矩阵 T，在说法上要简单些，因之我们采用了现在的说法．

§6 状态图

在上一节，我们看到线性移位寄存器的功能可以用状态转移的规律来刻划，具体地说：给了一个 n 次多项式 $f(\lambda)$，同构映射 S_0 就建立了 $G(f)$ 中序列与 $V_n(F)$ 中的向量之间的一个 1-1 对应．$V_n(F)$ 中的向量就代表状态，状态总共有 2^n 个．状态转移的规律可以形象地用一个状态图来表示，下面就介绍一下状态图的概念．

在平面上，我们用 2^n 个点来代表 2^n 个状态．如果状态 α 的下一状态是 β，即

$$\beta=\alpha T$$

（这里 T 是相应的状态转移矩阵），那么就从点 α 画一个箭头到点 β．这样得到的一个有向图就称为线性移位寄存器的状态图．显然，状态图把状态转移的关系完全表现出来了，因而也就表示了线性移位寄存器的功能．现在看两个例子：

当 $f(\lambda)=\lambda^3+\lambda+1$ 时，有 $2^3=8$ 个状态，状态转移矩阵为

$$T=\begin{pmatrix}0&0&1\\1&0&1\\0&1&0\end{pmatrix},$$

状态图如图 1-3．

当 $f(\lambda)=\lambda^3+\lambda^2+\lambda+1$ 时，有 8 个状态，状态转移矩阵为

$$T=\begin{pmatrix}0&0&1\\1&0&1\\0&1&1\end{pmatrix},$$

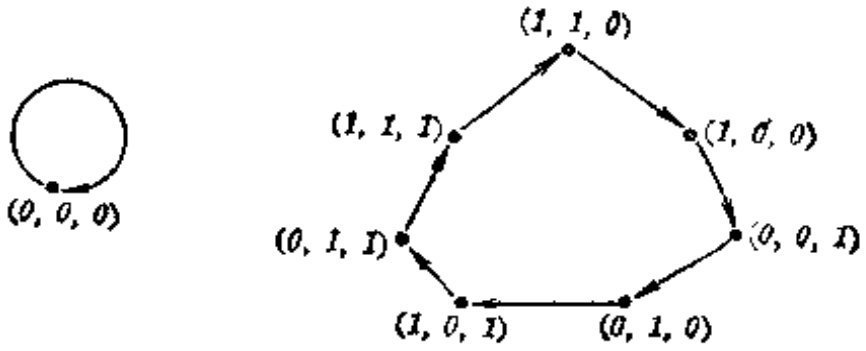


图 1-3

状态图如图 1-4.

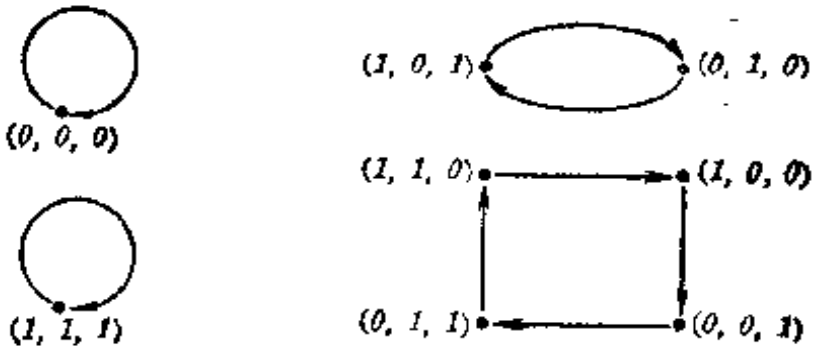


图 1-4

因为在状态图中，$\overset{\alpha}{\bullet} \longrightarrow \overset{\beta}{\bullet}$表示

$$\beta = \alpha T,$$

所以每一点只能作为一个箭头的起点；而每一点只能作为一个箭头的终点的充分必要条件是 T 可逆，也就是 $f(0) \neq 0$. 为了简单起见，下面只考虑 $f(0) \neq 0$ 的情形. 在这个情形下，每个状态 α 都有一个周期，即有正整数 p，使 $\alpha = \alpha T^p$. 当 p 为周期时，根据定理 9，状态

$$\alpha,\ \alpha T,\ \cdots,\ \alpha T^{p-1}$$

两两不同. 反映在状态图上，就是这 p 个状态构成一个圈（即简单闭路）. 一个圈上状态的个数称为圈的长度. 总结以上

分析，我们有

定理 10 设 $f(\lambda)\in F[\lambda]$，$f(0)\neq 0$. 于是 $G(f)$ 的状态图是由一些互不相交的圈所组成，而每个状态所在圈的圈长就等于这个状态的周期.

因为零状态总是变成零状态. 所以零状态总是单独构成一个长度为 1 的圈. 由此可知：线性移位寄存器的状态图至少由两个圈组成. 下面我们讨论如何由 $f(\lambda)$ 计算状态图中圈的圈长以及各种圈长的圈的个数.

为了讨论方便起见，我们指出在 $G(f)$ 中与圈相对应的概念.

如果两个周期序列 $\mathbf{a}$、$\mathbf{b}\in G(f)$ 只相差若干步位移，即有一非负整数 s，使

$$\mathbf{a}=L^s\mathbf{b},$$

我们就称 $\mathbf{a}$ 与 $\mathbf{b}$ 是平移等价的.

不难证明，平移等价是一等价关系，就是说，平移等价具有下面三条性质：

1) 反身性　$\mathbf{a}$ 与 $\mathbf{a}$ 自身平移等价.

取 $s=0$，且约定 $L^0=I$，即得

$$\mathbf{a}=L^0\mathbf{a}.$$

2) 对称性　由 $\mathbf{a}$ 与 $\mathbf{b}$ 平移等价可以推出 $\mathbf{b}$ 也与 $\mathbf{a}$ 平移等价.

设 $\mathbf{a}=L^s\mathbf{b}$. 令 $\mathbf{b}$ 的周期为 p，不妨假定 $s\leqslant p$，于是

$$L^{p-s}\mathbf{a}=L^p\mathbf{b}=\mathbf{b}.$$

3) 传递性　由 $\mathbf{a}$ 与 $\mathbf{b}$ 平移等价，$\mathbf{b}$ 与 $\mathbf{c}$ 平移等价，可以推出 $\mathbf{a}$ 与 $\mathbf{c}$ 平移等价.

由

$$\mathbf{a}=L^s\mathbf{b},\ \mathbf{b}=L^r\mathbf{c},$$

即得 $$\mathbf{a}=L^{s+r}\mathbf{c}.$$

因之，按平移等价的关系，$G(f)$中的序列被划分成一个个平移等价类．不难看出，$G(f)$的平移等价类与它的状态图上的圈是一回事．事实上，按照圈的定义，两个状态α，β在同一个圈上，就是说，有一非负整数s，使

$$\alpha=\beta T^s.$$

根据上一节的引理，有

$$S_0(L^s\mathbf{a})=(S_0\mathbf{a})T^s.$$

由此即得：序列$\mathbf{a}$与$\mathbf{b}$属于同一个平移等价类的充分必要条件是：$S_0\mathbf{a}$与$S_0\mathbf{b}$在同一个圈上．从而，序列$\mathbf{a}$所在的平移等价类中包含序列的个数就等于$S_0\mathbf{a}$所在圈的圈长．

平移等价的关系对任意两个序列当然都可以定义，不过，与$G(f)$中的序列平移等价的序列一定也在$G(f)$中，因之，只考虑同一个空间$G(f)$中的序列的平移等价关系并不妨害这个概念的一般性．

设多项式$f(\lambda)$有标准分解

$$f(\lambda)=q_1(\lambda)^{r_1}\cdots q_s(\lambda)^{r_s},$$

其中$q_1(\lambda)$，…，$q_s(\lambda)$是不同的不可约多项式．我们知道

$$G(f)=G(q_1^{r_1})\dotplus\cdots\dotplus G(q_s^{r_s}).$$

于是计算$G(f)$的圈长与圈数就可以分成两步：

1．计算$G(q^r)$的圈长与圈数，其中$q(\lambda)$是不可约多项式，$r\geqslant 1$．

2．已知$G(f)$与$G(g)$的圈长与圈数，其中$(f(\lambda),g(\lambda))=1$，计算$G(f)\dotplus G(g)$的圈长与圈数．

下面就分别讨论这两个问题：

设$q(\lambda)$是一l次不可约多项式．先看$G(q)$的状态图，$G(q)$中除去零序列外，其它序列的极小多项式都是$q(\lambda)$，因

而有相同的周期，也就是 $q(\lambda)$ 的周期 $p(q(\lambda))$. $G(q)$ 中除去零序列外，有序列 2^l-1 个，因之 $G(q)$ 的状态图中有 $\frac{2^l-1}{p(q(\lambda))}$ 个圈长为 $p(q(\lambda))$ 的圈，此外还有一个长度为 1 的圈.

一般地，在 $G(q(\lambda)^r)$ $(r\geqslant 1)$ 中，每个非零序列的极小多项式都具有形式 $q(\lambda)^k$ $(1\leqslant k\leqslant r)$. 以 $q(\lambda)^k$ 为极小多项式的序列有

$$\varphi(q(\lambda)^k)=2^{lk}-2^{l(k-1)}$$

个，它们的周期为

$$p(q(\lambda)^k)=2^t p(q(\lambda)),$$

其中 $2^{t-1}<k\leqslant 2^t$. 这部分序列在状态图中就给出 $\frac{2^{lk}-2^{l(k-1)}}{2^t p(q(\lambda))}$ 个圈长为 $2^t p(q(\lambda))$ 的圈. 取 $k=1, \cdots, r$, 再添上一个长度为 1 的圈，我们就得到 $G(q(\lambda)^r)$ 的状态图中全部的圈.

在上面的第二个例子中，

$$f(\lambda)=\lambda^3+\lambda^2+\lambda+1=(\lambda+1)^3,\ p(\lambda+1)=1,$$

读者不难验证这里的结论.

下面讨论第二个问题：

在 $(f(\lambda), g(\lambda))=1$ 的情形，

$$G(f(\lambda)g(\lambda))=G(f(\lambda))\dotplus G(g(\lambda)),$$

这是直和. 设 $G(f)$ 的状态图中有一个圈长为 u 的圈；$G(g)$ 的状态图中有一个圈长为 v 的圈，这就是说：在 $G(f)$ 中有一个平移等价类

$$\mathbf{a},\ L\mathbf{a},\ \cdots,\ L^{u-1}\mathbf{a};$$

在 $G(g)$ 中有一个平移等价类

$$\mathbf{b},\ L\mathbf{b},\ \cdots,\ L^{v-1}\mathbf{b}.$$

考虑所有形式为

$$L^i\mathbf{a}+L^j\mathbf{b}\quad (i=0,\ \cdots,\ u-1,\ j=0,\ \cdots,\ v-1)$$

的序列，它们一共有 uv 个. 如果 $\mathbf{a}$、$\mathbf{b}$ 的极小多项式分别是 $f_1(\lambda)$、$g_1(\lambda)$，显然$(f_1(\lambda),\ g_1(\lambda))=1$，根据定理 7，$L^i\mathbf{a}+L^j\mathbf{b}$ 的极小多项式为 $f_1(\lambda)g_1(\lambda)$. 我们知道，多项式 $f_1(\lambda)g_1(\lambda)$ 的周期为 $f_1(\lambda)$ 的周期与 $g_1(\lambda)$ 的周期的最小公倍数也就是 $[u,\ v]$. 因之上面的 uv 个序列被分成平移等价类，每一类含有$[u,\ v]$个序列，由此可知：分成的平移等价类的数目是

$$\frac{uv}{[u,\ v]}=(u,\ v).$$

这就告诉我们，$G(f)$ 中一个圈长为 u 的圈与 $G(g)$ 中一个圈长为 v 的圈给出了 $G(f)\dotplus G(g)$ 中 $(u,\ v)$ 个圈长为$[u,\ v]$的圈.

以上的讨论，对于任意的多项式 $f(\lambda)$，在原则上给出了一个求 $G(f)$ 的状态图中圈长与圈数的方法. 作为例子，下面计算

$$G((\lambda^3+\lambda+1)(\lambda^3+\lambda^2+\lambda+1))$$

的状态图的圈长与圈数. 为了书写方便，我们用$\langle u\rangle$表示一个圈长为 u 的圈，用 $m\langle u\rangle$表示 m 个圈长为 u 的圈. 于是 $G(\lambda^3+\lambda+1)$的状态图可以形式地表示为

$$\langle 1\rangle+\langle 7\rangle,$$

这就是说，这个状态图由一个圈长为 1 的圈与一个圈长为 7 的圈组成. 同样，$G(\lambda^3+\lambda^2+\lambda+1)$的状态图表示为

$$2\langle 1\rangle+\langle 2\rangle+\langle 4\rangle.$$

采用这种符号，上面关于圈长为 u 的圈与圈长为 v 的圈给出 $(u,\ v)$个圈长为 $[u,\ v]$ 的圈的结论可以用一个形式上的乘法来表示，即

$$\langle u\rangle\langle v\rangle=(u,\ v)\langle[u,\ v]\rangle.$$

于是 $G((\lambda^3+\lambda+1)(\lambda^3+\lambda^2+\lambda+1))$的状态图就是

$$(\langle 1\rangle+\langle 7\rangle)(2\langle 1\rangle+\langle 2\rangle+\langle 4\rangle)$$
$$=2\langle 1\rangle+\langle 2\rangle+\langle 4\rangle+2\langle 7\rangle+\langle 14\rangle+\langle 28\rangle.$$

这就是说：$G((\lambda^3+\lambda+1)(\lambda^3+\lambda^2+\lambda+1))$的状态图中有两个圈长为 1 的圈，两个圈长为 7 的圈以及圈长为 2、4、14、28 的圈各一个.

关于这种状态图的计算法，读者可参看：管纪文：«线性内动机理论 (I)» (吉林大学自然科学学报，1962 年，第二期，p. 117～146).

§7 *LR* 序列的一种表示法

反馈函数是一不可约多项式的 LR 序列，在实际上用得比较多，这一节就给出这类 LR 序列的一种表示法.

当 $f(\lambda)$是一个 n 次不可约多项式时，我们知道：它的根全在含有 2^n 个元素的有限域 $GF(2^n)$中. 域 $GF(2^n)$ 有 n 个自同构，这 n 个自同构组成一 n 阶循环群，它的一个生成元是

$$\pi_1:\beta\mapsto\beta^2,\quad \beta\in GF(2^n).$$

如果 α 是 $f(\lambda)$的一个根，那么 $f(\lambda)$的 n 个根就是 α, α^2, α^{2^2}, …, $\alpha^{2^{n-1}}$.

$GF(2^n)$包含 F 作为一个子域，$GF(2^n)$中在 π_1 下保持不动的元素只有 0、1，即 F 中的元素. 显然，对于 $GF(2^n)$中的任意元素 β，元素

$$\beta+\pi_1(\beta)+\cdots+\pi_1^{n-1}(\beta)$$

在 π_1 下不动，因之它属于 F，我们用 $Tr(\beta)$代表这个元素(称为 β 的迹)，即

$$Tr(\beta)=\beta+\pi_1(\beta)+\cdots+\pi_1^{n-1}(\beta)$$
$$=\beta+\beta^2+\cdots+\beta^{2^{n-1}}.$$

把 $GF(2^n)$ 看作 F 上的一个线性空间，Tr 就是 $GF(2^n)$ 到 F 的一个线性映射.

设 $$f(\lambda)=\lambda^n+c_{n-1}\lambda^{n-1}+\cdots+c_0$$ 是 $F[\lambda]$ 中一 n 次不可约多项式，而 α 是 $f(\lambda)$ 在 $GF(2^n)$ 中的一个根，即

$$\alpha^n+c_{n-1}\alpha^{n-1}+\cdots+c_0=0.$$

我们不难看出，对于任意的 $\beta\in GF(2^n)$，序列

$$(Tr(\beta),\ Tr(\beta\alpha),\ Tr(\beta\alpha^2),\cdots)$$

属于 $G(f)$. 事实上，对于任意的 $k\geqslant 0$，

$$\begin{aligned}&Tr(\beta\alpha^{n+k})+c_{n-1}Tr(\beta\alpha^{n+k-1})+\cdots+c_0Tr(\beta\alpha^k)\\&=Tr(\beta\alpha^{n+k}+c_{n-1}\beta\alpha^{n+k-1}+\cdots+c_0\beta\alpha^k)\\&=Tr(\beta\alpha^k(\alpha^n+c_{n-1}\alpha^{n-1}+\cdots+c_0))=Tr(0)=0.\end{aligned}$$

这就是说，上面的序列适合递推关系式

$$a_{n+k}+c_{n-1}a_{n+k-1}+\cdots+c_0a_k=0,$$

因而它属于 $G(f)$. 下面来证明这个结论的逆.

定理 11 $f(\lambda)$、α 如前. 对于 $G(f)$ 中的任一序列 $\mathbf{a}$ 都有一 $\beta\in GF(2^n)$，使

$$\mathbf{a}=(Tr(\beta),\ Tr(\beta\alpha),\ Tr(\beta\alpha^2),\ \cdots).$$

证明：此定理换个说法是：当 β 取遍 $GF(2^n)$ 中所有可能的值时，序列

$$(Tr(\beta),\ Tr(\beta\alpha),\ Tr(\beta\alpha^2),\ \cdots)$$

就给出了 $G(f)$ 中全部的序列. 因为 $G(f)$ 中有 2^n 个序列，$GF(2^n)$ 中有 2^n 个元素，所以为了证明本定理，只须证明：当 $\beta_1\neq\beta_2$ 时，

$$\begin{aligned}&(Tr(\beta_1),\ Tr(\beta_1\alpha),\ Tr(\beta_1\alpha^2),\ \cdots)\\&\neq(Tr(\beta_2),\ Tr(\beta_2\alpha),\ Tr(\beta_2\alpha^2),\ \cdots),\end{aligned}$$

或者说，当 $\gamma=\beta_1-\beta_2\neq 0$ 时，序列

$$(Tr(\beta_1),\ Tr(\beta_1\alpha),\ Tr(\beta_1\alpha^2),\ \cdots)$$
$$-(Tr(\beta_2),\ Tr(\beta_2\alpha),\ Tr(\beta_2\alpha^2),\ \cdots)$$
$$=(Tr(\gamma),\ Tr(\gamma\alpha),\ Tr(\gamma\alpha^2),\ \cdots)\neq 0.$$

用反证法：假如

$$(Tr(\gamma),\ Tr(\gamma\alpha),\ Tr(\gamma\alpha^2),\ \cdots)=0,$$

即
$$Tr(\gamma)=Tr(\gamma\alpha)=Tr(\gamma\alpha^2)=\cdots=0.$$

按 Tr 的定义，把前 n 项写出来就是

$$\gamma+\gamma^2+\gamma^{2^2}+\cdots+\gamma^{2^{n-1}}=0,$$
$$\gamma\alpha+\gamma^2\alpha^2+\gamma^{2^2}\alpha^{2^2}+\cdots+\gamma^{2^{n-1}}\alpha^{2^{n-1}}=0,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\gamma\alpha^{n-1}+\gamma^2\alpha^{2(n-1)}+\gamma^{2^2}\alpha^{(n-1)2^2}+\cdots+\gamma^{2^{n-1}}\alpha^{(n-1)2^{n-1}}=0.$$

用矩阵形式表示就是

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha & \alpha^2 & \alpha^{2^2} & \cdots & \alpha^{2^{n-1}} \\ \alpha^2 & \alpha^{2\times 2} & \alpha^{2\times 2^2} & \cdots & \alpha^{2\times 2^{n-1}} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \alpha^{n-1} & \alpha^{(n-1)2} & \alpha^{(n-1)2^2} & \cdots & \alpha^{(n-1)2^{n-1}} \end{pmatrix}\begin{pmatrix} \gamma \\ \gamma^2 \\ \gamma^{2^2} \\ \vdots \\ \gamma^{2^{n-1}} \end{pmatrix}=0.$$

由于 $f(\lambda)$ 是不可约多项式，它的 n 个根

$$\alpha,\ \alpha^2,\ \alpha^{2^2},\ \cdots,\ \alpha^{2^{n-1}}$$

两两不同，所以上面的矩阵正好是 Vandomonde 矩阵，它是可逆的．由此即得

$$\gamma=0.$$

这与假定 $\gamma\neq 0$ 矛盾．∎

定理 11 给出了 $G(f)$ 中序列的一种表示法，这种表示法在讨论 LR 序列的某些问题时是有用的．现在我们就利用这种表示法来解决 LR 序列的采样问题．

设
$$\mathfrak{a}=(a_0,\ a_1,\ a_2,\ \cdots)$$

是一 LR 序列，s 是一正整数，序列

$$\mathbf{a}^{(s)}=(a_0,\ a_s,\ a_{2s},\ \cdots)$$

称为序列 $\mathbf{a}$ 的一个采样，或者 s-采样. 我们的问题是：$\mathbf{a}^{(s)}$ 是否还是一 LR 序列，如果是 LR 序列，那么 $\mathbf{a}^{(s)}$ 的极小多项式与周期同 $\mathbf{a}$ 的极小多项式与周期有什么关系？这些问题的回答依赖于下面的基本事实.

定理 12 设 $f(\lambda)$ 为一 n 次不可约多项式，α 为 $f(\lambda)$ 的一个根. 如果 $\mathbf{a}\in G(f)$ 的 s-采样 $\mathbf{a}^{(s)}\neq\mathbf{0}$，那么 $\mathbf{a}^{(s)}$ 的极小多项式就是 α^s 的极小多项式.

证明：既然 $\mathbf{a}\in G(f)$，就有 $\beta\in GF(2^n)$，使

$$\mathbf{a}=(Tr(\beta),\ Tr(\beta\alpha),\ Tr(\beta\alpha^2),\ \cdots).$$

于是 $$\mathbf{a}^{(s)}=(Tr(\beta),\ Tr(\beta\alpha^s),\ Tr(\beta\alpha^{2s}),\ \cdots).$$

令 $\alpha^s=\gamma$，就有

$$\mathbf{a}^{(s)}=(Tr(\beta),\ Tr(\beta\gamma),\ Tr(\beta\gamma^2),\ \cdots).$$

如果 $\gamma=\alpha^s$ 的极小多项式是 $g(\lambda)$，那么仿照上面的证明，可证

$$\mathbf{a}^{(s)}\in G(g).$$

因为 α^s 的根小多项式是不可约的，所以只要 $\mathbf{a}^{(s)}\neq\mathbf{0}$，它的极小多项式就是 $g(\lambda)$. ∎

我们知道，$\mathbf{a}$ 的周期就是它的极小多项式 $f(\lambda)$ 的周期，而 $f(\lambda)$ 的周期也就是 $f(\lambda)$ 的根在 $GF(2^n)$ 的非零元素组成的乘法群中的阶. 显然，如果元素 α 的阶为 t，那么 α^s 的阶就是 $\frac{t}{(s,\ t)}$. 由此即得

推论 1 设 $f(\lambda)$ 为一不可约多项式，$\mathbf{a}\in G(f)$. 如果 $\mathbf{a}^{(s)}\neq\mathbf{0}$，那么

$$p(\mathbf{a}^{(s)})=\frac{p(\mathbf{a})}{(s,\ p(\mathbf{a}))}.$$

因为 $GF(2^n)$ 中元素的极小多项式的次数总是 n 的因子，所以有

推论 2 设 $f(\lambda)$ 是一 n 次不可约多项式，$\mathbf{a}\in G(f)$. 如果 $\mathbf{a}^{(s)}\neq\mathbf{0}$，而 $g(\lambda)$ 是它的极小多项式，那么 $g(\lambda)$ 的次数一定是 n 的因子.

从以上的讨论，当我们知道了采样序列，则对原来的序列也可以有一些了解.

设 $f(\lambda)$ 是一不可约多项式，α 是它的一个根，$\mathbf{a}\in G(f)$，$\mathbf{a}\neq\mathbf{0}$，而 $\mathbf{a}$ 的 s-采样 $\mathbf{a}^{(s)}$ 的极小多项式为 $g(\lambda)$. 我们知道 $g(\lambda)$ 就是 α^s 的极小多项式，即 $g(\alpha^s)=0$，因之

$$f(\lambda)\mid g(\lambda^s).$$

这就是说，如果 LR 序列 $\mathbf{a}$ 的极小多项式是一不可约多项式，而 $\mathbf{a}$ 的 s-采样 $\mathbf{a}^{(s)}$ 的极小多项式为 $g(\lambda)$，那么 $\mathbf{a}$ 的极小多项式就是 $g(\lambda^s)$ 的一个不可约因子. 由上面的推论 2 可知，$g(\lambda^s)$ 的不可约因子的次数一定是 $g(\lambda)$ 的次数的倍数.

第二章 m 序 列

§1 定义

我们已经讨论了 LR 序列的一般性质. 在 LR 序列中，所谓极大周期序列是用得较多的一种序列，现在来对这种序列作专门的讨论.

设 $$\mathbf{a}=(a_0, a_1, a_2, \cdots)\neq\mathbf{0}$$

是一周期序列. 如果已知它的极小多项式 $f(\lambda)$ 是 n 次的，我们要问，$\mathbf{a}$ 的周期最大是多少？根据上一章的讨论，从它的极小多项式可以写出一个状态转移矩阵 T，而 $\mathbf{a}$ 的周期就等于 $\mathbf{a}$ 的初始状态 $S_0(\mathbf{a})=(a_0, a_1, \cdots, a_{n-1})$ 相对于矩阵 T 的周期，也就是有最小的正整数 p，使

$$(a_0, a_1, \cdots, a_{n-1})=(a_0, a_1, \cdots, a_{n-1})T^p.$$

由第一章定理 9，我们知道：状态

$$S_0(\mathbf{a}),\ S_0(\mathbf{a})T,\ \cdots,\ S_0(\mathbf{a})T^{p-1}$$

必两两不同. $V_n(F)$ 中非零向量有 2^n-1 个，由此即得

$$p\leqslant 2^n-1.$$

这就是说，以 n 次多项式作为极小多项式的周期序列的周期最多是 2^n-1.

定义 设非零的周期序列 $\mathbf{a}$ 的极小多项式是 n 次的，如果 $\mathbf{a}$ 的周期恰好是 2^n-1，那么 $\mathbf{a}$ 就称为一极大周期序列，或 n 级极大周期序列.

为了叙述简便，以后将极大周期序列简称为 m 序列.

例如，周期序列

$$(0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 1,\ 0,\ 1,\ 0,\ 1,\ 1,\ 1,\ 1,\ \cdots)$$

的极小多项式是 $\lambda^4+\lambda^3+1$，而它的周期是

$$15=2^4-1,$$

它就是一个 4 级的 m 序列.

周期序列

$$(0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 0,\ 1,\ 1,\ \cdots)$$

的极小多项式是 $\lambda^4+\lambda^3+\lambda^2+\lambda+1$，而它的周期是 5，它就不是一个 m 序列.

设 $$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots)$$

是一 n 级 m 序列，它的极小多项式是 n 次多项式 $f(\lambda)$. 因为 m 序列是周期序列，所以 $f(0)\neq 0$. 我们知道：$G(f)$ 是 n 维的线性空间，而且由

$$\mathbf{a}\in G(f)$$

有 $$L^s\mathbf{a}\in G(f)\quad (s=1,\ 2,\ \cdots).$$

$\mathbf{a}$ 的周期是 2^n-1，换句话说，$\mathbf{a}$ 所在的平移等价类包含序列的个数是 2^n-1，由此可知：序列

$$\mathbf{a},\ L\mathbf{a},\ L^2\mathbf{a},\ \cdots,\ L^{2^n-2}\mathbf{a}$$

必两两不同. 它们显然都是非零序列，而 $G(f)$ 中非零序列的个数也是 2^n-1，因之它们正好是 $G(f)$ 中全部非零序列.

由 $f(0)\neq 0$ 可知 $(f(\lambda),\ \lambda^s)=1$，因而 $L^s\mathbf{a}$ 的极小多项式也是 $f(\lambda)$. 这就表明：$G(f)$ 中每个非零序列都以 $f(\lambda)$ 作为它的极小多项式，根据上一章的讨论：不难看出，$f(\lambda)$ 一定是不可约的. 事实上，假如 $f(\lambda)$ 可约，即 $f(\lambda)=f_1(\lambda)f_2(\lambda)$，那么 $G(f)$ 中的序列 $f_1(L)\mathbf{a}$ 就以 $f_2(\lambda)$ 为极小多项式.

我们知道：一个周期序列的周期就等于它的极小多项式的周期，因之，一个 n 级 m 序列的极小多项式 $f(\lambda)$ 的周期是 2^n-1. 在代数中，这样的多项式称为 n 次本原多项式. 反过

来，设 $f(\lambda)$ 是一 n 次本原多项式，于是 $G(f)$ 中非零序列都以 $f(\lambda)$ 作为它的极小多项式(因为 $f(\lambda)$ 不可约)，因而它们的周期都是 2^n-1，也就是说，它们都是 n 级 m 序列.

综合以上讨论，我们有

定理 1 如果 LR 序列是 m 序列，那么 $\mathbf{a}$ 的极小多项式是本原多项式；反过来，如果 $f(\lambda)$ 是本原多项式，那么 $G(f)$ 中每个非零序列都是 m 序列.

定理 1 表明：一个周期序列是不是 m 序列，就看它的极小多项式是不是本原多项式. 因之，为了产生 m 序列，设计线性移位寄存器的问题在原则上就归结为找本原多项式的问题. 如果 $f(\lambda)$ 是一 n 次本原多项式，那么 $G(f)$ 中所有非零序列都是 n 次 m 序列，而且对于任意一个非零序列 $\mathbf{a}\in G(f)$，序列

$$\mathbf{a},\ L\mathbf{a},\ \cdots,\ L^{p-1}\mathbf{a},\quad p=2^n-1$$

就是 $G(f)$ 中全部非零序列. 这就是说，在 $G(f)$ 中，由不同的初始状态出发(当然不是零状态)，得到的 m 序列虽然不同，但它们只不过相差若干步位移，或者说，它们都是平移等价的. 显然，平移等价的 m 序列有相同的极小多项式，因而 $G(f)$ 中全部非零序列正好构成一个平移等价类. 于是我们有

定理 2 在全部 n 级 m 序列中，平移等价类的个数就等于 n 次本原多项式的个数，也就等于

$$\frac{\varphi(2^n-1)}{n}.$$

如果把平移等价的 m 序列不加区别的话，那么上面的讨论表明：在 n 级 m 序列与 n 次本原多项式之间有一个 1--1 对应.

我们看到：m 序列有一个有趣的性质，那就是包含它的平

移等价类再添上零序列正好构成一个线性空间. 具体地说: 如果序列 $\mathbf{a}$ 的周期为 p, 那么集合

$$\mathbf{a},\ L\mathbf{a},\ \cdots,\ L^{p-1}\mathbf{a},\ \mathbf{0}$$

对加法是封闭的, 或者说, 对于任意的

$$0\leqslant i<j\leqslant p-1,$$

有 $0\leqslant k\leqslant p-1$, 使

$$L^i\mathbf{a}+L^j\mathbf{a}=L^k\mathbf{a}.$$

通常称这个性质为平移可加性. 实际上, 平移可加性是 m 序列的一个特征性质, 这就是说: 如果周期序列 $\mathbf{a}$ 具有平移可加性, 那么 $\mathbf{a}$ 一定是 m 序列. 设 $\mathbf{a}$ 的周期为 p, 而序列集合

$$\mathbf{a},\ L\mathbf{a},\ \cdots,\ L^{p-1}\mathbf{a},\ \mathbf{0}$$

构成的线性空间的维数为 n, 于是

$$p+1=2^n,\ p=2^n-1.$$

令 $f(\lambda)$ 为 $\mathbf{a}$ 的极小多项式, 次数为 m. 因为上面的这些序列全属于 $G(f)$, 所以 $n\leqslant m$. 另一方面, 由 $\mathbf{a}$ 的极小多项式的次数为 m 可知:

$\mathbf{a},\ L\mathbf{a},\ \cdots,\ L^{m-1}\mathbf{a}$ 线性无关, 于是有 $m\leqslant n$. 这就是说, $f(\lambda)$ 是一 n 次多项式, $\mathbf{a}$ 的周期为 2^n-1, 因而 $\mathbf{a}$ 是一个 m 序列.

§ 2 伪随机性

在一些场合, 人们常常希望获得用随机的方式产生的序列. 所谓随机的方式可以用一个通俗的例子来说明: 拿一个硬币, 我们规定它的正面(即有国徽的一面)代表 1, 反面(即有分值的一面)代表 0. 掷这个硬币, 按它是正面朝上或者反面朝上, 分别记下 1 或者 0. 连续掷硬币, 我们就得到一个 (0, 1)序列. 假如所用的硬币是均匀的, 而掷的方式是不带

倾向性的，我们就认为这样获得(0, 1)序列的方式是随机的．用随机的方式获得的序列称为随机序列．随机序列有某些重要的统计特性．

m 序列产生的方式有很强的规律性，从这一点看，它和随机序列有根本的区别．但是 m 序列却具有随机序列所具有的某些重要的统计特性，或者说，m 序列看上去很象随机序列．下面就来讨论 m 序列的这一方面的性质，它们有时统称为 m 序列的伪随机性．

设 $$\mathbf{a}=(a_0, a_1, a_2, \cdots)$$

是一个 n 级 m 序列，$f(\lambda)$ 是它的极小多项式，T 是对应的状态转移矩阵．我们知道，$\mathbf{a}$ 的周期为

$$p=2^n-1,$$

$\mathbf{a}$ 的不同的状态

$$S_0\mathbf{a}=(a_0, a_1, \cdots, a_{n-1}),$$
$$(S_0\mathbf{a})T=(a_1, a_2, \cdots, a_n),$$
$$(S_0\mathbf{a})T^2=(a_2, a_3, \cdots, a_{n+1}),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(S_0\mathbf{a})T^{p-1}=(a_{p-1}, a_p, \cdots, a_{n+p-2})$$

正好是 $V_n(F)$ 中全部非零向量．

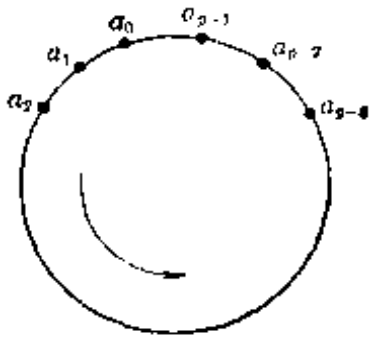


图 2-1

为了叙述方便，我们把 $\mathbf{a}$ 的一个周期

$$(a_0, a_1, a_2, \cdots, a_{p-1})$$

排在一个圆周上，a_{p-1} 的后面就接 a_0，如图 2-1 所示．显然，$\mathbf{a}$ 的每个状态在圆周上出现一次而且只出现一次．我们把这样的圆周简称为周期圆．

对于 $0<k\leqslant n$，任意一个 k 元(0, 1)序列

$$(b_1, \cdots, b_k)$$

可以扩充成一个 n 元序列

$$(b_1, \cdots, b_k, c_1, \cdots, c_{n-k}).$$

不同的扩充总共有 2^{n-k} 个. 因为周期圈上不包含 n 维零向量，所以 k 元序列 $(b_1, \cdots, b_k)$ 在周期圈上出现的次数为

$$\begin{cases} 2^{n-k}, & \text{当}(b_1, \cdots, b_k) \neq (0, \cdots, 0); \\ 2^{n-k}-1, & \text{当}(b_1, \cdots, b_k) = (0, \cdots, 0). \end{cases}$$

取 $k=1$，即得

定理 3 在 n 级 m 序列的一个周期中，1 出现的次数为 2^{n-1} 次；0 出现的次数为 $2^{n-1}-1$ 次.

这就是说，在 m 序列的一个周期中，0 与 1 出现的次数几乎相等. 这是 m 序列的伪随机性的第一条.

为了叙述下面的定理，我们先介绍一下游程的概念. 任意一个(0, 1)序列总可以看成是由一段 0 和一段 1 相间地排列而成的. 例如，序列

$$(0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$$

就是由 (0, 0, 0), (1), (0, 0), (1, 1), (0), (1), (0), (1, 1, 1, 1)这样 8 段组成的. 这样的段就称为游程. 游程所包含的元素个数称为它的长度. 例如，(0, 0, 0)是一个长度为 3 的 0 游程，(1, 1)是一个长度为 2 的 1 游程.

还以上面那个序列为例来说，它是由 8 个游程组成的，其中长度为 1 的有 4 个，在这 4 个当中，0 游程和 1 游程各占一半；长度为 2 的游程有两个，其中 0 游程和 1 游程各一个；长度为 3 的 0 游程一个；长度为 4 的 1 游程 1 个.

在一个序列

$$(a_0, a_1, \cdots, a_{p-1}, \cdots)$$

中，如果$(a_k, a_{k+1}, \cdots, a_{k+l-1})$是一个 0 游程(1 游程)，那么按

游程的定义，它的前一位 a_{k-1} 和后一位 a_{k+1}(如果有的话)一定是1(0).

定理4 在 n 级 m 序列的周期圈上，对于 $0<k\leqslant n-2$，长度为 k 的0游程出现 2^{n-k-2} 次；长度为 k 的1游程也出现 2^{n-k-2} 次；长度为 $n-1$ 的0游程出现一次；长度为 n 的1游程出现一次；而且这就是其中出现的全部游程.

证明：对于 $0<k\leqslant n-2$，$k+2$ 元序列

$$1\ \underbrace{0\ \cdots\ 0}_{k\text{个}}\ 1$$

与

$$0\ \overbrace{1\ \cdots\ 1}^{k\text{个}}\ 0$$

各出现 2^{n-k-2} 次，这就是前一半的结论.

为了证明定理的后一半，我们首先指出：长度大于 n 的游程是不可能有的. 否则，在周期圈上就要出现两个全是1或者全是0的状态，这是不可能的.

在周期圈上没有零状态，因之没有长度为 n 的0游程. 状态(1, 1, …, 1)，(0, 1, …, 1)，(1, …, 1, 0)(长度均为 n)在周期圈上各出现一次. 因为没有长度大于 n 的游程，所以在向量(1, 1, …, 1)的前后一定都是0，这就是说，在周期圈上有

$$(0,\ 1,\ 1,\ \cdots,\ 1,\ 0)$$

这样一个 $n+2$ 元序列. 在这里，上面的三个状态各出现一次，当然它们在其它地方就不可能再出现了. 由此可见，长度为 n 的1游程出现一次，但没有长度为 $n-1$ 的1游程.

在周期圈上，状态(1, 0, …, 0)与(0, …, 0, 1)各出现一次. 因为没有长度为 n 的0游程，所以在(1, 0, …, 0)之后一定是1，这就是说：在周期圈上有

$$(1,\ 0,\ \cdots,\ 0,\ 1)$$

这样一个 $n+1$ 元序列. 在这里，上面两个状态各出现一次，当然它们在其它地方也就不可能再出现了. 因之，长度为 $n-1$ 的 0 游程恰有一个.

按定理 4，不难算出，游程的总数是 2^{n-1}，其中长度为 1 的游程占 1/2，长度为 2 的游程占 1/4，等等，而且在同一长度的游程中，0 游程与 1 游程各占一半. 只是长度为 $n-1$ 与 n 的游程情况特殊.

这就是 m 序列伪随机性的第二条.

定理 3 是说明在 m 序列中 0 与 1 出现的次数，而定理 4 通过游程的概念进一步刻划了 0 与 1 出现的顺序.

为了刻划 0、1 出现的任意性，对于周期序列，我们来定义自相关函数.

在域 F 中，$\{0, 1\}$ 对于加法成一个 2 阶群，在复数域中，$\{1, -1\}$ 对于乘法也成一个 2 阶群. 映射 η:

$$\eta(0)=1,\ \eta(1)=-1$$

显然是这两个群的一个同构映射.

设 $$\mathbf{a}=(a_0, a_1, \cdots, a_{p-1}, \cdots)$$

是一周期为 p 的周期序列. 我们定义

$$C_{\mathbf{a}}(t)=\sum_{k=0}^{p-1}\eta(a_k)\eta(a_{k+t}),$$

$C_{\mathbf{a}}(t)$ 称为 $\mathbf{a}$ 的自相关函数.

因为 $\mathbf{a}$ 的周期是 p，所以显然有

$$C_{\mathbf{a}}(t)=C_{\mathbf{a}}(t+p).$$

因之，在以下讨论中，不妨假定 $0\leqslant t<p$.

定理 5 设 $\mathbf{a}$ 是一 n 级 m 序列，$p=2^n-1$，于是

$$C_{\mathbf{a}}(t)=\begin{cases} p, & \text{当 } t=0; \\ -1, & \text{当 } 0<t<p. \end{cases}$$

证明：当 $t=0$ 时，

$$C_{\mathbf{a}}(0)=\sum_{k=0}^{p-1}\eta(a_k)\eta(a_k)=\sum_{k=0}^{p-1}1=p.$$

当 $0<t<p$ 时，

$$C_{\mathbf{a}}(t)=\sum_{k=0}^{p-1}\eta(a_k)\eta(a_{k+t})=\sum_{k=0}^{p-1}\eta(a_k+a_{k+t}).$$

我们知道：$L^t\mathbf{a}$ 和 $\mathbf{a}$ 一样也是 n 级 m 序列，而且 $L^t\mathbf{a}$ 与 $\mathbf{a}$ 有相同的极小多项式．由 m 序列的平移可加性知：$\mathbf{a}+L^t\mathbf{a}\neq 0$ 也是一个 n 级 m 序列，而

$$(a_0+a_t,\ a_1+a_{1+t},\ \cdots,\ a_{p-1}+a_{p-1+t})$$

正是 m 序列 $\mathbf{a}+L^t\mathbf{a}$ 的一个周期．根据定理 3，其中 0 的个数比 1 的个数少 1，也就是说

$$\eta(a_k+a_{k+t})\quad(k=0,\ 1,\ \cdots,\ p-1)$$

中 1 的个数比 -1 的个数少 1．这就证明了：当 $0<t<p$ 时，

$$C_{\mathbf{a}}(t)=\sum_{k=0}^{p-1}\eta(a_k+a_{k+t})=-1.\ \blacksquare$$

这就是 m 序列伪随机性的第三条．

在 m 序列的某些应用中，这条性质具有特殊的重要性．

由于 m 序列具有定理 3、4、5 所叙述的性质，因之有人称 m 序列为伪随机序列．这个名称表明：虽然 m 序列产生的方式是完全确定的，远远不是随机的，但是它却具有随机序列的某些重要的统计特征，有时可以冒充随机序列来用．

定理 5 的证明主要是根据 m 序列的平移可加性，利用平移可加性，我们还可以得到另一个相仿的性质：

定理 6 设 $\mathbf{a}$ 为一 n 级 m 序列，把 0，1 看作通常的整数，有

$$\sum_{k=0}^{p-1}a_ka_{k+t}=\begin{cases}2^{n-1}, & \text{当 } t=0;\\ 2^{n-2}, & \text{当 } 0<t<p.\end{cases}$$

证明：当 $t=0$ 时，

$$\sum_{k=0}^{p-1} a_k^2 = \sum_{k=0}^{p-1} a_k$$

是 a 的一个周期中"1"出现的次数 2^{n-1}.

当 $0<t<p$ 时，$\sum_{k=0}^{p-1} a_k a_{k+t}$ 就等于序列

$$(a_0,\ a_1,\ \cdots,\ a_{p-1})$$

与

$$(a_t,\ a_{t+1},\ \cdots,\ a_{p+t-1})$$

对应位上同时都是 1 的位数. 考察元素对

$$(a_k,\ a_{k+t}) \quad (k=0,\ 1,\ \cdots,\ p-1),$$

它们不外是 (1, 1), (1, 0), (0, 1), (0, 0)这 4 种情形. 设 (1, 1)这种情形出现 x 次，于是

$$\sum_{k=0}^{p-1} a_k a_{k+t} = x.$$

下面就来计算 x 的值. 因为序列

$$(a_0,\ a_1,\ \cdots,\ a_{p-1})$$

中有 2^{n-1} 个 1, $2^{n-1}-1$ 个 0, 所以由(1, 1)共出现 x 次可知 (1, 0)这种情形出现 $2^{n-1}-x$ 次；同样理由，(0, 1)这种情形出现的次数也是 $2^{n-1}-x$. 我们知道

$$(a_0+a_t,\ a_1+a_{t+1},\ \cdots,\ a_{p-1}+a_{p+t-1})$$

也是 m 序列的一个周期，其中"1"出现 2^{n-1} 次. 只有在(1, 0)和(0, 1)这两种情形才使

$$a_k+a_{k+t}=1,$$

因之有

$$2(2^{n-1}-x)=2^{n-1},$$

$$x=2^{n-2}. \blacksquare$$

§3 m 序列的采样

在第一章§7, 我们对 LR 序列的采样作了一般的讨论，

得到的主要结论是：

设 $f(\lambda)$ 是一个不可约多项式，α 是 $f(\lambda)$ 的一个根，$\mathbf{a}\in G(f)$．如果 $\mathbf{a}$ 的 s 采样 $\mathbf{a}^{(s)}\neq\mathbf{0}$，那么 $\mathbf{a}^{(s)}$ 的极小多项式就是元素 α^s 的极小多项式．

现在我们就在这个基础上来讨论 m 序列的采样．

定理 7 设 $\mathbf{a}$ 是一 n 级 m 序列，周期为 $p=2^n-1$，s 是一正整数．如果 $(s,\ p)=1$，那么 $\mathbf{a}^{(s)}$ 也是周期为 p 的 n 级 m 序列．每个 n 级 m 序列都平移等价于 $\mathbf{a}$ 的这样一个采样．

证明：令 $f(\lambda)$ 是 $\mathbf{a}$ 的极小多项式，α 是 $f(\lambda)$ 的一个根．因为 $f(\lambda)$ 是本原多项式，所以 α 是域 $GF(2^n)$ 中一个本原元素．我们知道，α^s 是本原元素的充分必要条件是 $(s,\ p)=1$，而本原元素的极小多项式是本原多项式．不难看出：当 $(s,\ p)=1$ 时，$\mathbf{a}^{(s)}$ 的前 p 位分量不过是 $\mathbf{a}$ 的前 p 位分量的一个重新排列，所以 $\mathbf{a}^{(s)}$ 一定不是零序列，这就证明了定理的前一半．

设 $\mathbf{b}$ 是任意一个 n 级 m 序列，$g(\lambda)$ 是 $\mathbf{b}$ 的极小多项式，β 是 $g(\lambda)$ 的一个根．既然 β 是域 $GF(2^n)$ 中一个本原元素，显然有一正整数 s 使 $\beta=\alpha^s$，且 $(s,\ p)=1$．于是 $\mathbf{a}^{(s)}$ 的极小多项式也是 $g(\lambda)$．我们知道，$G(g)$ 中全部非零序列都互相平移等价，这就证明了定理的后一半．

定理 8 设 $\mathbf{a}$ 是一 n 级 m 序列，周期为 $p=2^n-1$．$\mathbf{a}$ 的 2^i 采样 $(i=0,\ 1,\ \cdots,\ n-1)$ 全与 $\mathbf{a}$ 平移等价．对于任意的正整数 r，s，如果 $(r,\ p)=(s,\ p)=1$，那么 $\mathbf{a}^{(r)}$ 与 $\mathbf{a}^{(s)}$ 平移等价的充分必要条件是：有一非负整数 j，使同余式

$$s\equiv 2^j r \pmod{p}$$

成立．

证明：我们知道，对于任意的 $\beta\in GF(2^n)$，元素

$$\beta,\ \beta^2,\ \beta^{2^2},\ \cdots,\ \beta^{2^{n-1}}$$

有相同的极小多项式，而且如果 $\beta,\ \gamma\in GF(2^n)$ 有相同的极小多项式，那么一定有非负整数 j，使

$$\beta=\gamma^{2^j}.$$

因为两个 m 序列平移等价的充分必要条件是它们有相同的极小多项式，所以定理 8 不过是上述结论的另一种说法.

在整数模 p 的环中，全体可逆元素，也就是与 p 互素的数，对乘法组成一个群，记为 $Z/(p)^*$. 在这个群中，数

$$\{1,\ 2,\ 2^2,\ \cdots,\ 2^{n-1}\}$$

构成一个阶为 n 的子群，记为 H. 相对于子群 H，群 $Z/(p)^*$ 被分解成陪集

$$C_1=H,\ C_2,\ \cdots,\ C_t,$$

这里 $t=\varphi(2^n-1)/n$.

定理 8 换个说法就是：对于 $r,\ s\in Z/(p)^*$（这里我们把 $Z/(p)$ 中的元素记为 $0,\ 1,\ \cdots,\ p-1$），采样 $\mathbf{a}^{(r)}$ 与 $\mathbf{a}^{(s)}$ 平移等价的充分必要条件为 r，s 属于同一个陪集. 因之，如果我们从每个陪集中取一个数作为代表，这些代表组成一个集合 R，那么从任意一个 n 级 m 序列 $\mathbf{a}$ 出发，对每个 $r\in R$，作 $\mathbf{a}$ 的 r 采样 $\mathbf{a}^{(r)}$，我们就得到了全部 n 极的两两不平移等价的 m 序列. 因为与一个 m 序列平移等价的全部序列是很容易从这个序列写出来的，所以通过上述步骤，在知道了一个 n 级 m 序列之后，在原则上我们就可以得到全部的 n 级 m 序列. 下面来看一个例子：

取 $n=5$，于是 $p=2^5-1=31$.

$$Z/(31)^*=\{1,\ 2,\ 3,\ \cdots,\ 30\},$$

$$H=\{1,\ 2,\ 4,\ 8,\ 16\}.$$

$Z/(31)^*$ 被分解成陪集：

$$C_1 = H - \{1, 2, 4, 8, 16\},$$
$$C_2 = 3H - \{3, 6, 12, 24, 17\},$$
$$C_3 - 5H = \{5, 10, 20, 9, 18\},$$
$$C_4 = 7H = \{7, 14, 28, 25, 19\},$$
$$C_5 = 11H = \{11, 22, 13, 26, 21\},$$
$$C_6 = 15H - \{15, 30, 29, 27, 23\}.$$

在每个陪集中，譬如说，取最小的数作为代表，就有

$$R = \{1, 3, 5, 7, 11, 15\}.$$

取 $f(\lambda) = \lambda^5 + \lambda^2 + 1$，我们来证明：$f(\lambda)$ 是一个本原多项式. 由于 31 是素数，所以 5 次不可约多项式都是本原的，因而只要证明 $\lambda^5+\lambda^2+1$ 不可约就行了. 假如它可约，就一定要有一个 1 次或者 2 次的不可约因子. 1 次和 2 次的不可约多项式有

$$\lambda, \quad \lambda+1, \quad \lambda^2+\lambda+1.$$

由

$$f(0) = 1, \quad f(1) = 1$$

可知：λ, $\lambda+1$ 都不是 $f(\lambda)$ 的因子. 因为

$$\lambda^2+\lambda+1 \mid \lambda^3+1,$$

而

$$\lambda^5+\lambda^2+1 \equiv 1 \pmod{\lambda^3+1},$$

所以

$$\lambda^2+\lambda+1 \nmid \lambda^5+\lambda^2+1.$$

这就证明了 $\lambda^5+\lambda^2+1$ 不可约，从而它是一个本原多项式.

从初始状态 $(1, 0, 0, 0, 0)$ 出发，以 $f(\lambda)$ 作为反馈函数，得到一个周期为 31 的 m 序列：

$$\mathbf{a} = (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1,$$
$$1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, \cdots),$$

这里写出的是 $\mathbf{a}$ 的一个周期，以后就不断重复. 利用

$$a_k = a_{k+31} \quad (k = 0, 1, 2, \cdots),$$

立即可以写出

$$\mathbf{a}^{(3)}=(1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 1,\ 1,\ 1,$$
$$1,\ 0,\ 1,\ 1,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 1,\ 1,\ 0,\ \cdots).$$

同样可以写出 $\mathbf{a}^{(5)}$, $\mathbf{a}^{(7)}$, $\mathbf{a}^{(11)}$, $\mathbf{a}^{(15)}$(读者自己试一下). 而

$$\mathbf{a},\ \mathbf{a}^{(3)},\ \mathbf{a}^{(5)},\ \mathbf{a}^{(7)},\ \mathbf{a}^{(11)},\ \mathbf{a}^{(15)}$$

就是全部的两两不平移等价的5级 m 序列，其余的5级 m 序列必与其中之一平移等价. 这6个 m 序列的极小多项式也就是全部的5次本原多项式.

在知道了一个 m 序列之后，要求它的极小多项式是不难的，在下一章我们将介绍一种算法. 对于 n 级 m 序列，只要知道它的前 $2n$ 位就可以定出它的极小多项式了.

以上讨论说明：在我们知道了一个 n 次本原多项式之后，可以通过如下的步骤来求全部的 n 次本原多项式：

1. 把群 $Z/(p)^*$ 按子群

$$H=\{1,\ 2,\ 2^2,\ \cdots,\ 2^{n-1}\}$$

分解成陪集，在每一陪集中选一个代表，它们构成一集合 R，这里 $p=2^n-1$.

2. 以已知的本原多项式 $f(\lambda)$ 作为反馈函数，从初始状态 $(1,\ 0,\ \cdots,\ 0)$（或任意一个非零状态出发）生成一个 m 序列 $\mathbf{a}$.

3. 对每个 $r\in R$，作 $\mathbf{a}^{(r)}$（实际上只要求出 $\mathbf{a}^{(r)}$ 的前 $2n$ 位）.

4. 按下一章的算法求出 $\mathbf{a}^{(r)}$ 的极小多项式.

这样，我们在原则上就可以得到全部的 n 次本原多项式. 当 n 不太大时，整个过程不难在计算机上实现. 因之，重要的问题是如何找出第一个本原多项式. 现在有人已造出次数 $\leqslant 168$ 的本原多项式表，每次一个（见附录 II）.

定理8告诉我们：一个 m 序列的2采样总是与它平移等

价的. 现在问:有没有这样的 m 序列,它的 2 采样与它相等呢?下面的定理给了肯定的回答.

定理 9 设 $f(\lambda)$ 是一 n 次本原多项式,在 $G(f)$ 中存在唯一的 m 序列 $\mathbf{a}$,有

$$\mathbf{a}^{(2)}=\mathbf{a}.$$

证明:令 α 是 $f(\lambda)$ 的一个根,$\alpha\in GF(2^n)$. 我们知道:$G(f)$ 中的序列可以唯一地表示成

$$(Tr(\beta),\ Tr(\beta\alpha),\ Tr(\beta\alpha^2),\ \cdots),$$

其中 $\beta\in GF(2^n)$. 取 $\beta=1$,序列

$$\mathbf{a}=(Tr(1),\ Tr(\alpha),\ Tr(\alpha^2),\ \cdots)$$

就满足定理的要求,即 $\mathbf{a}^{(2)}=\mathbf{a}$. 事实上,令

$$\mathbf{a}=(a_0,\ a_1,\ a_2,\ \cdots),$$

$$\mathbf{a}^{(2)}=(b_0,\ b_1,\ b_2,\ \cdots),$$

其中 $a_k=Tr(\alpha^k),\ b_k=Tr(\alpha^{2k})$.

按定义,

$$\begin{aligned}b_k&=Tr(\alpha^{2k})=\alpha^{2k}+\alpha^{2^2k}+\cdots+\alpha^{2^nk}\\&=\alpha^{2k}+\alpha^{2^1k}+\cdots+\alpha^k=Tr(\alpha^k)=a_k.\end{aligned}$$

这就证明了 $\mathbf{a}^{(2)}=\mathbf{a}$.

再来证唯一性. 设

$$\mathbf{x}=(x_0,\ x_1,\ x_2,\ \cdots)$$

是 $G(f)$ 中一个 m 序列,适合 $\mathbf{x}^{(2)}=\mathbf{x}$. 对 $\mathbf{x}$ 有 $-\beta\in GF(2^n)$,使

$$x_k=Tr(\beta\alpha^k)\quad(k=0,\ 1,\ 2,\ \cdots).$$

$\mathbf{x}^{(2)}=\mathbf{x}$ 也就是

$$x_{2k}=x_k\quad(k=0,\ 1,\ 2,\ \cdots)$$

或者

$$Tr(\beta\alpha^{2k})=Tr(\beta\alpha^k)\quad(k=0,\ 1,\ 2,\ \cdots).$$

反复应用等式 $Tr(\beta\alpha^k)=Tr(\beta\alpha^{2k})$,即得

$$Tr(\beta\alpha^k)=Tr(\beta\alpha^{2k})=Tr(\beta\alpha^{2^2k})=\cdots$$
$$=Tr(\beta\alpha^{2^{n-1}k}) \quad (k=0,\ 1,\ 2,\ \cdots).$$

而 $$(\beta\alpha^{2^{n-1}k})^2=\beta^2\alpha^{2^nk}=\beta^2\alpha^k,$$

于是 $$Tr(\beta\alpha^k)=Tr(\beta\alpha^{2^{n-1}k})$$
$$=Tr((\beta\alpha^{2^{n-1}k})^2)$$
$$=Tr(\beta^2\alpha^k) \quad (k=0,\ 1,\ 2,\ \cdots).$$

由 LR 序列表示的唯一性，即得

$$\beta=\beta^2,$$
$$\beta=0 \text{ 或 } 1.$$

因为 $\mathbf{x}$ 是 m 序列，$\beta\neq 0$，所以 $\beta=1$，$\mathbf{x}=\mathbf{a}$，唯一性得证.

我们称适合关系 $\mathbf{a}^{(2)}=\mathbf{a}$ 的 m 序列为自然状态的 m 序列. 定理 9 换个说法就是：在 m 序列的每个平移等价类中都有唯一的一个自然状态的 m 序列.

因为 $Tr(\alpha^k)$ 的计算比较复杂，所以定理 9 虽然肯定了自然状态的 m 序列的存在，但是没有给出一个有效的方法来求它. 下面再针对这个问题作一些讨论.

对无穷序列 $\mathbf{a}$，我们定义

$$O\mathbf{a}=\mathbf{a}^{(2)}.$$

这就是说，把取一个序列的 2 采样看成是 $V(F)$ 上的一个变换. 显然，O 是 $V(F)$ 的一个线性变换，而且

$$O^2\mathbf{a}=\mathbf{a}^{(2^2)}.$$

一般地， $$O^i\mathbf{a}=\mathbf{a}^{(2^i)}.$$

定理 8 告诉我们：对于任意一个 n 次本原多项式 $f(\lambda)$，线性变换 O 以及 $O^i(i=1,\ 2,\ \cdots)$ 保持子空间 $G(f)$ 不变，也就是把 $G(f)$ 中的序列还变成 $G(f)$ 中的序列. 因之，$O^i(i=1,\ 2,\ \cdots)$ 可以看成 $G(f)$ 上的线性变换. 由于 $G(f)$ 中非零序列的周期都是 $p=2^n-1$，所以限制在 $G(f)$ 上，我们有

$$C^n = I,$$

这里 I 是单位变换.

顺便说一下，用线性变换的语言，定理 9 可以叙述成：在 $G(f)$ 中，线性变换 C 有唯一的一个对应于特征值 1 的特征向量.

定理 10 设 $f(\lambda)$ 是一 n 次本原多项式，α 是 $f(\lambda)$ 的一个根，而

$$\mathbf{a} = (Tr(1),\ Tr(\alpha),\ Tr(\alpha^2),\ \cdots)$$

是 $G(f)$ 中自然状态的 m 序列，于是对于 $G(f)$ 中任一个序列

$$\mathbf{b} = (b_0,\ b_1,\ b_2,\ \cdots)$$

有 $$\mathbf{b} + C\mathbf{b} + C^2\mathbf{b} + \cdots + C^{n-1}\mathbf{b} = b_0\mathbf{a}.$$

证明：取 $\beta \in GF(2^n)$，使

$$\mathbf{b} = (Tr(\beta),\ Tr(\beta\alpha),\ Tr(\beta\alpha^2),\ \cdots),$$

即 $$b_k = Tr(\beta\alpha^k) \quad (k = 0,\ 1,\ 2,\ \cdots).$$

令 $$\mathbf{b} + C\mathbf{b} + \cdots + C^{n-1}\mathbf{b} = \mathbf{c} = (c_0,\ c_1,\ c_2,\ \cdots),$$

于是
$$\begin{aligned} c_k &= b_k + b_{2k} + b_{2^2k} + \cdots + b_{2^{n-1}k} \\ &= Tr(\beta\alpha^k) + Tr(\beta\alpha^{2k}) + \cdots + Tr(\beta\alpha^{2^{n-1}k}) \\ &= Tr(\beta(\alpha^k + \alpha^{2k} + \cdots + \alpha^{2^{n-1}k})) \\ &= Tr(\beta)Tr(\alpha^k) = b_0a_k. \end{aligned}$$

这就证明了

$$\mathbf{c} = b_0\mathbf{a}. \ \blacksquare$$

定理 10 给出了一个求自然状态的 m 序列的方法. 对于任意一个本原多项式 $f(\lambda)$，取初始状态 $(1, 0, \cdots, 0)$，由反馈函数 $f(\lambda)$ 生成一个 m 序列 $\mathbf{b}$，作

$$\mathbf{b} + C\mathbf{b} + \cdots + C^{n-1}\mathbf{b},$$

因为 $b_0 = 1$，所以这就是 $G(f)$ 中自然状态的 m 序列.

第三章　综合算法

§1　问题的提出

前面在对 LR 序列的讨论中，我们总是假定已经知道了这个序列的极小多项式，也就是产生这个序列的级数最低的线性移位寄存器．在知道了一个序列之后，怎样求出它的极小多项式呢？这就是现在要讨论的问题．在实际问题中，我们当然不可能知道一个无穷序列，而所能知道的只不过是一段有限长的序列，在这种情况下，我们希望求出能够产生这一段序列的一个级数最低的线性移位寄存器．下面就来解决这个问题．在解决了这个问题之后，求 LR 序列的极小多项式的问题自然也就解决了．

下面我们把要解决的问题确切地提出来．设

$$\mathbf{a}=(a_0,\ a_1,\ \cdots,\ a_{N-1}) \tag{1}$$

是域 F(即 $GF(2)$)上的一个N位的序列，而

$$f(\lambda)=\lambda^n+c_{n-1}\lambda^{n-1}+\cdots+c_0 \tag{2}$$

是一线性移位寄存器的反馈函数．所谓这个线性移位寄存器能够产生序列 a，就是说：当初始状态是

$$(a_0,\ a_1,\ \cdots,\ a_{n-1})$$

时，它产生的序列的前 N 位正好就是 a，换句话说：等式

$$a_{n+k}+c_{n-1}a_{n+k-1}+\cdots+c_0a_k=0 \tag{3}$$

对于 $k=0,\ 1,\ \cdots,\ N-n-1$ 成立．

如果在有限序列(1)的后面添上一串 0，使它成为一个无限序列，那么所得的序列就可以看作空间 $V(F)$ 中的一个元

素. 以后我们总是把有限序列与这样得到的无限序列等同起来而不加区别. 在这个意义下，左移变换 L 对序列 $\mathbf{a}$ 是有意义的. 于是等式(3)就相当于说：序列 $f(L)\mathbf{a}$ 的前 $N-n$ 位全是 0. 以后我们就用这个说法来代替等式(3). 为了更方便地刻划一个序列的前若干位是 0 这个事实，我们引入下面的记号：

定义 1 设 m 是一正整数. $V^{(m)}$代表空间 $V(F)$中所有前 m 位是零的序列组成的集合. 当 $m\leqslant 0$ 时，约定 $V^{(m)}=V(F)$.

例如，$V^{(2)}$就是全体形如

$$(0,\ 0,\ a_2,\ a_3,\ \cdots)$$

的序列组成的集合.

容易验证：$V^{(m)}$是线性空间 $V(F)$的子空间，而且当 $m_1\leqslant m_2$ 时，有

$$V^{(m_1)}\supset V^{(m_2)}.$$

对于左移变换 L，有

$$LV^{(m)}\subset V^{(m-1)}.$$

一般地，如果 $g(\lambda)$是一个 r 次多项式，那么

$$g(L)V^{(m)}\subset V^{(m-r)}.$$

定义 2 对于 $\mathbf{a}$、$\mathbf{b}\in V(F)$，如果 $\mathbf{a}-\mathbf{b}$ 在 $V^{(m)}$中，那么就说 $\mathbf{a}$ 与 $\mathbf{b}$ 模 $V^{(m)}$同余，记为

$$\mathbf{a}\equiv\mathbf{b}(\mathrm{mod}\ V^{(m)}),$$

或者简记为

$$\mathbf{a}\equiv\mathbf{b}(V^{(m)}).$$

不难看出，当 $m>0$ 时，$\mathbf{a}\equiv\mathbf{b}(V^{(m)})$就意味着序列 $\mathbf{a}$ 与 $\mathbf{b}$ 的前 m 位分量相同. 当 $m\leqslant 0$ 时，$V^{(m)}=V(F)$，对于任意的序列 $\mathbf{a}$、$\mathbf{b}$ 都有

$$\mathbf{a}\equiv\mathbf{b}(V^{(m)}).$$

因之，在这个情况下，同余式对 $\mathbf{a}$、$\mathbf{b}$ 没有给任何约束.

容易验证：对于 $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in V(F)$，由

$$\mathbf{a} \equiv \mathbf{b}(V^{(m)}),\ \mathbf{c} \equiv \mathbf{d}(V^{m})$$

立即推出 $$\mathbf{a}+\mathbf{c} \equiv \mathbf{b}+\mathbf{d}(V^{(m)}).$$

如果 $g(\lambda)$是一 r 次多项式，那么由

$$\mathbf{a} \equiv \mathbf{b}(V^{(m)})$$

可知： $$g(L)\mathbf{a} \equiv g(L)\mathbf{b}(V^{(m-r)}).$$

显然，当 $m>0$ 时，$\mathbf{a} \equiv \mathbf{0}(V^{(m)})$，就相当于说：$\mathbf{a}$ 的前 m 位分量为 0.

在作了这些准备之后，我们可以对一个线性移位寄存器产生一个序列的前 N 位这件事给出另一个说法. 因为线性移位寄存器完全被它的反馈函数所刻划，所以下面只谈反馈函数，而不提线性移位寄存器.

定义 3 设 $\mathbf{a} \in V(F)$，$f(\lambda)$是一个 l 次的多项式. 如果

$$f(L)\mathbf{a} \equiv \mathbf{0}(V^{(k-l)}),$$

那么我们就说：$f(\lambda)$可以产生序列 $\mathbf{a}$ 的前 k 位.

显然，这个说法与开始的分析是一致的.

因为当 $m \leqslant 0$ 时，$V^{(m)}=V(F)$，所以当 $l \geqslant k$ 时，任意一个 l 次多项式都可以产生一个序列的前 k 位.

为了以后叙述方便，在定义 3 中可以包括 $k=0$ 的情形. 按定义：任意一个非零多项式都可以产生一个序列的前 0 位. 显然，$f(\lambda)=1$，即 $f(\lambda)$是零次多项式，是可以产生一个序列的前 0 位的次数最低的多项式.

定义 4 对于正整数 k，我们用 $\mathbf{e}_k$ 代表第 k 位分量是 1，而其余分量全是 0 的序列.

例如， $$\mathbf{e}_1=(1, 0, 0, \cdots),$$

$$\mathbf{e}_2=(0, 1, 0, \cdots).$$

显然，$\mathbf{e}_k \equiv \mathbf{0}(V^{(k-1)})$；当 $r<k$ 时，$L^r\mathbf{e}_k = \mathbf{e}_{k-r}$；$\mathbf{e}_k \not\equiv \mathbf{0}(V^{(k)})$. 由此可知：零次多项式 $f(\lambda)=1$ 可以产生 $\mathbf{e}_k$ 的前 $k-1$ 位. 如果 $f(\lambda)$ 的次数 $l<k$，那么

$$f(L)\mathbf{e}_k = \mathbf{e}_{k-l}(V^{(k-l)}),$$

这就是说：任意一个次数小于 k 的多项式都不可能产生 $\mathbf{e}_k$ 的前 k 位. 因之，产生 $\mathbf{e}_k$ 的前 k 位的最低次多项式的次数是 k. 根据定义 3. 任意一个 k 次多项式都可以产生 $\mathbf{e}_k$ 的前 k 位. 以后为了确定起见，我们总是取

$$\lambda^k+1$$

作为产生 $\mathbf{e}_k$ 的前 k 位的一个最低次的多项式.

§2 迭代算法

现在来解决最开始提出的问题. 确切地说，那问题就是：对于任意的序列 $\mathbf{a}\in V(F)$，对于任意的正整数 N，要找出一个次数最低的多项式 $f_N(\lambda)$，它可以产生序列 $\mathbf{a}$ 的前 N 位.

应该指出：从以下的讨论可以看出，在求 $f_N(\lambda)$ 时，不牵涉到序列 $\mathbf{a}$ 的第 N 位以后的分量，因之总可以认为所给的序列是 $V(F)$ 中的无限序列. 我们称下面给出的求 $f_N(\lambda)$ 的算法为迭代算法，这是因为对于 $0\leqslant n\leqslant N$，我们的算法是依次地求可产生序列 $\mathbf{a}$ 的前 n 位的一个次数最低的多项式 $f_n(\lambda)$，而算法的主要步骤就是在已经有了 $f_i(\lambda)(i=0,1,\cdots,n)$ 之后，如何求出 $f_{n+1}(\lambda)$.

在给出算法之前，我们先证明两条引理.

引理 1 设 $\mathbf{a}\in V(F)$，$n\geqslant 0$，多项式 $f(\lambda)$ 可以产生 $\mathbf{a}$ 的前 n 位，但不能产生 $\mathbf{a}$ 的前 $n+1$ 位，$f(\lambda)$ 的次数为 l. 如果多项式 $g(\lambda)$ 可以产生 $\mathbf{a}$ 的前 $n+1$ 位，$g(\lambda)$ 的次数为 l'，那么

$$l'\geqslant n+1-l.$$

证明：根据条件，有

$$f(L)\mathbf{a}\equiv\mathbf{0}(V^{(n-l)}), \tag{1}$$

$$g(L)\mathbf{a}\equiv\mathbf{0}(V^{(n+1-l')}), \tag{2}$$

而

$$f(L)\mathbf{a}\not\equiv\mathbf{0}(V^{(n+1-l)}), \tag{3}$$

由(1)，(3)可知

$$f(L)\mathbf{a}\equiv\mathbf{e}_{n+1-l}(V^{(n+1-l)}). \tag{4}$$

用反证法：假如不等式不成立，即

$$l'<n+1-l.$$

于是由(4)以及上一节的讨论可知：

$$g(L)f(L)\mathbf{a}\equiv\mathbf{e}_{n+1-l-l'}(V^{(n+1-l-l')}),$$

即

$$g(L)f(L)\mathbf{a}\not\equiv\mathbf{0}(V^{(n+1-l-l')}).$$

但是用 $f(L)$ 作用在(2)的两边却有

$$f(L)g(L)\mathbf{a}=g(L)f(L)\mathbf{a}\equiv\mathbf{0}(V^{(n+1-l-l')}).$$

这是矛盾的，因而不等式必成立. ∎

由引理1即得

引理2 设 $\mathbf{a}\in V(F)$，$n\geqslant 0$，$f_n(\lambda)$ 是可以产生 $\mathbf{a}$ 的前 n 位的一个次数最低的多项式，次数为 l_n，而 $g(\lambda)$ 是一个可以产生 $\mathbf{a}$ 的前 $n+1$ 位的多项式，次数为 l. 于是有

$$l\geqslant l_n,$$

而当 $f_n(\lambda)$ 不能产生 $\mathbf{a}$ 的前 $n+1$ 位时，有

$$l\geqslant\max(l_n,\ n+1-l_n).$$

证明：因为可以产生 $\mathbf{a}$ 的前 $n+1$ 位的多项式，当然可以产生 $\mathbf{a}$ 的前 n 位，所以 $l\geqslant l_n$ 是明显的.

当 $f_n(\lambda)$ 不能产生 $\mathbf{a}$ 的前 $n+1$ 位时，由引理1：$l\geqslant n+1-l_n$. 结合这两个不等式，就有 $l\geqslant\max(l_n,\ n+1-l_n)$.

下面来给出迭代算法：对于 $\mathbf{a}\in V(F)$，我们定义

$$f_0(\lambda)=1,$$

显然 $f_0(\lambda)$ 是可以产生 a 的前 0 位的一个次数最低的多项式. 假设已经有了 $f_0(\lambda)$, $f_1(\lambda)$, …, $f_n(\lambda)$, 它们分别是可以产生序列 a 的前0, 1, …, n 位的多项式, 次数分别为 $l_0, l_1, \cdots, l_n$, 而且 $l_0 \leqslant l_1 \leqslant \cdots \leqslant l_n$. 下面分几种情况来求 $f_{n+1}(\lambda)$:

1) 如果 $f_n(\lambda)$ 能产生 a 的前 $n+1$ 位, 那么就取 $f_{n+1}(\lambda)=f_n(\lambda)$. 这里 $l_{n+1}=l_n$.

2) 如果 $f_n(\lambda)$ 不能产生 a 的前 $n+1$ 位, 那么再区别以下的情形:

2.1) $l_0=l_1=\cdots=l_n$.

因为 $l_0=0$, 所以 $l_0=l_1=\cdots=l_n=0$. 这就是说: 在序列 a 中有

$$a_0=a_1=\cdots=a_{n-1}=0, \text{而 } a_n\neq 0,$$

或者说

$$\mathbf{a}\equiv \mathbf{e}_{n+1}(V^{(n+1)}).$$

取 $f_{n+1}(\lambda)=\lambda^{n+1}+1$, $l_{n+1}=n+1$. 我们知道: 可以产生 $\mathbf{e}_{n+1}$ 的前 $n+1$ 位的多项式至少是 $n+1$ 次的, 因之, $f_{n+1}(\lambda)$ 是可以产生 a 的前 $n+1$ 位的一个次数最低的多项式. 这时, $l_n<l_{n+1}$.

2.2) 在 $l_0, l_1, \cdots, l_{n-1}$ 中有一个比 l_n 小. 设 l_m 是最后一个比 l_n 小的数, 即

$$l_m<l_{m+1}=\cdots=l_n.$$

按作法 1): $f_m(\lambda)$ 一定不能产生 a 的前 $m+1$ 位, 即

$$f_m(L)\mathbf{a}\equiv \mathbf{e}_{m-l_m+1}(V^{(m-l_m+1)}). \tag{5}$$

因为 $f_n(\lambda)$ 不能产生 a 的前 $n+1$ 位, 所以

$$f_n(L)\mathbf{a}\equiv \mathbf{e}_{n-l_n+1}(V^{(n-l_n+1)}). \tag{6}$$

再分两种情形:

2.2.1) $n-l_n+1\leqslant m-l_m+1$

由(5)、(6)，有

$$[f_n(L)-L^{(m-l_m)-(n-l_n)}f_m(L)]\mathbf{a}$$
$$\equiv \mathbf{0}(V^{(n+1-l_n)}). \tag{7}$$

因为 $\lambda^{(m-l_m)-(n-l_n)}f_m(\lambda)$ 的次数为

$$(m-l_m)-(n-l_n)+l_m=l_n-(n-m)<l_n,$$

所以多项式 $f_n(\lambda)-\lambda^{(m-l_m)-(n-l_n)}f_m(\lambda)$ 的次数为 l_n. (7)式表明：这个多项式可以产生序列 a 的前 $n+1$ 位. 我们就取它为 $f_{n+1}(\lambda)$，这时 $l_{n+1}=l_n$.

2.2.2) $n-l_n+1>m-l_m+1$

由(5)、(6)，有

$$[L^{(n-l_n)-(m-l_m)}f_n(L)-f_m(L)]\mathbf{a}$$
$$\equiv \mathbf{0}(V^{(m+1-l_m)}). \tag{8}$$

因为 $\lambda^{(n-l_n)-(m-l_m)}f_n(\lambda)$ 的次数为

$$(n-l_n)-(m-l_m)+l_n=(n-m)+l_m>l_m,$$

所以 $\lambda^{(n-l_n)-(m-l_m)}f_n(\lambda)-f_m(\lambda)$ 是一个次数为 $(n-m)+l_m$ 的多项式. 显然

$$m+1-l_m=(n+1)-[(n-m)+l_m],$$

因之，(8)式表明，取

$$f_{n+1}(\lambda)=\lambda^{(n-l_n)-(m-l_m)}f_n(\lambda)-f_m(\lambda),$$

$f_{n+1}(\lambda)$ 可以产生 a 的前 $n+1$ 位，这时，

$$l_{n+1}=(n-l_n)-(m-l_m)+l_n>l_n.$$

综合以上各种情形，我们都求出了 $f_{n+1}(\lambda)$，它可以产生 a 的前 $n+1$ 位，而且 $f_{n+1}(\lambda)$ 的次数 $l_{n+1}\geqslant l_n$. 这就是迭代算法，它给出了依次构造多项式 $f_0(\lambda)$，$f_1(\lambda)$，…的步骤，其中 $f_n(\lambda)$ 可以产生序列 a 的前 n 位. 在实际应用中，所给的序列常常是有限长的，这一点并不影响以上算法的应用，因为在构造 $f_n(\lambda)$ 时，结果与 n 位以后的分量无关. 如果所给的序列

是 N 位的，那么只要算到 $f_N(\lambda)$就行了.

要判断可以产生前 n 位的多项式 $f_n(\lambda)$ 能不能产生前 $n+1$ 位是容易的. 设多项式

$$f_n(\lambda)=\lambda^{l_n}+c_1\lambda^{l_n-1}+\cdots+c_{l_n}$$

可以产生序列 $\mathbf{a}=(a_0, a_1, \cdots)$的前 n 位，令

$$d_n=a_n+c_1a_{n-1}+\cdots+c_{l_n}a_{n-l_n}.$$

如果 $d_n=0$，那么 $f_n(\lambda)$就能够产生 $\mathbf{a}$ 的前 $n+1$ 位，否则，$f_n(\lambda)$就不能产生 $\mathbf{a}$ 的前 $n+1$ 位.

下面我们来证明：由以上算法作出的多项式都是次数最低的.

定理 1 设 $\mathbf{a}\in V(F)$，而

$$f_0(\lambda), f_1(\lambda), \cdots, f_n(\lambda), \cdots$$

是按迭代算法造出的多项式，$f_n(\lambda)$的次数为 $l_n(n=0, 1, \cdots)$. 于是 $f_n(\lambda)$是可以产生 $\mathbf{a}$ 的前 n 位的一个次数最低的多项式，在 $f_n(\lambda)$不能产生 $\mathbf{a}$ 的前 $n+1$ 位的情形下，我们有

$$l_{n+1}=\max(l_n, n+1-l_n) \quad (n=0, 1, \cdots).$$

证明：我们对 n 作归纳法：

$n=0$ 时，结论是显然的.

假设定理的结论对于多项式

$$f_0(\lambda), f_1(\lambda), \cdots, f_n(\lambda)$$

成立.

如果 $f_n(\lambda)$也能产生前 $n+1$ 位，那么按算法，$f_{n+1}(\lambda)=f_n(\lambda)$，$l_{n+1}=l_n$，既然 l_n 是可以产生 $\mathbf{a}$ 的前 n 位的多项式的最低次数，$l_{n+1}=l_n$ 当然也是可以产生 $\mathbf{a}$ 的前 $n+1$ 位的多项式的最低次数.

如果 $f_n(\lambda)$不能产生 $\mathbf{a}$ 的前 $n+1$ 位，根据引理 2，只要证明了 $l_{n+1}=\max(l_n, n+1-l_n)$，$l_{n+1}$ 必然就是可以产生 $\mathbf{a}$ 的

前 $n+1$ 位的多项式的最低次数. 下面分三种情形来看:

1) $l_0=l_1=\cdots=l_n=0$.

这时, $f_{n+1}(\lambda)=\lambda^{n+1}+1$, $l_{n+1}=n+1$, 显然有

$$l_{n+1}=n+1=\max(0,\ n+1)=\max(l_n,\ n+1-l_n).$$

2) 有 $m<n$ 使 $l_m<l_{m+1}=\cdots=l_n$, 且

$$n-l_n+1\leqslant m-l_m+1.$$

这时, $l_{n+1}=l_n$. 由引理 2, $l_{n+1}\geqslant\max(l_n,\ n+1-l_n)$, 因而等式成立.

3) 有 $m<n$ 使 $l_m<l_{m+1}=\cdots=l_n$, 而

$$n-l_n+1>m-l_m+1.$$

这时, $l_{n+1}=(n-m)+l_m$. 根据归纳法假定, 由 $l_m<l_{m+1}$ 可知 $f_m(\lambda)$ 不能产生 a 的前 $m+1$ 位, 于是 $l_{m+1}=\max(l_m,\ m+1-l_m)$. 再由 $l_m<l_{m+1}$, 可知

$$l_n=l_{m+1}=m+1-l_m.$$

因之,

$$\begin{aligned}l_{n+1}&=(n-m)+l_m=n-(m-l_m)\\&=n-(l_n-1)=n+1-l_n.\end{aligned}$$

由引理 2, 即得

$$l_{n+1}=\max(l_n,\ n+1-l_n).$$

根据归纳法原理: 定理的结论普遍成立. ∎

定理 1 表明, 迭代算法对于任意一个 $\mathbf{a}\in V(F)$, 都给出一串多项式 $f_0(\lambda)$, $f_1(\lambda)$, $\cdots$, $f_n(\lambda)$, $\cdots$, 其中 $f_n(\lambda)$ 是可以产生 a 的前 n 位的一个次数最低的多项式. 一般地说, 可以产生 a 的前 n 位的次数最低的多项式不是唯一的, 可是这个最低的次数 l_n 是由 a 的前 n 位唯一决定的. 根据迭代算法及定理 1, 关于这些次数有以下的结论:

定理 2 设 $\mathbf{a}\in V(F)$, 而 l_n 是可以产生 a 的前 n 位的最低次多项式的次数($n=0,\ 1,\ 2,\ \cdots$). 于是

1) $0=l_0\leqslant l_1\leqslant\cdots\leqslant l_n\leqslant\cdots$;

2) $l_{n+1}=l_n$ 或者 $l_{n+1}=n+1-l_n$;

3) 如果 $2l_n>n$, 那么 $l_{n+1}=l_n$;

4) 如果有 $m<n$ 使 $l_m<l_{m+1}=\cdots=l_n<l_{n+1}$, 那么

$$(n+1)-l_{n+1}=(m+1)-l_m.$$

证明: 1), 2)是显然的.

对于 3), 用反证法: 假如 $l_{n+1}\neq l_n$, 就有

$$l_n<l_{n+1}=n+1-l_n.$$

于是 $$2l_n<n+1 \text{ 或者 } 2l_n\leqslant n,$$

这与所给条件相矛盾, 因之 $l_{n+1}=l_n$.

对于 4), 根据算法, 由 $l_n<l_{n+1}$ 可知

$$l_{n+1}=n-m+l_m,$$

即 $$(n+1)-l_{n+1}=(m+1)-l_m.$$

下面来看一个例子. 设

$$\mathbf{a}=(1001000111),$$

用迭代算法来求产生这 10 位序列的一个最低次多项式.

对于 $n=0$, 首先取

$$f_0(\lambda)=1,\quad l_0=0.$$

$d_0=a_0=1$, 按§ 2 的 2.1), 取

$$f_1(\lambda)=\lambda+1,\quad l_1=1.$$

$d_1=a_1+a_0=1$, 按§ 2 的 2.2.1), 取

$$f_2(\lambda)=f_1(\lambda)+f_0(\lambda)=\lambda,\quad l_2=1.$$

$d_2=a_2=0$, 按§ 2 的 1), 取

$$f_3(\lambda)=f_2(\lambda)=\lambda,\quad l_3=1.$$

$d_3=a_3=1$, 这时

$$l_0<l_1=l_2=l_3,$$

即 $m=l_m=0$, $n=3$, $l_3=1$, 按§ 2 的 2.2.2), 取

$$f_4(\lambda)=\lambda^2 f_3(\lambda)+f_0(\lambda)=\lambda^3+1,\quad l_4=3.$$

$d_4=a_4+a_1=0$, 按§2的1),取

$$f_5(\lambda)=f_4(\lambda)=\lambda^3+1,\quad l_5=3.$$

$d_5=a_5+a_2=0$, 按§2的1), 取

$$f_6(\lambda)=f_5(\lambda)=\lambda^3+1,\quad l_6=3.$$

$d_6=a_6+a_3=1$, 这时

$$l_3<l_4=l_5=l_6,$$

即 $m=3$, $l_3=1$, $n=6$, $l_6=3$,

$$(6-l_6)-(3-l_3)=1,$$

按§2的2.2.2), 取

$$f_7(\lambda)=\lambda f_6(\lambda)+f_3(\lambda)=\lambda^4,\quad l_7=4.$$

$d_7=a_7=1$, 按§2的2.2.1),取

$$f_8(\lambda)=f_7(\lambda)+f_6(\lambda)=\lambda^4+\lambda^3+1,\quad l_8=4.$$

$d_8=a_8+a_7+a_4=0$, 按§2的1), 取

$$f_9(\lambda)=f_8(\lambda)=\lambda^4+\lambda^3+1,\quad l_9=4.$$

$d_9=a_9+a_8+a_5=0$, 按§2的1), 取

$$f_{10}(\lambda)=f_9(\lambda)=\lambda^4+\lambda^3+1,\quad l_{10}=4.$$

$\lambda^4+\lambda^3+1$ 就是产生 a 这个10位序列的一个最低次的多项式.

显然,迭代算法很容易在计算机上实现,占用的存贮量不大.

§3 唯一性问题

在前面已经指出,对于任意的序列 a,能够产生 a 的前 N 位的最低次多项式不一定是唯一的, 现在就来讨论在什么条件下它是唯一的.

引理3 设 $\mathbf{a}\in V(F)$, $f_N(\lambda)$是产生 a 的前 N 位的一个

次数最低的多项式，次数为 l_N. 如果 $\mathbf{b}$ 是 $G(f_N)$ 中以 $\mathbf{a}$ 的前 l_N 位作为初始状态的序列，那么

1) $\mathbf{a}\equiv\mathbf{b}(V^{(N)})$;

2) $\mathbf{b}$ 的极小多项式为 $f_N(\lambda)$.

证明：因为 $\mathbf{a}$ 的前 N 位能够被 $f_N(\lambda)$ 产生，所以 $\mathbf{a}$ 的前 N 位完全被 $\mathbf{a}$ 的前 l_N 位按 $f_N(\lambda)$ 所表示的线性关系唯一决定. $\mathbf{b}$ 的分量也是被它的前 l_N 位(初始状态)按 $f_N(\lambda)$ 所表示的线性关系唯一决定，因之 $\mathbf{b}$ 的前 N 位与 $\mathbf{a}$ 的前 N 位完全一样，这就是 1).

至于 2)，由于 $\mathbf{b}\in G(f_N)$，当然有

$$f_N(L)\mathbf{b}=\mathbf{0}.$$

如果 $\mathbf{b}$ 的极小多项式不是 $f_N(\lambda)$，就有一个次数比 l_N 低的多项式 $g(\lambda)$ 使

$$g(L)\mathbf{b}=\mathbf{0},$$

那么 $g(\lambda)$ 就可以产生 $\mathbf{b}$ 的前 N 位. 因为 $\mathbf{a}$ 与 $\mathbf{b}$ 的前 N 位相同，所以 $g(\lambda)$ 也可以产生 $\mathbf{a}$ 的前 N 位. 这与 $f_N(\lambda)$ 是次数最低这一点相矛盾，因之，$f_N(\lambda)$ 是 $\mathbf{b}$ 的极小多项式. ∎

定理 3 设 $\mathbf{a}\in V(F)$，l_N 是可以产生 $\mathbf{a}$ 的前 N 位的最低次多项式的次数. 于是能够产生 $\mathbf{a}$ 的前 N 位的最低次多项式是唯一的充分必要条件为 $2l_N\leqslant N$.

证明：先证充分性. 设 $2l_N\leqslant N$.

假如 $f(\lambda)$、$g(\lambda)$ 是两个次数为 l_N 的多项式，它们都能够产生 $\mathbf{a}$ 的前 N 位. 在 $G(f)$ 中取序列 $\mathbf{b}$，它以 $\mathbf{a}$ 的前 l_N 位作为初始状态. 由引理 3，$\mathbf{b}$ 的前 N 位与 $\mathbf{a}$ 的前 N 位相同，因之多项式 $g(\lambda)$ 能够产生 $\mathbf{b}$ 的前 N 位，即

$$g(L)\mathbf{b}\equiv\mathbf{0}(V^{(N-l_N)})$$

这就是说,序列 $g(L)\mathbf{b}$的前 $N-l_N$ 位为 0. 由条件, $N-l_N \geqslant l_N$, 而显然 $g(L)\mathbf{b} \in G(f)$, 在 $G(f)$中前 l_N 位为 0 的序列只有零序列,由此得

$$g(L)\mathbf{b}=\mathbf{0}.$$

根据引理 3, $\mathbf{b}$ 的极小多项式是 $f(\lambda)$, 因之

$$f(\lambda)\mid g(\lambda).$$

由 $f(\lambda)$ 与 $g(\lambda)$有相同的次数,即得

$$f(\lambda)=g(\lambda),$$

这就证明了唯一性.

假设 $2l_N>N$,我们来证,至少有两个次数为 l_N 的多项式,它们都能产生 $\mathbf{a}$ 的前 N 位.

考虑序列 $\mathbf{a}$ 与 $\mathbf{a}+\mathbf{e}_{N+1}$, 这两个序列的前 N 位相同, 而第 $N+1$ 位不同. 如果 $f(\lambda)$是一个能够产生 $\mathbf{a}$ 的前 N 位的最低次多项式, 次数为 l_N, $f(\lambda)$也是能够产生 $\mathbf{a}+\mathbf{e}_{N+1}$ 的前 N 位的一个次数最低的多项式. 设 $g_1(\lambda)$、$g_2(\lambda)$分别是能够产生 $\mathbf{a}$、$\mathbf{a}+\mathbf{e}_{N+1}$的前 $N+1$ 位的次数最低的多项式. 根据定理 2 的 3),多项式 $g_1(\lambda)$、$g_2(\lambda)$的次数也都是 l_N. 显然 $g_1(\lambda) \neq g_2(\lambda)$, 而它们都能产生 $\mathbf{a}$ 的前 N 位. ∎

推论 1 设 $\mathbf{a} \in V(F)$, l_N 是产生 $\mathbf{a}$ 的前 n 位的最低次多项式的次数($n=0, 1, 2, \cdots$). 如果对某个 $N>0$ 有 $2l_N \leqslant N$, 那么对于任意的 k, $2l_N \leqslant k \leqslant N$, 都有 $l_k=l_N$, 而且那个唯一的产生 $\mathbf{a}$ 的前 N 位的次数最低的多项式 $f_N(\lambda)$也是产生 $\mathbf{a}$ 的前 k 位的唯一的次数最低的多项式.

证明:用反证法. 假设有一个 k,

$$2l_N \leqslant k < N,$$

使 $l_k \neq l_N$. 取 k_0为适合这个不等式的最大下标, 由定理 2 的 2), 有

$$l_N = l_{k_0+1} = k_0 + 1 - l_{k_0}.$$

因为 $k_0 \geqslant 2l_N$, $l_{k_0} < l_N$, 所以

$$l_N > 2l_N + 1 - l_N = l_N + 1.$$

这是矛盾的，因而 $l_k = l_N$. 结论的其余部分由定理 3 的唯一性即得. ∎

由定理 3 和推论 1 可知

推论 2 如果 **a** 是一个以 $f(\lambda)$为极小多项式的 LR 序列，$f(\lambda)$的次数为 l，那么按迭代算法算出的 $f_{2l}(\lambda)$就是 $f(\lambda)$.

这个结果表明，迭代算法也是求一个 LR 序列的极小多项式的有效方法.

第四章　线性自动机的基本概念

§1　线性自动机的定义

在计算机、通讯设备以及自动控制的装置中，线性移位寄存器只是一种非常特殊的线路．比线性移位寄存器更广一些，同时也是常用的所谓线性反馈线路（或称线性时序线路）．线性自动机就是这类线路的一个数学抽象，它包括线性移位寄存器作为一个特殊情形，对它的研究是对线性移位寄存器研究的一个自然的继续，也是一个有意义的补充．这一章就是介绍线性自动机的概念，并对它的性质作一些初步的讨论．

在给出线性自动机的定义之前，先简单地介绍一下自动机的概念．自动机是在出现了电子计算机之后逐步形成的一个数学概念．自动机的框图如图 4-1．自动机的变化是按离散的时间节拍进行的，自动机的内部结构除去有信号转换的功能外，还有记忆的功能，因而在每一特定的时刻，它都处于一特定的状态．在给了一组输入信号之后，一方面自动机给出一组相应的输出信号，另一方面，自动机的内部状态也发生变化．当然，在每一时刻，自动机的输出既依赖于输入，也依赖于原来自动机的内部状态，而自动机的下一时刻的内部状态也是既依赖于输入，也依赖于原来自动机的状态．所谓定义一个自动机，就是给出：可能的输入组成的集合、全部

图　4-1

状态的集合、可能的输出组成的集合以及输出对于输入和内部状态的依赖关系、下一时刻的状态对于输入和原来的状态的依赖关系. 显然，自动机是一个非常广泛的概念. 我们不打算对一般的自动机作什么讨论，而是给出适当的限制，得出线性自动机的概念.

首先，假如自动机有 r 个输入端，每个输入端在每个时刻都有两种可能的信号，那么就可以同处理线性移位寄存器的办法一样，用域 F（即 $GF(2)$）中的两个元素 0 与 1 来代表这两个信号. 这样，自动机在每个时刻的输入就可以用域 F 上的一个 r 维向量

$$u=(u_1,\ u_2,\ \cdots,\ u_r)$$

来表示. 同样，假如自动机有 m 个输出端，它的输出可以用域 F 上的 m 维向量

$$y=(y_1,\ y_2,\ \cdots,\ y_m)$$

来表示. 如果自动机的线路中有 n 个记忆元件，那么它在每一时刻的内部状态就可以用域 F 上的一个 n 维向量

$$s=(s_1,\ s_2,\ \cdots,\ s_n)$$

来表示.

因为自动机是按离散的时间节拍变化的，所以我们用

$$u(t)=(u_1(t),\ \cdots,\ u_r(t)),$$
$$y(t)=(y_1(t),\ \cdots,\ y_m(t)),$$
$$s(t)=(s_1(t),\ \cdots,\ s_n(t))$$

分别代表自动机在时刻 t 的输入、输出与状态，而 t 的取值为 0, 1, 2, ….

如果在自动机的输入、输出与状态之间有关系：

$$s(t+1)=s(t)A+u(t)B, \tag{1}$$
$$y(t)=s(t)C+u(t)D. \tag{2}$$

其中 A 是 $n\times n$ 矩阵; B 是 $r\times n$ 矩阵; C 是 $n\times m$ 矩阵; D 是 $r\times m$ 矩阵; $t=0, 1, 2, \cdots$. 那么这样的自动机就称为线性自动机. 矩阵 A, B, C, D 称为线性自动机的刻划矩阵. 线性自动机的状态的维数 n (即线路中记忆元件的个数)称为线性自动机的维数.

例如, 图 4-2 所示的线路就表示一个 4 维的线性自动机. 图中"⊕"代表加法器. 按图中线路可以看出:

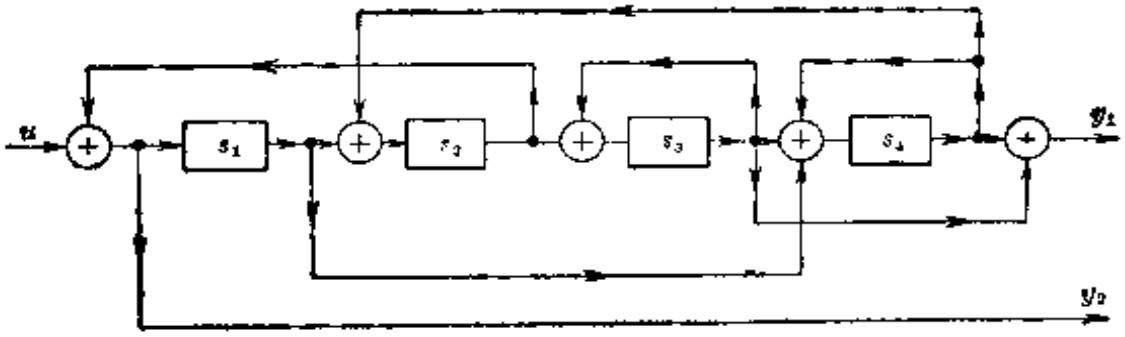


图 4-2

$$
\begin{aligned}
&s_1(t+1)=s_2(t)+u(t),\\
&s_2(t+1)=s_1(t)+s_4(t),\\
&s_3(t+1)=s_2(t)+s_3(t),\\
&s_4(t+1)=s_1(t)+s_3(t)+s_4(t),\\
&y_1(t)=s_3(t)+s_4(t),\\
&y_2(t)=s_2(t)+u(t).
\end{aligned}
$$

用矩阵写出来, 就是

$$
s(t+1)=s(t)\begin{pmatrix}0&1&0&1\\1&0&1&0\\0&0&1&1\\0&1&0&1\end{pmatrix}+u(t)(1\ 0\ 0\ 0),
$$

$$y(t)=s(t)\begin{pmatrix}0&0\\0&1\\1&0\\1&0\end{pmatrix}+u(t)\,(0\ 1).$$

这个线性自动机的刻划矩阵就是

$$A=\begin{pmatrix}0&1&0&1\\1&0&1&0\\0&0&1&1\\0&1&0&1\end{pmatrix},\quad B=(1\ 0\ 0\ 0),$$

$$C=\begin{pmatrix}0&0\\0&1\\1&0\\1&0\end{pmatrix},\quad D=(0\ 1).$$

显然，线性移位寄存器是线性自动机的一个特殊情形. 譬如图 4-3 所示的线性移位寄存器的刻划矩阵为

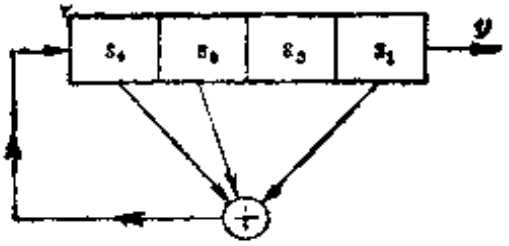


图 4-3

$$A=\begin{pmatrix}0&0&0&1\\1&0&0&0\\0&1&0&1\\0&0&1&1\end{pmatrix},\quad B=0,$$

$$C=\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\quad D=0.$$

因为线性移位寄存器没有输入，所以矩阵 B 与 D 全为 0.

如果线性自动机 M 的输入、输出与状态集合分别是域 F 上的 r 维、m 维与 n 维的向量空间，那么 M 就称为一个 (r, m, n) 自动机.

对于线性自动机，只要确定了它的初始状态 $s(0)$，任意一串输入序列

$$u(0),\ u(1),\ \cdots,\ u(T)$$

就决定一串输出序列

$$y(0),\ y(1),\ \cdots,\ y(T),$$

同时也就决定一串状态序列

$$s(0),\ s(1),\ \cdots,\ s(T),\ s(T+1).$$

由公式(1)、(2)，不难得出

$$\begin{aligned}s(1)&=s(0)A+u(0)B,\\ s(2)&=s(1)A+u(1)B\\ &=[s(0)A+u(0)B]A+u(1)B\\ &=s(0)A^2+u(0)BA+u(1)B,\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\end{aligned}$$

一般地，

$$s(t+1)=s(0)\,A^{t+1}+\sum_{j=0}^{t}u(j)BA^{t-j}\quad(t=0,\ 1,\ \cdots,\ T).\tag{3}$$

这里约定 $A^0=I$. 同样地，利用(2)、(3)可得

$$\begin{aligned}y(0)&=s(0)C+u(0)D,\\ y(1)&=s(1)C+u(1)D\end{aligned}\tag{4}$$

$$
\begin{aligned}
&= [s(0)A + u(0)B]C + u(1)D \\
&= s(0)AC + u(0)BC + u(1)D \\
y(2) &= s(2)C + u(2)D \\
&= [s(0)A^2 + u(0)BA + u(1)B]C + u(2)D \\
&= s(0)A^2C + u(0)BAC + u(1)BC + u(2)D, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}
$$

一般地，

$$
\begin{aligned}
y(t) &= s(t)C + u(t)D \\
&= \left[s(0)A^t + \sum_{j=0}^{t-1} u(j)BA^{t-j-1}\right]C + u(t)D \\
&= s(0)A^tC + \sum_{j=0}^{t-1} u(j)BA^{t-j-1}C + u(t)D \\
&\qquad (t = 1, \cdots, T). \qquad (5)
\end{aligned}
$$

公式(3)，(4)，(5)给出了由输入序列到输出序列的一般的转换公式.

§2 自动机的等价、同构与相似

自动机的功能主要是实现由输入到输出的转换，至于自动机的内部状态及其转移，不过是实现由输入到输出的转换的必要手段. 从这个观点，我们对于自动机引入下面的概念.

设 M_1 是一个(r, m, n_1)自动机，M_2是一个(r, m, n_2)自动机. 这里 M_1 与 M_2 有相同的输入与输出空间，而它们的状态空间则不一定相同. 设 $s^{(1)}$是 M_1 的一个状态，$s^{(2)}$是 M_2 的一个状态. 如果当 M_1 的初始状态处于 $s^{(1)}$，M_2 的初始状态处于 $s^{(2)}$时，对于任意一串输入序列，M_1 与 M_2 都给出相同的输出序列，那么我们就说 M_1 的状态 $s^{(1)}$ 与 M_2 的状态 $s^{(2)}$ 是等价的. 如果对于 M_1的每一个状态，都有 M_2 的一个状态

与之等价. 反过来,对于 M_2 的每一个状态也都有 M_1 的一个状态与之等价. 则称线性自动机 M_1 与 M_2 等价. 显然,等价的线性自动机可以实现相同的由输入到输出的转换. 因之,在功能上等价的线性自动机可以互相代替.

如果在线性自动机 M_1 与 M_2 的状态之间可以建立一个 1-1 对应,使相互对应的状态是等价的,那么就说,自动机 M_1 与 M_2 是同构的. 显然,同构的自动机必然等价. 同构的自动机有相同数目的状态,因而 $n_1=n_2$,即同构的线性自动机有相同的维数.

设 M_1, M_2 都是 (r, m, n) 自动机, M_1 的刻划矩阵为 A_1, B_1, C_1, D_1; M_2 的刻划矩阵为 A_2, B_2, C_2, D_2. 如果有一个 $n\times n$ 可逆矩阵 P 使

$$A_2=P^{-1}A_1P,\ B_2=B_1P,\ C_2=P^{-1}C_1,\ D_2=D_1, \tag{1}$$

那么自动机 M_1 与 M_2 就称为相似的.

定理 1 相似的自动机是同构的.

证明: 设 P 是适合(1)的可逆矩阵. 因为 P 是可逆的,所以由状态 s 到状态 sP 的对应是一个 1-1 对应. 为了证明这两个自动机是同构的,只需要证明状态 s 与状态 sP 等价就可以了.

设自动机 M_1 的初始状态为 s, 自动机 M_2 的初始状态为 sP, 而 $u(0)$, $u(1)$, $\cdots$, $u(T)$ 是任意一串输入序列. 由 §1 (4)、(5): M_1 的输出序列为

$$y^{(1)}(0)=sC_1+u(0)D_1$$

$$y^{(1)}(t)=sA_1^tC_1+\sum_{j=0}^{t-1}u(j)B_1A_1^{t-j-1}C_1+u(t)D_1$$

$$(t=1, \cdots, T),$$

根据(1): M_2 的输出序列为

$$
\begin{aligned}
y^{(2)}(0) &= sPC_2 + u(0)D_2 \\
&= sP(P^{-1}C_1) + u(0)D_1 \\
&= sC_1 + u(0)D_1,
\end{aligned}
$$

$$
\begin{aligned}
y^{(2)}(t) &= sPA_2^tC_2 + \sum_{j=0}^{t-1} u(j)B_2A_2^{t-j-1}C_2 + u(t)D_2 \\
&= sP(P^{-1}A_1P)^t(P^{-1}C_1) \\
&\quad + \sum u(j)(B_1P)(P^{-1}A_1P)^{t-j-1}(P^{-1}C_1) + u(t)D_1 \\
&= sA_1^tC_1 + \sum_{j=0}^{t-1} u(j)B_1A_1^{t-j-1}C_1 + u(t)D_1 \\
&\qquad (t=1, \cdots, T).
\end{aligned}
$$

因之，$y^{(1)}(t) = y^{(2)}(t)$ $(t=0, 1, \cdots, T)$. 这就证明了状态 s 与状态 sP 是等价的. ∎

对于同一个自动机的两个状态，我们当然也可以考虑它们是否等价的问题. 同一个自动机的两个等价的状态实现相同的由输入到输出的转换功能，在这个意义上，等价的状态是多余的. 如果线性自动机没有两个不同的状态是等价的，那么这个自动机就称为极小的. 显然，如果一个自动机的两个状态都与另一个自动机的一个状态等价，那么这两个状态就相互等价. 因之，对于两个极小的自动机，如果它们等价，那么就一定同构. 这就说明：对于极小的自动机来说，等价与同构这个概念是一致的.

§3 线性自动机的极小化

这一节我们要来证明：任意一个线性自动机都等价于一个极小的线性自动机. 为此，我们从分析状态等价的条件着手.

设 M 是一个 (r, m, n) 自动机，它的刻划矩阵为 A, B,

C, D. 设 s 与 $\bar{s}$ 是 M 的两个等价的状态. 这就是说: 不论是取 s 还是 $\bar{s}$ 作为初始状态, 对于任意一串输入序列

$$u(0),\ u(1),\ \cdots,\ u(T),$$

自动机 M 都给出相同的输出序列. 具体写出来就有

$$sC+u(0)D=\bar{s}C+u(0)D,$$

$$sA^tC+\sum_{j=0}^{t-1}u(j)BA^{t-j-1}C+u(t)D$$

$$=\bar{s}A^tC+\sum_{j=0}^{t-1}u(j)BA^{t-j-1}C+u(t)D$$

$$(t=1,\ \cdots,\ T).$$

由此即得, 状态 s 与 $\bar{s}$ 等价的充分必要条件为

$$sA^jC=\bar{s}A^jC\quad(j=0,\ 1,\ 2,\ \cdots). \tag{1}$$

因为 A 是 $n\times n$ 矩阵, 它的极小多项式的次数最多是 n, 所以对于 $t\geqslant n$, A^t 都可以通过 I, A, $\cdots$, A^{n-1} 线性表出. 因之, 条件(1)可以归结为

$$sA^jC=\bar{s}A^jC\quad(j=0,\ 1,\ \cdots,\ n-1). \tag{2}$$

令

$$K=(C,\ AC,\ \cdots,\ A^{n-1}C), \tag{3}$$

这里 K 是一个 $n\times nm$ 矩阵. 显然, 条件(2)就相当于

$$sK=\bar{s}K.$$

总结以上讨论, 我们有

定理 2 设 $(r,\ m,\ n)$ 自动机 M 的刻划矩阵为 A, B, C, D, 而 K 为(3)给出的矩阵. 于是 M 的状态 s 与 $\bar{s}$ 等价的充分必要条件为

$$sK=\bar{s}K.$$

矩阵 K 称为自动机 M 的判别矩阵.

状态的等价显然是一个等价关系, 因之自动机 M 的全部

状态在等价关系下被分成若干等价类，属于同一类的状态两两等价.

自动机 M 的全部状态组成域 F 上的 n 维向量空间 S. 令 S_0 为 S 中全部适合条件

$$sK=0$$

的向量所成的集合. 显然，S_0 是 S 的一个于空间. 如果状态 s 与 $\bar{s}$ 等价，即

$$sK=\bar{s}K,$$

移项得

$$(s-\bar{s})K=0,$$

也就是 $s-\bar{s}\in S_0$，反过来当然也成立. 这就证明了：

推论 1 状态空间 S 按子空间 S_0 分成的陪集就是状态的等价类.

如果矩阵 K 的秩是 n_1，那么根据线性方程组的理论，S_0 的维数是 $n-n_1$. 于是 S 按子空间 S_0 分成的陪集的个数就是 2^{n_1}. 由此可知：

推论 2 自动机 M 是极小的充分必要条件为 M 的判别矩阵 K 的秩等于状态空间的维数.

下面来看一个例子：

设线性自动机 M 的刻划矩阵为

$$A=\begin{pmatrix}0&1&0&0\\1&0&0&0\\1&1&0&1\\1&1&1&0\end{pmatrix},\quad B=(1\ 0\ 0\ 0),$$

$$C=\begin{pmatrix}0\\0\\0\\1\end{pmatrix},\quad D=(0).$$

M 的判别矩阵为

$$K=\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&1&0&1\\1&0&1&0\end{pmatrix}.$$

由 $$(s_1,\ s_2,\ s_3,\ s_4)K=0$$

即得 $$s_3=0,\ s_4=0,$$

这就是说，S_0 是由形式为$(s_1,\ s_2,\ 0,\ 0)$的向量组成的，也就是

$$S_0=\{(1,\ 0,\ 0,\ 0),\ (0,1,0,0),(1,1,0,0),(0,0,0,0)\}.$$

状态空间 S 按子空间 S_0 分成的陪集是：

$$\{(1,\ 0,\ 0,\ 0),(0,\ 1,\ 0,\ 0),(1,\ 1,\ 0,\ 0),(0,\ 0,\ 0,\ 0)\},$$
$$\{(1,\ 0,\ 1,\ 0),(0,\ 1,\ 1,\ 0),(1,\ 1,\ 1,\ 0),(0,\ 0,\ 1,\ 0)\},$$
$$\{(1,\ 0,\ 0,\ 1),(0,\ 1,\ 0,\ 1),(1,\ 1,\ 0,\ 1),(0,\ 0,\ 0,\ 1)\},$$
$$\{(1,\ 0,\ 1,\ 1),(0,\ 1,\ 1,\ 1),(1,\ 1,\ 1,\ 1),(0,\ 0,\ 1,\ 1)\}.$$

它们也就是自动机 M 的状态的等价类.

设 M 是任意一个线性自动机，下面来构造一个与 M 等价的极小的自动机. 假定 M 的判别矩阵 K 的秩为 n_1，当然在矩阵 K 中就有 n_1 个线性无关的列，而其余的列都可以通过这 n_1 列线性表出. 我们首先证明

引理 1 设 A 为一个 $n\times n$ 矩阵，C 为一个 $n\times m$ 矩阵. 如果矩阵

$$K=(C,\ AC,\ \cdots,\ A^{n-1}C)$$

的秩为 n_1，那么 $n_1\leqslant n$，而且矩阵

$$K_1=(C,\ AC,\ \cdots,\ A^{n_1-1}C)$$

的秩也是 n_1.

证明：因为矩阵 K 的行数为 n，所以 $n_1\leqslant n$ 是显然的. 设矩阵 K_1 的秩为 n_2，显然 $n_2\leqslant n_1$. 假如 $n_2\neq n_1$，即 $n_2<n_1$. 在

这个情形，不难看出，一定有 $0<l<n_1$ 使矩阵 A^lC 中各列都可以被矩阵$(C, AC, \cdots, A^{l-1}C)$中的列线性表出(应用抽屉原则)．用矩阵的运算来表示，就是有矩阵 $Q_0, Q_1, \cdots, Q_{l-1}$，使

$$A^lC=CQ_0+ACQ_1+\cdots+A^{l-1}CQ_{l-1},$$

其中 $Q_0, \cdots, Q_{l-1}$ 都是 $m\times m$ 矩阵．由此立即推出：A^tC $(l<t)$，也都可以通过 $C, AC, \cdots, A^{l-1}C$ 表成上面的形式．这就表明：矩阵 K 中的列都可以被矩阵$(C, AC, \cdots, A^{l-1}C)$中的列线性表出，即 $n_1\leqslant n_2<n_1$．这是矛盾的．■

引理1 说明：如果矩阵 K 的秩为 n_1，那么 n_1 个线性无关的列可以在矩阵

$$K_1=(C, AC, \cdots, A^{n_1-1}C)$$

中取．令 T 为这样取出的 n_1 个线性无关的列组成的 $n\times n_1$ 矩阵．因为 K 中各列都是矩阵 T 的列的线性组合，所以当且仅当 $sT=0$ 时，$sK=0$．

引理2 如果 $n\times n_1$ 矩阵 T 的秩为 n_1，那么可以找到一个 $n_1\times n$ 矩阵 R，使

$$RT=I_{n_1},$$

这里 I_{n_1} 代表 $n_1\times n_1$ 单位矩阵．

证明：由 $n\times n_1$矩阵 T 的秩为 n_1 可知矩阵 T 的列是线性无关的．线性无关的向量组总可以扩充成整个空间的一组基．这就是说：可以找到一个 $n\times(n-n_1)$矩阵 T_1，使矩阵(T, T_1)可逆．令 R_0 是矩阵(T, T_1)的逆矩阵，把 R_0 相应地分块为

$$R_0=\begin{pmatrix} R \\ R_1 \end{pmatrix},$$

其中 R 为 $n_1\times n$ 矩阵；R_1 为 $(n-n_1)\times n$ 矩阵．由

$$\begin{pmatrix} R \\ R_1 \end{pmatrix}(T\ \ T_1)=\begin{pmatrix} RT & RT_1 \\ R_1T & R_1T_1 \end{pmatrix}=I_n$$

即得 $$RT=I_{n_1}.$$ ∎

设自动机 M 的刻划矩阵为 A, B, C, D, 矩阵 K, T, R 的定义如上. 我们作矩阵

$$\hat{A}=RAT, \quad \hat{B}=BT,$$
$$\hat{C}=RC, \quad \hat{D}=D.$$

令 $\hat{M}$ 为以 $\hat{A}$, $\hat{B}$, $\hat{C}$, $\hat{D}$ 为刻划矩阵的线性自动机. $\hat{M}$ 是一个(r, m, n_1)自动机.

定理 3 符号同上. 自动机 M 的状态 s 与自动机 $\hat{M}$ 的状态 sT 等价. 自动机 $\hat{M}$ 是与自动机 M 等价的一个极小的自动机.

证明: 按矩阵 T、R 的选择, 有

$$(I-TR)T=T-TRT=T-TI_{n_1}=T-T=0.$$

因为矩阵 K 的每一列都是矩阵 T 的各列的线性组合, 所以由 $(I-TR)T=0$ 可知

$$(I-TR)K=0,$$

或者 $$K=TRK.$$

根据(3), 比较等式的两边即得

$$A^jC=TRA^jC \quad (j=0, 1, \cdots, n-1).$$

我们知道: A 的方幂全可以表成 I, A, $\cdots$, A^{n-1} 的线性组合, 因之

$$A^jC=TRA^jC \quad (j=0, 1, 2, \cdots). \tag{4}$$

下面来证明: 状态 s 与 sT 等价. 按等价的定义, 也就是要证明

$$sC+u(0)D=(sT)\hat{C}+u(0)\hat{D}$$
$$=sTRC+u(0)D,$$

以及 $$sA^tC+\sum_{j=0}^{t-1}u(j)BA^{t-j-1}C+u(t)D$$

$$=(sT)\hat{A}^t\hat{C}+\sum_{j=1}^{t-1}u(j)\hat{B}\hat{A}^{t-j-1}\hat{C}+u(t)\hat{D}.$$

根据(4)：$TRC=C$，这就证明了第一个等式．反复应用(4)，得

$$\begin{aligned}(sT)\hat{A}^t\hat{C}&=(sT)(RAT)^tRC\\&=sT(RAT)^{t-1}RATRC\\&=sT(RAT)^{t-1}RAC\\&=sT(RAT)^{t-2}RATRAC\\&=sT(RAT)^{t-2}RA^2C\\&=\cdots\cdots\cdots\cdots\\&=sTRA^tC=sA^tC.\end{aligned}$$

同样地，
$$\begin{aligned}u(j)\hat{B}\hat{A}^{t-j-1}\hat{C}&=u(j)BT(RAT)^{t-j-1}RC\\&=u(j)BTRA^{t-j-1}C=u(j)BA^{t-j-1}C\\&\qquad(j=1,\ 2,\ \cdots,\ t-1).\end{aligned}$$

再根据 $D=\hat{D}$，上面的计算就证明了第二个等式，因而状态与状态 sT 等价．这个结论表明：对于自动机 M 的每一个状态 s 都有自动机 $\hat{M}$ 的状态 sT 与之等价．反过来，对于 $\hat{M}$ 的每一个状态 $\hat{s}$，$\hat{s}R$是 M 的一个状态．由$(\hat{s}R)T=\hat{s}$可知：$\hat{s}$与$\hat{s}R$等价．这就说明：自动机 $\hat{M}$ 与自动机 M 等价．

因为自动机 M 的状态的等价类有 2^{n_1} 个，$\hat{M}$ 的状态有 2^{n_1} 个，所以自动机 $\hat{M}$ 是极小的．∎

例：设线性自动机 M 的刻划矩阵为

$$A=\begin{pmatrix}1&0&1&1&0\\0&0&1&0&0\\0&1&0&1&1\\0&1&0&0&0\\1&1&0&0&1\end{pmatrix},\quad B=\begin{pmatrix}1&0&1&1&1\\0&0&1&1&1\end{pmatrix},$$

$$C=\begin{pmatrix}0 & 1\\ 1 & 1\\ 0 & 1\\ 1 & 0\\ 1 & 1\end{pmatrix},\quad D=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}.$$

于是 $$K=(C,\ AC,\ A^2C,\ A^3C,\ A^4C)$$

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

不难看出：K 的秩为 2，且前两列线性无关，即

$$T=\begin{pmatrix}0 & 1\\ 1 & 1\\ 0 & 1\\ 1 & 0\\ 1 & 1\end{pmatrix}.$$

取 $$R=\begin{pmatrix}1 & 1 & 0 & 0 & 0\\ 1 & 0 & 0 & 0 & 0\end{pmatrix},$$

就有 $$RT=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

于是 $$\hat{A}=RAT=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix},$$

$$\hat{B}=BT=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix},$$

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

$$\hat{D}=D=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}.$$

以 $\hat{A}$, $\hat{B}$, $\hat{C}$, $\hat{D}$ 为刻划矩阵的自动机 $\hat{M}$ 就是与自动机 M 等价的一个极小自动机.

极小化之后的自动机 $\hat{M}$ 的判别矩阵为

$$\hat{K}=(\hat{C},\ \hat{A}\hat{C},\ \cdots,\ \hat{A}^{n_1-1}\hat{C}).$$

根据(4)，得

$$\hat{A}^i\hat{C}=(R\Delta T)^iRC$$
$$=RA^iC.$$

这就表明：$\hat{K}$ 就是矩阵 RK 的最左边的 n_1m 列. 按引理 2：矩阵 T 可以取自矩阵 K 的最左边的 n_1m 列，因而矩阵 $\hat{K}$ 中包含一个 $n_1\times n_1$ 的单位矩阵作为它的子矩阵.

最后，我们证明

定理 4 等价的极小的线性自动机一定相似.

证明：设 M_1 与 M_2 是两个等价的极小的线性自动机，它们的刻划矩阵分别是 A_1, B_1, C_1, D_1 与 A_2, B_2, C_2, D_2. 我们知道：等价的极小的自动机是同构的，因而它们有相同的维数. 令它们的状态空间都是域 F 上的 n 维向量空间 S. 同构就决定了自动机 M_1 与自动机 M_2 的状态之间的一个 1–1 对应. 我们用 $\bar{s}$ 表示与 M_1 的状态 s 对应的 M_2 的状态. 由 s 与 $\bar{s}$ 等价，取输入序列为零序列，即得

$$sA_1^jC_1=\bar{s}A_2^jC_2\quad(j=0,\ 1,\ 2,\ \cdots),$$

这就是说：

$$sK_1=\bar{s}K_2,$$

其中 K_1 与 K_2 分别是自动机 M_1 与 M_2 的判别矩阵. 因为 M_2 是极小的，所以矩阵 K_2 的秩为 n. 令 T_2 为 K_2 中 n 个线性无关的列组成的矩阵，而 T_1 为 K_1 中相应的列所成的矩阵，于是

$$sT_1=\bar{s}T_2.$$

因为 T_2 可逆，所以有

$$\bar{s}=sT_1T_2^{-1}=sP,\quad P=T_1T_2^{-1}.$$

我们知道：s 到 $\bar{s}$ 是一个 1-1 对应，因而矩阵 P 一定是一个可逆矩阵.

任取一个输入 u，由 s 与 sP 等价，即得

$$sC_1+uD_1=sPC_2+uD_2.$$

令 $u=0$，由 s 的任意性可知

$$C_1=PC_2,\ C_2=C_1P^{-1}.$$

令 $s=0$，由 u 的任意性可知

$$D_1=D_2.$$

对于任意一个输入 u，状态 s 的下一状态为

$$sA_1+uB_1;$$

状态 sP 的下一状态为

$$sPA_2+uB_2.$$

容易证明，等价的状态的下一状态必然也等价(证明留给读者)，由此即得

$$\begin{aligned}sPA_2+uB_2&=(sA_1+uB_1)P\\&=sA_1P+uB_1P.\end{aligned}$$

再利用 s 与 u 的任意性，即得

$$PA_2=A_1P,\ A_2=P^{-1}A_1P.$$

$$B_2=B_1P.$$

这就证明了自动机 M_1 与 M_2 相似. ∎

结合定理 3 与定理 4，我们可以知道：对每个线性自动机都有一个与之等价的极小的自动机，而且这个极小的自动机在相似的意义下是唯一决定的.

§4 线性自动机的标准形

设线性自动机 M 的刻划矩阵为 A, B, C, D. 由方程 $s(t+1)=s(t)A+u(t)B$看出：矩阵 A 刻划了自动机 M 的状态转移的规律. 通常我们称矩阵 A 为自动机 M 的状态转移矩阵,它反映了自动机 M 的内部线路.

上面已经证明,每个线性自动机 M 都等价于一个极小的线性自动机 $\hat{M}$, 它的刻划矩阵为 $\hat{A}$, $\hat{B}$, $\hat{C}$, $\hat{D}$. 根据线性代数的结果(见附录 1), 对于每个矩阵 $\hat{A}$ 都有一个可逆矩阵 P 使 $P^{-1}\hat{A}P$ 为有理标准形, 即 $P^{-1}\hat{A}P$ 是由一些初等有理块组成的准对角矩阵. 综合这些结果,得

定理 5 每个线性自动机 M 都等价于一个极小的线性自动机 $\tilde{M}$, 它的刻划矩阵为 $\tilde{A}$, $\tilde{B}$, $\tilde{C}$, $\tilde{D}$, 其中状态转移矩阵 $\tilde{A}$ 为有理标准形. 矩阵 $\tilde{A}$ 除去有理块的次序外是被 M 唯一决定的.

线性自动机 $\tilde{M}$ 就称为线性自动机 M 的一个标准形或一个标准化的实现.

我们知道：线性移位寄存器的状态转移矩阵是一个有理块.因之,具有标准形的线性自动机的内部线路是由若干个互相独立的线性移位寄存器组成的.这就是定理 5 的实际意义.

例如:线性自动机 M 的刻划矩阵为

$$A=\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix},\quad B=(0\ 1),$$

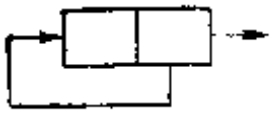
$$C=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad D=(1\ 0).$$

容易验证,M 已经是极小的. 取

$$P=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},$$

于是
$$P^{-1}=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},$$
$$P^{-1}AP=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\quad BP=(0\ 1),$$
$$P^{-1}C=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},\quad D=(1\ 0).$$

矩阵
$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$
是线性移位寄存器



的状态转移矩阵. 读者不难画出这个具有标准形的自动机的线路图.

§5 线性自律机、状态图

没有输入的线性自动机称为线性自律机. 对于线性自律机, 刻划矩阵只有 A 与 C, 它的基本方程为
$$s(t+1)=s(t)A, \tag{1}$$
$$y(t)=s(t)C. \tag{2}$$
自律机的输出完全被它的初始状态 $s(0)$ 决定. 事实上, 由(1)、(2)可知
$$y(t)=s(0)A^tC\quad(t=0,\ 1,\ 2,\ \cdots). \tag{3}$$
因之, 自律机的功能主要是被它的状态转移矩阵 A 所决定.

设 S 是自律机 M 的状态空间, 维数为 n. 状态转移矩阵 A 通过等式(1)给出了状态空间 S 的一个线性变换:
$$s\mapsto sA. \tag{4}$$
下面我们利用关于线性变换的一些概念和结果来分析状

态转移的规律：首先给出几个定义。所谓状态转移矩阵 A 的极小多项式，是指一个次数最低的多项式 $m(\lambda)$，使

$$m(A)=0;$$

所谓状态 s 相对于 A 的极小多项式，是指一个次数最低的多项式 $m_s(\lambda)$，使

$$sm_s(A)=0.$$

与第一章所用的方法一样，为了描述自律机 M 的状态转移的规律，我们引入自律机 M 的状态图的概念。假如自动机 M 是 n 维的，那么 M 有 2^n 个状态，我们用 2^n 个点来代表这些状态。如果 $s_2=s_1A$，那么就从代表 s_1 的点到代表 s_2 的点之间画一个箭头，这样得到的图就是 M 的状态图。同在第一章中一样，在状态图上可以讨论状态圈。例如：设自动机 M 的状态转移矩阵为

$$A=\begin{pmatrix}1&1&0\\1&0&1\\0&1&1\end{pmatrix}.$$

于是状态有 8 个，状态图如图 4-4。

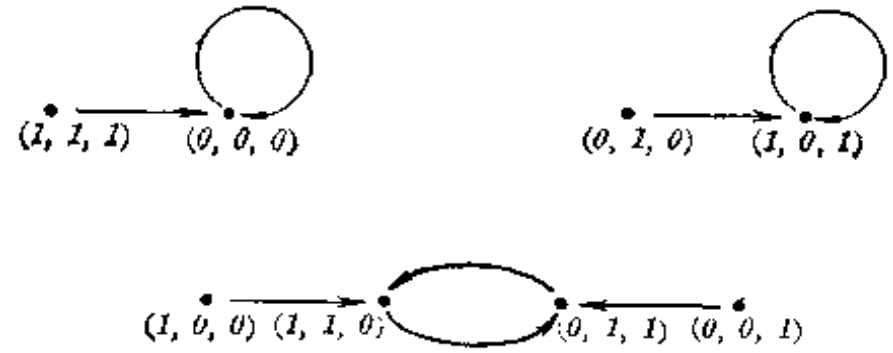


图 4-4

在这个状态图中，有三个状态圈，两个圈长为 1，一个圈长为 2。

很明显，一个状态 s 是在某一状态圈上的充分必要条件是：有一正整数 l，使

$$sA^l = s. \tag{5}$$

适合等式(5)的最小正整数 l 就是圈长，它也称为状态 s 的周期.

从上面的例子可以看出：在状态图上，有的状态在圈上，有的状态不在圈上. 下面就来讨论一个状态在圈上的条件以及周期的求法.

定理 6 设自律机 M 的状态转移矩阵为 A，状态 s 相对于 A 的极小多项式为 $m_s(\lambda)$，于是状态 s 在圈上的充分必要条件是：$m_s(\lambda)$ 的常数项不为零，也就是 $m_s(0) \neq 0$.

证明：我们知道，状态 s 在圈上的充分必要条件是有一正整数 l，使

$$sA^l = s,$$

或者

$$s(A^l - I) = 0. \tag{6}$$

如果状态 s 是在圈上，那么(6)成立，由极小多项式 $m_s(\lambda)$ 的性质可知

$$m_s(\lambda) \mid \lambda^l - 1.$$

因而 $m_s(\lambda)$ 的常数项不为零. 反过来，如果 $m_s(\lambda)$ 的常数项不为零，那么根据有限域上多项式的性质，就有一个正整数 l 使 $m_s(\lambda) \mid \lambda^l - 1$，从而(6)成立. ∎

推论 1 设自律机 M 的状态转移矩阵为 A. 于是 M 的状态全在圈上的充分必要条件是：A 的极小多项式 $m(\lambda)$ 的常数项不为零.

证明：设状态转移矩阵 A 的极小多项式 $m(\lambda)$ 的常数项不为零，状态 s 的极小多项式为 $m_s(\lambda)$. 于是

$$m_s(\lambda) \mid m(\lambda).$$

由此可知：$m_s(\lambda)$ 的常数项也不为零，因而状态 s 在圈上. 这

就是说，M 的每一个状态都在圈上.

如果矩阵 A 的极小多项式 $m(\lambda)$ 的常数项为零，根据线性代数的结果(见附录 I)，一定有一个状态 s 以 $m(\lambda)$ 作为它的极小多项式，那么这个状态就不在圈上. 换句话说，如果 M 的每个状态全在圈上，那么 A 的极小多项式的常数项不为零. ∎

定理 7 设自律机 M 的状态转移矩阵为 A，A 的极小多项式为 $m(\lambda)$. 如果

$$m(\lambda)=\lambda^r m_1(\lambda),$$

其中 $m_1(0)\neq 0$，那么状态 s 在圈上的充分必要条件为

$$s\in SA^r.$$

证明：因为 A 的极小多项式为 $m(\lambda)=\lambda^r m_1(\lambda)$，所以 SA^r 中的状态的极小多项式全是 $m_1(\lambda)$ 的因子. 由此可知：SA^r 中状态的极小多项式的常数项全不为零，从而全在圈上.

根据线性代数的结果(见附录 I)，由 A 的极小多项式为 $m(\lambda)=\lambda^r m_1(\lambda)$ 有空间分解

$$S=SA^r\dotplus Sm_1(A).$$

$Sm_1(A)$ 中状态的极小多项式全是 λ^r 的因子. 如果 s 不属于 SA^r，那么

$$s=s_1+s_2,\quad s_1\in SA^r,\quad s_2\in Sm_1(A),$$

其中 $s_2\neq 0$. 设 s_1、s_2 的极小多项式分别为 $m_0(\lambda)$，λ^{r_1}，$1\leqslant r_1\leqslant r$. 显然

$$(\lambda^{r_1},\ m_0(\lambda))=1.$$

于是 $s=s_1+s_2$ 的极小多项式为

$$\lambda^{r_1}m_0(\lambda),$$

它的常数项为零，因而不在圈上. ∎

显然，对于两个相似的自律机，它们的状态图除去状态的

标号不同外是完全一样的. 因之为了考察状态图的构造，相似的自律机可以不加区别.

假如自律机 M 的状态转移矩阵为 A，而 A 的极小多项式的常数项不为零(这就相当于说：A 是可逆的). 在这个情况下，M 的状态图全部由圈构成. 根据线性变换的有理标准形的结果，状态空间 S 可以分解成一些循环子空间的直和

$$S = S_1 + S_2 + \cdots + S_r,$$

适当取基，A 在每个循环子空间上的矩阵是一个有理块. 我们知道，有理块就相当于一个线性移位寄存器. 因之，按第一章 § 6 的方法，可以算出每个循环子空间 S_i 中状态所成的圈数和圈长. 由每个 S_i 的圈数和圈长，再按第一章 § 6 的方法，就可以算出自律机 M 的状态图的圈数和圈长. 这就是说：在状态转移矩阵是可逆的情况下，在原则上我们有办法算出状态图的圈数和圈长，也就是可以知道状态图的构造. 至于一般自律机的状态图，除去圈以外还有分枝，情况比较复杂，这里就不讨论了.

§ 6 单输出的自律机

设线性自律机 M 的刻划矩阵为 A 与 C，其中 A 是 $n \times n$ 矩阵，C 是 $n \times 1$ 矩阵. 这时，自律机 M 的输出 $y(t)$ 就是一个数，是 0 或 1. 这样的自律机称为单输出的自律机. M 的判别矩阵为

$$K = (C,\ AC,\ \cdots,\ A^{n-1}C),$$

它是一 $n \times n$ 矩阵.

设判别矩阵 K 的秩为 n_1. 根据 § 3 引理 2：K 的最左边的 n_1 列 $(C,\ AC,\ \cdots,\ A^{n_1-1}C)$ 必线性无关，即

$$K = (T,\ T_1),$$

其中 T 为一 $n\times n_1$ 矩阵，秩为 n_1. 取 $n_1\times n$ 矩阵 R，使

$$RT=I_{n_1}.$$

按§3的办法对 M 作极小化，得到一个与 M 等价的极小的自律机 $\hat{M}$. $\hat{M}$ 的刻划矩阵为

$$\hat{A}=RAT,\ \hat{C}=RC,$$

$\hat{M}$ 的判别矩阵

$$\begin{aligned}\hat{K}&=(\hat{C},\ \hat{A}\hat{C},\ \cdots,\ \hat{A}^{n_1-1}\hat{C})\\&=RT=I_{n_1}.\end{aligned}$$

由

$$(\hat{C},\ \hat{A}\hat{C},\ \cdots,\ \hat{A}^{n_1-1}\hat{C})=I_{n_1}$$

可知

$$\hat{C}=\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix},$$

而

$$\hat{A}=\begin{pmatrix}0&0&0&\cdots&C_0\\1&0&0&\cdots&C_1\\0&1&0&\cdots&C_2\\&&\cdots\cdots\cdots\cdots&&\\0&0&0&\cdots&C_{n_1-1}\end{pmatrix}.$$

这就说明：极小化之后的单输出的自律机正好是一个线性移位寄存器. 总结以上讨论，就是

定理8 每个单输出的自律机都等价于一个线性移位寄存器. 线性移位寄存器都是极小的单输出的自律机.

对于列向量 C 我们也可以定义它相对于矩阵 A 的极小多项式，那就是次数最低的多项式 $m_0(\lambda)$，使

$$m_0(A)C=0.$$

由上面的讨论不难看出，如果单输出的自律机 M 的刻划矩阵为 A、C，那么与 M 等价的线性移位寄存器的反馈多项式正

是列向量C相对于矩阵A的极小多项式，它当然是矩阵A的极小多项式的因子.

对于一般的自律机，把上面的结论应用到每个输出端的输出序列，就得到

定理9 设自律机M的刻划矩阵为A、C，输出向量为$y(t)=(y_1(t), \cdots, y_m(t))$. 对于任意的初始状态，输出序列

$$y_i=(y_i(0), y_i(1), y_i(2), \cdots) \quad (i=1, \cdots, m)$$

都是LR序列，它们的极小多项式都是A的极小多项式的因子.

到现在为止，我们就弄清楚了在线性自动机中，线性移位寄存器所占的地位.

附录 I　线性变换的有理标准形

为了第四章的需要，在这个附录中我们将定义有限维线性空间中线性变换的有理标准形，并且证明：每个线性变换的矩阵都可以化成有理标准形.

在这里我们假定 F 是一个任意的域，即对域 F 不作任何限制.

§1　极小多项式

设 V 是域 F 上的一个 n 维线性空间.

我们知道，线性空间 V 的全体线性变换对于加法与数量乘法也构成域 F 上的一个线性空间. 在 V 中取定一组基之后，每个线性变换都对应一个 $n\times n$ 矩阵，显然，这是由全体线性变换所成的线性空间到全体 $n\times n$ 矩阵所成的线性空间的一个同构映射. 全体 $n\times n$ 矩阵所成的空间是 n^2 维的，因此全体线性变换所成的线性空间也是 n^2 维的. 由此可知：在这个空间中，任意 n^2+1 个线性变换一定是线性相关的. 特别地，对于任意一个线性变换 $\mathbf{A}$，线性变换

$$\mathbf{I},\ \mathbf{A},\ \mathbf{A}^2,\ \cdots,\ \mathbf{A}^{n^2}$$

是线性相关的. 这就是说：有不全为 0 的数 $c_0,\ c_1,\ c_2,\ \cdots,\ c_{n^2}$ 存在，使等式

$$c_0\mathbf{I}+c_1\mathbf{A}+c_2\mathbf{A}^2+\cdots+c_{n^2}\mathbf{A}^{n^2}=0$$

成立. 这一事实换个说法就是：在多项式环 $F[\lambda]$ 中有一个次数不超过 n^2 的非零多项式 $f(\lambda)$ 使

$$f(\mathbf{A})=\mathbf{0}.$$

定义1 设 $\mathbf{A}$ 是 n 维线性空间 V 的一个线性变换. 在所有适合条件 $f(\mathbf{A})=\mathbf{0}$ 的非零多项式 $f(\lambda)$ 中次数最低而且首项系数为1的多项式称为 $\mathbf{A}$ 的极小多项式.

显然,一个线性变换的极小多项式是唯一确定的. 它的重要性首先反映在下面的定理中:

定理1 设线性变换 $\mathbf{A}$ 的极小多项式为 $m(\lambda)$, $f(\lambda)\in F[\lambda]$. $f(\mathbf{A})=\mathbf{0}$ 的充分必要条件为 $m(\lambda)\mid f(\lambda)$.

证明: 如果 $m(\lambda)\mid f(\lambda)$, 即

$$f(\lambda)=m(\lambda)f_1(\lambda),$$

那么
$$f(\mathbf{A})=m(\mathbf{A})f_1(\mathbf{A})=\mathbf{0}.$$

这就证明了条件的充分性. 反过来,假设

$$f(\mathbf{A})=\mathbf{0}.$$

根据带余除法: 有

$$f(\lambda)=q(\lambda)m(\lambda)+r(\lambda),$$

其中 $r(\lambda)=0$ 或者 $r(\lambda)$ 的次数低于 $m(\lambda)$ 的次数. 于是

$$r(\mathbf{A})=f(\mathbf{A})-q(\mathbf{A})m(\mathbf{A})=\mathbf{0},$$

由极小多项式的定义可知 $r(\lambda)=0$, 即

$$m(\lambda)\mid f(\lambda). \blacksquare$$

定理1表明: 只要知道了 $\mathbf{A}$ 的极小多项式 $m(\lambda)$, 全部适合条件 $f(\mathbf{A})=\mathbf{0}$ 的多项式 $f(\lambda)$ 也就清楚了, 它们就是 $m(\lambda)$ 的全部倍式.

设线性变换 $\mathbf{A}$ 的极小多项式为 $m(\lambda)$, 于是 $m(\mathbf{A})$ 就是零变换, 对于 V 中任意一个向量 α, 当然有

$$m(\mathbf{A})\alpha=\mathbf{0}.$$

但是对于某个固定的向量 α, 在适合条件

$$f(\mathbf{A})\alpha=\mathbf{0}$$

的多项式$f(\lambda)$中，$m(\lambda)$就不一定是次数最低的. 为了进一步分析线性变换的性质，我们引入：

定义2 设$\mathbf{A}$是n维线性空间V的一个线性变换，V中的α是一固定的向量. 在所有适合条件$f(\mathbf{A})\alpha=\mathbf{0}$的多项式$f(\lambda)$中，次数最低而且首项系数为1的多项式称为向量$\alpha$相对于$\mathbf{A}$的极小多项式.

在不致引起混淆的情况下，这个多项式也简称为α的极小多项式.

与定理1相仿，可以证明：

定理2 设$\mathbf{A}$是n维线性空间V的一个线性变换，V中的α相对于$\mathbf{A}$的极小多项式为$m_\alpha(\lambda)$，$f(\lambda)\in F[\lambda]$. $f(\mathbf{A})\alpha=\mathbf{0}$的充分必要条件为$m_\alpha(\lambda)\mid f(\lambda)$.

证明留给读者.

由定理2可知，向量α相对于$\mathbf{A}$的极小多项式一定是$\mathbf{A}$的极小多项式的因子.

下面来分析一下向量的极小多项式. 设向量α相对于线性变换$\mathbf{A}$的极小多项式为$m_\alpha(\lambda)$，而

$$m_\alpha(\lambda)=\lambda^l+c_{l-1}\lambda^{l-1}+\cdots+c_1\lambda+c_0.$$

由$m_\alpha(\mathbf{A})\alpha=\mathbf{0}$，即

$$(\mathbf{A}^l+c_{l-1}\mathbf{A}^{l-1}+\cdots+c_1\mathbf{A}+c_0\mathbf{I})\alpha$$
$$=\mathbf{A}^l\alpha+c_{l-1}\mathbf{A}^{l-1}\alpha+\cdots+c_1\mathbf{A}\alpha+c_0\alpha=\mathbf{0}$$

可知，向量组

$$\alpha,\ \mathbf{A}\alpha,\ \cdots,\ \mathbf{A}^{l-1}\alpha,\ \mathbf{A}^l\alpha$$

线性相关. $m_\alpha(\lambda)$的次数最低，就表示向量组

$$\alpha,\ \mathbf{A}\alpha,\ \cdots,\ \mathbf{A}^{l-1}\alpha$$

一定线性无关. 把$m_\alpha(\mathbf{A})\alpha=0$改写一下，就是

$$\mathbf{A}^l\alpha=-c_{l-1}\mathbf{A}^{l-1}\alpha-\cdots-c_1\mathbf{A}\alpha-c_0\alpha. \tag{1}$$

这就是说：$\mathbf{A}^l\alpha$ 可以由 α, $\mathbf{A}\alpha$, …, $\mathbf{A}^{l-1}\alpha$ 线性表出. 反复应用等式(1)不难证明，只要 $m\geqslant l$, 向量 $\mathbf{A}^m\alpha$ 都可以由向量组 α, $\mathbf{A}\alpha$, …, $\mathbf{A}^{l-1}\alpha$ 线性表出.

以上分析表明：如果向量 α 相对于线性变换 $\mathbf{A}$ 的极小多项式是 l 次的，那么向量组

$$\alpha,\ \mathbf{A}\alpha,\ \cdots,\ \mathbf{A}^{l-1}\alpha$$

线性无关，而 l 维子空间 $L(\alpha,\ \mathbf{A}\alpha,\ \cdots,\ \mathbf{A}^{l-1}\alpha)$ 是 $\mathbf{A}$ 的一个不变子空间. 因为子空间的维数不可能超过整个空间的维数，所以 $l\leqslant n$. 这就是说：向量的极小多项式的次数最多是 n.

下面来看看线性变换的极小多项式与向量的极小多项式的关系以及不同的向量的极小多项式之间的关系.

定理 3 设 $\mathbf{A}$ 是 n 维线性空间 V 的一个线性变换. 如果空间 V 是由向量 α_1, …, α_t 生成的，即 $V=L(\alpha_1,\ \cdots,\ \alpha_t)$, 那么 $\mathbf{A}$ 的极小多项式 $m(\lambda)$ 是向量 α_i 相对于 $\mathbf{A}$ 的极小多项式 $m_{\alpha_i}(\lambda)$ $(i=1,\ \cdots,\ t)$ 的最小公倍式.

证明：令

$$f(\lambda)=[m_{\alpha_1}(\lambda),\ \cdots,\ m_{\alpha_t}(\lambda)].$$

由 $m_{\alpha_i}(\lambda)\mid m(\lambda)$ $(i=1,\ \cdots,\ t)$ 可知 $f(t)\mid m(\lambda)$. 为了证明 $m(\lambda)\mid f(\lambda)$, 只需要证 $f(\mathbf{A})=\mathbf{0}$ 就行了. 因为 $f(\lambda)$ 是 $m_{\alpha_i}(\lambda)$ 的倍式，所以

$$f(\mathbf{A})\alpha_i=\mathbf{0}\quad(i=1,\ \cdots,\ t).$$

既然空间 V 中每个向量 α 都能表成 α_1, …, α_t 的线性组合，即

$$\alpha=c_1\alpha_1+\cdots+c_t\alpha_t.$$

于是 $$f(\mathbf{A})\alpha=c_1f(\mathbf{A})\alpha_1+\cdots+c_tf(\mathbf{A})\alpha_t=\mathbf{0}.$$

这就是说：$f(\mathbf{A})$ 把空间 V 中每个向量都变到 $\mathbf{0}$, 因而 $f(\mathbf{A})=\mathbf{0}$. 由 $f(\lambda)\mid m(\lambda)$, $m(\lambda)\mid f(\lambda)$ 即得 $m(\lambda)=f(\lambda)$. ∎

定理4 设 $\mathbf{A}$ 是 n 维线性空间 V 的一个线性变换，α_1、$\alpha_2 \in V$，它们的极小多项式分别为 $m_1(\lambda)$、$m_2(\lambda)$. 如果 $(m_1(\lambda), m_2(\lambda))=1$，那么向量 $\alpha=\alpha_1+\alpha_2$ 的极小多项式是 $m_1(\lambda)m_2(\lambda)$.

证明：令 α 的极小多项式为 $m(\lambda)$. 显然

$$m_1(\mathbf{A})m_2(\mathbf{A})\alpha=m_1(\mathbf{A})m_2(\mathbf{A})\alpha_1 + m_1(\mathbf{A})m_2(\mathbf{A})\alpha_2=\mathbf{0},$$

因之，$m(\lambda)\mid m_1(\lambda)m_2(\lambda)$. 由 $m(\mathbf{A})\alpha=\mathbf{0}$ 即得

$$m(\mathbf{A})\alpha_1+m(\mathbf{A})\alpha_2=0,$$

两边用 $m_1(\mathbf{A})$ 作用，得

$$m_1(\mathbf{A})m(\mathbf{A})\alpha_2=\mathbf{0}.$$

于是 $m_2(\lambda)\mid m_1(\lambda)m(\lambda)$. 因为 $(m_1(\lambda), m_2(\lambda))=1$，所以有

$$m_2(\lambda)\mid m(\lambda).$$

同理可证，$m_1(\lambda)\mid m(\lambda)$. 再根据 $(m_1(\lambda), m_2(\lambda))=1$ 即得

$$m_1(\lambda)m_2(\lambda)\mid m(\lambda). \blacksquare$$

定理4不难推广到多个向量的情形.

推论 设 $\mathbf{A}$ 是 n 维线性空间 V 的一个线性变换，α_1，…，$\alpha_s \in V$，它们的极小多项式分别为 $m_1(\lambda)$，…，$m_s(\lambda)$. 如果当 $i\neq j$ 时有

$$(m_i(\lambda), m_j(\lambda))=1,$$

那么向量 $\alpha=\alpha_1+\cdots+\alpha_s$ 的极小多项式是

$$m_1(\lambda)\cdots m_s(\lambda).$$

证明留给读者.

定理5 设 $\mathbf{A}$ 是 n 维线性空间 V 的一个线性变换. 如果 $\mathbf{A}$ 的极小多项式是 $m(\lambda)$，那么在空间 V 中一定存在一个向量 α，它的极小多项式就是 $m(\lambda)$，从而 $\mathbf{A}$ 的极小多项式 $m(\lambda)$ 的次数不超过 n.

证明：设 $m(\lambda)$ 在 $F[\lambda]$ 中的标准分解式为

$$m(\lambda)=p_1(\lambda)^{e_1}\cdots p_r(\lambda)^{e_r},$$

其中 $p_1(\lambda)$，…，$p_r(\lambda)$ 是不同的不可约多项式，$e_i\geqslant 1$ $(i=1$ …，$r)$．利用定理 4 的推论，我们只需要证明，对每个不可约多项式的方幂 $p_i(\lambda)^{e_i}$ 都可以找到一个向量 α_i，它以 $p_i(\lambda)^{e_i}$ 为极小多项式就行了．下面来看 $p_1(\lambda)^{e_1}$ 的情形，其余的可以完全一样地讨论．令

$$m_1(\lambda)=\frac{m(\lambda)}{p_1(\lambda)^{e_1}}=p_2(\lambda)^{e_2}\cdots p_r(\lambda)^{e_r},$$

$$g_1(\lambda)=p_1(\lambda)^{e_1-1}m_1(\lambda).$$

因为 $m(\lambda)$ 是 $\mathbf{A}$ 的极小多项式，所以 $g_1(\mathbf{A})\neq\mathbf{0}$．既然 $g_1(\mathbf{A})$ 不是零变换，在 V 中就一定有一个向量 β_1，它的象不为 $\mathbf{0}$，即

$$g_1(\mathbf{A})\beta_1\neq\mathbf{0}.$$

令 $\alpha_1=m_1(\mathbf{A})\beta_1$．显然

$$\begin{aligned}p_1(\mathbf{A})^{e_1}\alpha_1&=p_1(\mathbf{A})^{e_1}m_1(\mathbf{A})\beta_1\\&=m(\mathbf{A})\beta_1=\mathbf{0}.\end{aligned}$$

因之 α_1 的极小多项式一定是 $p_1(\lambda)^{e_1}$ 的因子，也就是 $p_1(\lambda)^k$，$k\leqslant e_1$．假如 $k<e_1$，即 $k\leqslant e_1-1$，那就有

$$p_1(\mathbf{A})^{e_1-1}\alpha_1=\mathbf{0}.$$

但是

$$\begin{aligned}p_1(\mathbf{A})^{e_1-1}\alpha_1&=p_1(\mathbf{A})^{e_1-1}m_1(\mathbf{A})\beta_1\\&=g_1(\mathbf{A})\beta_1\neq\mathbf{0}.\end{aligned}$$

这就说明，向量 α_1 的极小多项式就是 $p_1(\lambda)^{e_1}$．按同样的方法可以找到向量 α_2，…，α_r，它们分别以 $p_2(\lambda)^{e_2}$，…，$p_r(\lambda)^{e_r}$ 为极小多项式．于是向量 $\alpha=\alpha_1+\cdots+\alpha_r$ 的极小多项式就是 $m(\lambda)$．∎

应该看到，定理 5 的结论比开始时我们对极小多项式的了解大大推进了一步．在下定义时，我们只能说 n 维线性空

间的线性变换的极小多项式的次数不超过 n^2，但实际上它的次数不超过 n.

作为本节的结束，我们证明：

定理 6 设 $\mathbf{A}$ 是 n 维线性空间 V 的一个线性变换，$\alpha\in V$，$g(\lambda)\in F[\lambda]$. 如果 α 的极小多项式为 $m(\lambda)$，那么向量 $\beta=g(\mathbf{A})\alpha$ 的极小多项式是

$$\frac{m(\lambda)}{(m(\lambda),\ g(\lambda))}.$$

证明：令 β 的极小多项式为 $f(\lambda)$，而

$$(m(\lambda),\ g(\lambda))=d(\lambda),$$

$$m(\lambda)=d(\lambda)m_1(\lambda),\ g(\lambda)=d(\lambda)g_1(\lambda).$$

显然

$$\begin{aligned} m_1(\mathbf{A})\beta&=m_1(\mathbf{A})g(\mathbf{A})\alpha\\ &=g_1(\mathbf{A})m(\mathbf{A})\alpha=\mathbf{0}, \end{aligned}$$

因之，$f(\lambda)\mid m_1(\lambda)$. 反过来，由

$$f(\mathbf{A})\beta=f(\mathbf{A})g(\mathbf{A})\alpha=\mathbf{0}$$

可知

$$m(\lambda)\mid f(\lambda)g(\lambda),$$

即

$$m_1(\lambda)\mid f(\lambda)g_1(\lambda).$$

因为 $(m_1(\lambda),\ g_1(\lambda))=1$，所以有

$$m_1(\lambda)\mid f(\lambda).$$

这就证明了

$$f(\lambda)=m_1(\lambda)=\frac{m(\lambda)}{(m(\lambda),\ g(\lambda))}.\ \blacksquare$$

由定理 6 得：

推论 设向量 α 的极小多项式为 $m(\lambda)$，$g(\lambda)\in F[\lambda]$. 于是向量 $g(\mathbf{A})\alpha$ 的极小多项式总是 $m(\lambda)$ 的因子；$g(\mathbf{A})\alpha$ 与 α 有相同的极小多项式的充分必要条件是

$$(m(\lambda),\ g(\lambda))=1.$$

§2 循环子空间

设 $\mathbf{A}$ 是 n 维线性空间 V 的一个线性变换. 我们知道, 对于空间 V 的向量 $\alpha_1, \cdots, \alpha_s$, 由它们生成的子空间 $L(\alpha_1, \cdots, \alpha_s)$ 是包含向量 $\alpha_1, \cdots, \alpha_s$ 的最小的子空间. 但是 $L(\alpha_1, \cdots, \alpha_s)$不一定是 $\mathbf{A}$ 的不变子空间. 现在要来看一看包含 $\alpha_1, \cdots, \alpha_s$ 的最小的不变子空间是什么样子的.

设 W 是包含 $\alpha_1, \cdots, \alpha_s$ 的线性变换 $\mathbf{A}$ 的一个不变子空间. 因为 W 是不变子空间, 所以由 $\alpha_1 \in W$ 可知 $\mathbf{A}\alpha_1 \in W$, 同样 $\mathbf{A}^2\alpha_1, \mathbf{A}^3\alpha_1, \cdots$以及它们的线性组合也都属于 W. 换句话说, 由 $\alpha_1 \in W$ 可知对于任意的 $f(\lambda) \in F[\lambda]$ 都有 $f(\mathbf{A})\alpha_1 \in W$. 对于 $\alpha_2, \cdots, \alpha_s$ 也有同样的结论. 因之, 如果不变子空间 W 包含 $\alpha_1, \cdots, \alpha_s$, 那么 W 就一定包含所有形式为

$$f_1(\mathbf{A})\alpha_1 + \cdots + f_s(\mathbf{A})\alpha_s$$

的向量, 其中 $f_1(\lambda), \cdots, f_s(\lambda)$是任意的多项式. 不难看出, 所有上述形式的向量构成线性变换 $\mathbf{A}$ 的一个不变子空间, 而上面的分析表明, 它就是包含 $\alpha_1, \cdots, \alpha_s$ 的最小的不变子空间. 我们称这个子空间为由向量 $\alpha_1, \cdots, \alpha_s$ 生成的不变子空间, 而 $\alpha_1, \cdots, \alpha_s$ 称为这个不变子空间的一组生成元.

定义 3 设 $\mathbf{A}$ 是 n 维线性空间 V 的一个线性变换. 由一个向量生成的不变子空间称为循环子空间.

下面来分析一下循环子空间的情况:

设循环子空间 W 是由向量 α 生成的, 而 α 相对于线性变换 $\mathbf{A}$ 的极小多项式是

$$m(\lambda) = \lambda^l + c_{l-1}\lambda^{l-1} + \cdots + c_1\lambda + c_0.$$

我们从上一节的讨论知道: 向量组 $\alpha, \mathbf{A}\alpha, \cdots, \mathbf{A}^{l-1}\alpha$ 是线性无关的, 而向量 $\mathbf{A}^k\alpha (k \geqslant l)$ 全可以表成它们的线性组合. 因之由循环子空间的定义即得

$$W=L(\alpha,\ \mathbf{A}\alpha,\ \cdots,\ \mathbf{A}^{l-1}\alpha),$$

这里 $\alpha, \mathbf{A}\alpha, \cdots, \mathbf{A}^{l-1}\alpha$ 正是 W 的一组基. 于是我们得出的第一个结论是：由 α 生成的循环子空间的维数等于 α 的极小多项式的次数.

因为 $\mathbf{A}^i\alpha(i\geqslant 0)$ 的极小多项式是 α 的极小多项式的因子，所以根据定理 3：$\mathbf{A}$ 限制在循环子空间上的极小多项式就等于它的生成元的极小多项式. 这是第二个结论.

令 $\varepsilon_1=\alpha,\ \varepsilon_2=\mathbf{A}\alpha,\ \cdots,\ \varepsilon_{l-1}=\mathbf{A}^{l-2}\alpha,\ \varepsilon_l=\mathbf{A}^{l-1}\alpha,$

它是循环子空间 $L(\alpha,\ \mathbf{A}\alpha,\ \cdots,\ \mathbf{A}^{l-1}\alpha)$ 的一组基. 把 $\mathbf{A}$ 限制在循环子空间上，我们来看在这组基下的矩阵是什么. 由关系式

$$\begin{aligned}
&\mathbf{A}\varepsilon_1=\mathbf{A}\alpha=\varepsilon_2,\\
&\mathbf{A}\varepsilon_2=\mathbf{A}^2\alpha=\varepsilon_3,\\
&\cdots\cdots\cdots\cdots\\
&\mathbf{A}\varepsilon_{l-1}=\mathbf{A}^{l-1}\alpha=\varepsilon_l,\\
&\mathbf{A}\varepsilon_l=\mathbf{A}^l\alpha=-c_0\varepsilon_1-c_1\varepsilon_2-\cdots-c_{l-1}\varepsilon_l,
\end{aligned}$$

可见 $\mathbf{A}$ 在这组基下的矩阵是

$$A_W=\begin{pmatrix}
0 & 0 & 0 & \cdots & 0 & -c_0\\
1 & 0 & 0 & \cdots & 0 & -c_1\\
0 & 1 & 0 & \cdots & 0 & -c_2\\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\
0 & 0 & 0 & \cdots & 0 & -c_{l-2}\\
0 & 0 & 0 & \cdots & 1 & -c_{l-1}
\end{pmatrix}. \tag{1}$$

定义 4 象(1)这样的矩阵，即主对角线下的一排是1，其余位置上除最后一列外全是0，称为一个有理块.

于是第三个结论是：把线性变换限制在循环子空间上考虑，它在一组适当的基下的矩阵是有理块.

通过简单的行列式计算，不难得出

$$|\lambda I - A_w| = \lambda^l + c_{l-1}\lambda^{l-1} + \cdots + c_1\lambda + c_0.$$

这就是说：限制在循环子空间上，线性变换的极小多项式与特征多项式是一致的．这就是第四个结论．

上面的讨论还表明：一个有理块完全被它的特征多项式（也就是极小多项式）所决定．

定义 5 如果一个有理块的特征多项式是一个不可约多项式的方幂，那么它就称为初等有理块．

下面要证明的主要结论是：对于任何一个线性变换，总可以找到一组基，使它在这组基下的矩阵是由若干个初等有理块组成的准对角矩阵．换个说法，就是：对于任何一个线性变换，整个空间一定可以分解成若干个循环子空间的直和，而且把线性变换限制在每个循环子空间上，极小多项式都是不可约多项式的方幂．证明这个结论，将是下一节的任务．

最后我们指出：对于 n 维线性空间 V 的一个线性变换 $\mathbf{A}$，空间 V 本身是一个循环子空间的充分必要条件是：$\mathbf{A}$ 的极小多项式的次数为 n．或者说，$\mathbf{A}$ 的极小多项式就等于它的特征多项式．读者不难写出这一结论的证明．

§3 空间的分解

现在来证明前面提出的关于空间分解的结果，证明分几步完成：

设 V 是域 F 上一个 n 维线性空间，$\mathbf{A}$ 是 V 的一个线性变换．

作为空间分解的第一步，我们来证明

定理 7 空间 V 总可以分解成一些不变子空间的直和，限制在每个不变子空间上，$\mathbf{A}$ 的极小多项式都是不可约多项式的方幂．

证明：设 $\mathbf{A}$ 的极小多项式为

$$m(\lambda)=p_1(\lambda)^{e_1}\cdots p_r(\lambda)^{e_r},\ e_i\geqslant 1\quad (i=1,\ \cdots,\ r),$$

其中 $p_1(\lambda)$，$\cdots$，$p_r(\lambda)$ 是不同的不可约多项式．令

$$m_i(\lambda)=\frac{m(\lambda)}{p_i(\lambda)^{e_i}}=p_1(\lambda)^{e_1}\cdots p_{i-1}(\lambda)^{e_{i-1}}p_{i+1}(\lambda)^{e_{i+1}}\cdots p_r(\lambda)^{e_r},$$

$$V_i=m_i(\mathbf{A})V\quad (i=1,\ \cdots,\ r),$$

显然，
$$p_i(\mathbf{A})^{e_i}V_i=p_i(\mathbf{A})^{e_i}m_i(\mathbf{A})V$$
$$=m(\mathbf{A})V=\mathbf{0}.$$

这就是说，限制在不变子空间 V_i 上，$\mathbf{A}$ 的极小多项式是不可约多项式 $p_i(\lambda)$ $(i=1,\ \cdots,\ r)$ 的方幂．

下面就来证明

$$V=V_1\dotplus\cdots\dotplus V_r.$$

为此要证明两点：第一，V 中每个向量 α 都可以表成

$$\alpha=\alpha_1+\cdots+\alpha_r,\ \alpha_i\in V_i\quad (i=1,\ \cdots,\ r);$$

第二，零向量的表示法是唯一的．

显然，$(m_1(\lambda),\ \cdots,\ m_r(\lambda))=1$，因之有多项式 $u_1(\lambda)$，$\cdots$，$u_r(\lambda)$，使

$$1=u_1(\lambda)m_1(\lambda)+\cdots+u_r(\lambda)m_r(\lambda).$$

于是对于 V 中每个向量 α 都有

$$\alpha=u_1(\mathbf{A})m_1(\mathbf{A})\alpha+\cdots+u_r(\mathbf{A})m_r(\mathbf{A})\alpha,$$

其中　$u_i(\mathbf{A})m_i(\mathbf{A})\alpha\in m_i(\mathbf{A})V=V_i\quad (i=1,\ \cdots,\ r)$．

这就证明了第一点．

假设有关系式

$$\alpha_1+\cdots+\alpha_r=0,\ \alpha_i\in V_i\quad (i=1,\ \cdots,\ r).$$

用 $m_i(\mathbf{A})$ 作用等式的两边，在 $i\neq j$ 时，由

$$m_i(\mathbf{A})\alpha_j=\mathbf{0}$$

即得
$$m_i(\mathbf{A})\alpha_i=\mathbf{0}.$$

我们知道，$p_i(\mathbf{A})^{e_i}\alpha_i=\mathbf{0}$，而

$$(m_i(\lambda),\ p_i(\lambda)^{e_i})=1,$$

于是有多项式 $u(\lambda)$，$v(\lambda)$ 使

$$u(\lambda)m_i(\lambda)+v(\lambda)p_i(\lambda)^{e_i}=1.$$

因之有　　$\alpha_i=u(\mathbf{A})m_i(\mathbf{A})\alpha_i+v(\mathbf{A})p_i(\mathbf{A})^{e_i}\alpha_i=\mathbf{0}.$

这就证明了第二点．∎

由定理 7：空间分解的问题就归结为每个不变子空间的分解，而线性变换限制在每个不变子空间上的极小多项式是不可约多项式的方幂．下面就集中讨论这种情形，换句话说，假定所讨论的线性变换的极小多项式是不可约多项式的方幂．

引理 1　设线性变换 $\mathbf{A}$ 的极小多项式为 $p(\lambda)^l$，这里 $p(\lambda)$ 是一个不可约多项式，W 是 $\mathbf{A}$ 的一个不变子空间，$\alpha\in V$．如果 $f(\lambda)$ 是一个次数最低且首项系数为 1 的多项式，使得

$$f(\mathbf{A})\alpha\in W.$$

那么 $f(\lambda)\mid p(\lambda)^l$，或者说，$f(\lambda)=p(\lambda)^k$，$k\leqslant l$．

证明：根据带余除法，有

$$p(\lambda)^l=q(\lambda)f(\lambda)+r(\lambda),$$

其中 $r(\lambda)=0$，或者 $r(\lambda)$ 的次数低于 $f(\lambda)$ 的次数．于是

$$q(\mathbf{A})f(\mathbf{A})\alpha+r(\mathbf{A})\alpha=p(\mathbf{A})^l\alpha=\mathbf{0},$$

$$r(\mathbf{A})\alpha=-q(\mathbf{A})f(\mathbf{A})\alpha\in W.$$

由 $f(\lambda)$ 的规定可知 $r(\lambda)=0$，因而

$$f(\lambda)\mid p(\lambda)^l.\ \blacksquare$$

定理 8　设 $\mathbf{A}$ 是 n 维线性空间 V 的一个线性变换，$\mathbf{A}$ 的极小多项式为 $p(\lambda)^l$，这里 $p(\lambda)$ 是一个不可约多项式．于是空间 V 总可以分解成一些循环子空间的直和．

证明：因为空间 V 是有限维的，所以 V 总可以由有限多

个向量生成(在§2的意义下). 设V是由$\alpha_1, \cdots, \alpha_r$这$r$个向量生成的. 下面对$r$作归纳法来证明一个更强的结论,即:如果空间$V$是由$r$个向量生成的,那么$V$总可以分解成不超过$r$个循环子空间的直和.

当$r=1$时,V本身就是一个循环子空间,结论显然成立.

假定结论对于生成元的个数小于r的情形是成立的,现在来看生成元的个数等于r的情形:

令$\alpha_1, \cdots, \alpha_r$是$V$的一组生成元,而$W$是由$\alpha_1, \cdots, \alpha_{r-1}$生成的不变子空间. 根据归纳法假定,$W$可以分解成不超过$r-1$个循环子空间的直和

$$W=V_1\dotplus\cdots\dotplus V_s,\ s\leqslant r-1,$$

其中V_i的生成元为$\beta_i(i=1, \cdots, s)$. 假如$s<r-1$,那么V就可以由少于r个向量生成,根据归纳法假定,结论对V也成立. 因之下面只要考虑$s=r-1$的情形. 假如$\alpha_r\in W$,那么$W=V$,结论就被证明了. 下面假定

$$\alpha\notin W.$$

令β_i的极小多项式为$p(\lambda)^{t_i}(i=1, \cdots, r-1)$,$\alpha_r$的极小多项式为$p(\lambda)^k$. 我们首先指出,这里不妨假定

$$t_i\geqslant k\quad(i=1, \cdots, r-1). \tag{2}$$

假如不是这种情形,譬如说,$t_{r-1}<k$,我们就用β_{r-1}来代替原来的α_r,考虑由$\beta_1, \cdots, \beta_{r-2}, \alpha_r$生成的不变子空间,根据归纳法假定,它也可以分解成不超过$r-1$个循环子空间的直和. 这样反复进行下去,最后一个向量的极小多项式的次数逐步降低,直到满足条件(2)为止.

令V'是由α_r生成的循环子空间. 假如

$$W\cap V'=\{0\},$$

那么问题就解决了,这时我们有

$$V=W\dotplus V'=V_1\dotplus\cdots\dotplus V_{r-1}\dotplus V'.$$

下面来看 $W\cap V'\neq\{0\}$的情形. 我们知道: V' 中的向量都可以表成 $g(\mathbf{A})\alpha_r$ 的形式, 其中 $g(\lambda)$是多项式. 令 $f(\lambda)$是一个次数最低且首项系数为 1 的多项式,使

$$f(\mathbf{A})\alpha_r\in W.$$

由引理 1, $f(\lambda)=p(\lambda)^{k_1}$, 再由 $W\cap V'\neq\{0\}$可知 $k_1<k$. 这就是说

$$p(\mathbf{A})^{k_1}\alpha_r=g_1(\mathbf{A})\beta_1+\cdots+g_{r-1}(\mathbf{A})\beta_{r-1}. \tag{3}$$

两边用 $p(\mathbf{A})^{k-k_1}$ 作用,得

$$p(\mathbf{A})^{k-k_1}g_1(\mathbf{A})\beta_1+\cdots+p(\mathbf{A})^{k-k_1}g_{r-1}(\mathbf{A})\beta_{r-1}=\mathbf{0}.$$

根据直和的定义,就有

$$p(\mathbf{A})^{k-k_1}g_i(\mathbf{A})\beta_i=\mathbf{0}\quad(i=1,\cdots,r-1),$$

因之

$$p(\lambda)^{t_i}\mid p(\lambda)^{k-k_1}g_i(\lambda)\quad(i=1,\cdots,r-1),$$

$$p(\lambda)^{t_i-k+k_1}\mid g_i(\lambda)\quad(i=1,\cdots,r-1).$$

由 $t_i\geqslant k(i=1,\cdots,r-1)$就有

$$t_i-k+k_1\geqslant k_1\quad(i=1,\cdots,r-1),$$

于是

$$p(\lambda)^{k_1}\mid g_i(\lambda)\quad(i=1,\cdots,r-1).$$

令

$$g_i(\lambda)=h_i(\lambda)p(\lambda)^{k_1}\quad(i=1,\cdots,r-1),$$

(3)可以改写成

$$p(\mathbf{A})^{k_1}[\alpha_r-h_1(\mathbf{A})\beta_1-\cdots-h_{r-1}(\mathbf{A})\beta_{r-1}]=\mathbf{0}.$$

令

$$\beta_r=\alpha_r-h_1(\mathbf{A})\beta_1-\cdots-h_{r-1}(\mathbf{A})\beta_{r-1}.$$

既然 $\beta_1,\cdots,\beta_{r-1},\alpha_r$ 生成空间 V, 向量 $\beta_1,\cdots,\beta_{r-1},\beta_r$ 当然也生成空间 V. 设 β_r 生成的循环子空间为 V_r, 我们来证明

$$W\cap V_r=\{0\}.$$

用反证法: 假如 $W\cap V_r\neq\{0\}$. 这就是说, 在 V_r 中有一非零向量属于 W, 由引理 1, 有

$$p(\mathbf{A})^{k_2}\beta_r\in W,\quad k_2<k_1.$$

由此即得 $$p(\mathbf{A})^{k_r}\alpha_r \in W.$$

这与原来 k_1 的选择相矛盾. 因而 $W \cap V_r = \{0\}$, 从而

$$V = W \dotplus V_r = V_1 \dotplus \cdots \dotplus V_{r-1} \dotplus V_r.$$

根据归纳法原理, 结论普遍成立. ∎

结合定理 7 与定理 8, 我们就得到了所要的结果:

定理 9 对于任意一个线性变换 $\mathbf{A}$, 线性空间 V 总可以分解成一些循环子空间的直和, 而 $\mathbf{A}$ 在每个循环子空间上的极小多项式都是不可约多项式的方幂.

这样的分解以后简称空间 V 对于线性变换 $\mathbf{A}$ 的**标准分解**.

因为在循环子空间上, 适当取基, 线性变换的矩阵是一个有理块, 所以定理 9 换个说法就是

定理 9′ 对于任意一个线性变换 $\mathbf{A}$, 在空间 V 中都有一组基, $\mathbf{A}$ 在这组基下的矩阵为由初等有理块组成的准对角矩阵.

换成矩阵的语言, 也就是

定理 9″ 对于任意一个 $n \times n$ 矩阵 A, 都有一个可逆矩阵 P, 使 $P^{-1}AP$ 为由初等有理块组成的准对角矩阵.

下面我们来讨论一下标准分解的唯一性问题.

设 $$V = V_1 \dotplus V_2 \dotplus \cdots \dotplus V_m$$

是空间 V 对于线性变换 $\mathbf{A}$ 的一个标准分解, $f_i(\lambda)$ 是线性变换 $\mathbf{A}$ 在循环子空间 $V_i (i = 1, \cdots, m)$ 上的极小多项式. 当然, 每个 $f_i(\lambda)$ 都是不可约多项式的方幂. 这样, 空间 V 的每个标准分解就决定一个多项式组

$$f_1(\lambda), f_2(\lambda), \cdots, f_m(\lambda). \tag{4}$$

这个多项式组中的多项式可能有重复出现的, 重复出现的也考虑在内. 下面我们要证明: 虽然空间 V 的标准分解可以有

很多，但是它们所决定的多项式组(4)却总是相同的. 换句话说，多项式组(4)被线性变换 $\mathbf{A}$ 所唯一决定，与具体的标准分解无关.

因为多项式组(4)中的多项式全是不可约多项式的方幂，所以为了证明多项式组(4)的唯一性，只需要证明：对于任何一个不可约多项式的方幂 $p(\lambda)^t$，它在多项式组(4)出现的次数(即重复数) 是被线性变换 $\mathbf{A}$ 所唯一决定就行了. 为此我们证明

引理 2 设 W 是线性变换 $\mathbf{A}$ 的一个循环子空间，$\mathbf{A}$ 在 W 上的极小多项式为 $q(\lambda)^s$，$q(\lambda)$ 是一个不可约多项式，$p(\lambda)$ 是一个次数为 l 的不可约多项式. 于是

$$d(p(\mathbf{A})^tW)=\begin{cases} d(W), & \text{当 } p(\lambda)\neq q(\lambda), \\ \mathbf{0}, & \text{当 } p(\lambda)=q(\lambda),\ s\leqslant t, \\ (s-t)l, & \text{当 } p(\lambda)=q(\lambda),\ s>t. \end{cases}$$

这里 $d(W)$ 表示子空间 W 的维数.

证明：设 W 是由向量 α 生成的，α 的极小多项式是 $q(\lambda)^s$. 显然，$p(\mathbf{A})^tW$ 是由向量 $p(\mathbf{A})^t\alpha$ 生成的循环子空间.

当 $q(\lambda)\neq p(\lambda)$，也就是 $(p(\lambda)^t, q(\lambda)^s)=1$ 时，根据 § 1 定理 6 的推论，$p(\mathbf{A})^t\alpha$ 与 α 有相同的极小多项式，因而 $d(p(\mathbf{A})^tW)=d(W)$.

当 $q(\lambda)=p(\lambda)$，$s\leqslant t$ 时，显然有

$$p(\mathbf{A})^t\alpha=\mathbf{0},$$

即

$$d(p(\mathbf{A})^tW)=\mathbf{0}.$$

当 $q(\lambda)=p(\lambda)$，$s>t$ 时，根据 § 1 定理 6，$p(\mathbf{A})^t\alpha$ 的极小多项式为 $p(\lambda)^{s-t}$. 因为 $p(\lambda)=q(\lambda)$ 的次数是 l，所以 $p(\lambda)^{s-t}$ 的次数是 $(s-t)l$，因而我们有 $d(p(\mathbf{A})^tW)=(s-t)l$. ∎

设 $p(\lambda)$ 是任意一个不可约多项式，$p(\lambda)$ 的次数为 l，

$t\geqslant 1$. 由标准分解式即得

$$p(\mathbf{A})^{t-1}V = p(\mathbf{A})^{t-1}V_1 \dotplus \cdots \dotplus p(\mathbf{A})^{t-1}V_m,$$

$$p(\mathbf{A})^{t}V = p(\mathbf{A})^{t}V_1 \dotplus \cdots \dotplus p(\mathbf{A})^{t}V_m.$$

因为它们是直和，所以有

$$d(p(\mathbf{A})^{t-1}V) = \sum_{i=1}^{m} d(p(\mathbf{A})^{t-1}V_i),$$

$$d(p(\mathbf{A})^{t}V) = \sum_{i=1}^{m} d(p(\mathbf{A})^{t}V_i).$$

于是 $$d(p(\mathbf{A})^{t-1}V) - d(p(\mathbf{A})^{t}V)$$

$$= \sum_{i=1}^{m} [d(p(\mathbf{A})^{t-1}V_i) - d(p(\mathbf{A})^{t}V_i)].$$

设 $\mathbf{A}$ 在循环子空间 V_i 上的极小多项式是 $p_i(\lambda)^{s_i}$，于是根据引理 2，就有

$$d(p(\mathbf{A})^{t-1}V_i) - d(p(\mathbf{A})^{t}V_i) = \begin{cases} \mathbf{0}, & \text{当 } p_i(\lambda) \neq p(\lambda), \\ \mathbf{0}, & \text{当 } p_i(\lambda) = p(\lambda), s_i < t, \\ l, & \text{当 } p_i(\lambda) = p(\lambda), s_i \geqslant t, \end{cases}$$

因之 $$d(p(\mathbf{A})^{t-1}V) - d(p(\mathbf{A})^{t}V) = n_t l,$$

其中 n_t 是多项式组(4)中出现的 $p(\lambda)$ 的方幂且方次 $\geqslant t$ 的多项式的个数. 由此可知，$n_t - n_{t+1}$ 就是多项式组(4)中 $p(\lambda)^t$ 出现的次数. 这就是说，在多项式组(4)中某个不可约多项式的方幂 $p(\lambda)^s$ 出现的次数完全被下列子空间

$$p(\mathbf{A})^{t}V \quad (t=0, 1, 2, \cdots)$$

的维数所决定，这些当然与标准分解无关，因而 V 的不同的标准分解必然给出相同的多项式组(4).

定义 6 由 V 的标准分解所给出的多项式组 (4) 称为线性变换 $\mathbf{A}$ 的初等因子.

上面的讨论说明：线性变换的初等因子中每一个多项式

都对应空间 V 的标准分解中一个循环子空间，因而就决定了准对角矩阵中一个初等有理块．这就证明了

定理 10 定理 9′ 中所说的由初等有理块组成的准对角矩阵，除去其中初等有理块排列的次序外，完全被线性变换 **A** 唯一决定．

定义 7 定理 10 中所说的准对角矩阵称为线性变换 **A** 的有理标准形．

显然，只要知道了线性变换 **A** 的初等因子，就可以写出 **A** 的有理标准形．例如，在实数域上一个 10 维的线性空间中，线性变换 **A** 的初等因子为

$$(\lambda-2)^3,\ (\lambda-2)^2,\ (\lambda-2)^2,\ (\lambda-2),\ (\lambda^2+\lambda+1).$$

$(\lambda-2)^3=\lambda^3-6\lambda^2+12\lambda-8$ 所对应的初等有理块是

$$\begin{pmatrix} 0 & 0 & 8 \\ 1 & 0 & -12 \\ 0 & 1 & 6 \end{pmatrix},$$

$(\lambda-2)^2=\lambda^2-4\lambda+4$ 所对应的初等有理块为

$$\begin{pmatrix} 0 & -4 \\ 1 & 4 \end{pmatrix},$$

$(\lambda-2)$ 所对应的初等有理块为

$$(2),$$

$\lambda^2+\lambda+1$ 所对应的初等有理块为

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

于是线性变换 **A** 的有理标准形为

$$\begin{pmatrix} 0 & 0 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -12 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}.$$

至于怎样求一个线性变换的初等因子，在一般的代数书上都有讨论，这里就不叙述了.

最后，我们来看一下初等因子与极小多项式以及特征多项式的关系：

设线性变换 $\mathbf{A}$ 的初等因子为

$$p_1(\lambda)^{e_{11}},\ p_1(\lambda)^{e_{12}},\ \cdots,\ p_1(\lambda)^{e_{1r_1}},$$
$$p_2(\lambda)^{e_{21}},\ p_2(\lambda)^{e_{22}},\ \cdots,\ p_2(\lambda)^{e_{2r_2}},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$p_s(\lambda)^{e_{s1}},\ p_s(\lambda)^{e_{s2}},\ \cdots,\ p_s(\lambda)^{e_{sr_s}},$$

其中 $p_1(\lambda),\ p_2(\lambda),\ \cdots,\ p_s(\lambda)$ 是不同的不可约多项式，而且

$$e_{i1}\geqslant e_{i2}\geqslant\cdots\geqslant e_{ir_i},\ r_i\geqslant 1\quad (i=1,\ 2,\ \cdots,\ s).$$

因为每个初等因子都对应有理标准形中一个有理块，而对应的有理块的特征多项式就是这个初等因子，所以全部初等因子的乘积就等于线性变换 $\mathbf{A}$ 的特征多项式.

每个初等因子对应空间 V 的标准分解中的一个循环子空间，而线性变换 $\mathbf{A}$ 在对应的循环子空间上的极小多项式就

是这个初等因子，因而，根据§1定理3即得：线性变换$\mathbf{A}$的极小多项式$m(\lambda)$就等于初等因子中那些方次最高的不可约多项式的方幂的乘积，即

$$m(\lambda)=p_1(\lambda)^{e_{11}}p_2(\lambda)^{e_{21}}\cdots p_s(\lambda)^{e_{s1}}.$$

从以上分析即得

定理11 设线性变换$\mathbf{A}$的特征多项式为$f(\lambda)$，极小多项式为$m(\lambda)$．于是$m(\lambda)|f(\lambda)$，或者说，$f(\mathbf{A})=\mathbf{0}$，同时$m(\lambda)$与$f(\lambda)$有相同的不可约因子．

$f(\mathbf{A})=\mathbf{0}$就是通常所谓的Cayley-Hamilton定理．

附录 II　本原多项式

本附录中给出一张本原多项式的表. 表中列出次数≤168的本原多项式，每个次数给出一个本原多项式. 下面的本原多项式有两种形式：对某一个次数，如果有本原的三项式 $f(\lambda)=\lambda^n+\lambda^k+1$，就取 k 最小的那一个；如果没有 n 次的本原三项式，就取形式为 $f(\lambda)=\lambda^n+\lambda^{a+b}+\lambda^b+\lambda^a+1$ 的本原多项式，在这种形式的多项式中，a 取最小的，对最小的 a 再取最小的 b，且 $0<a<b<n-a$.

在表中，对每个多项式只写出多项式中出现的项的次数，如

125, 108, 107, 1, 0

就代表多项式 $g(\lambda)=\lambda^{125}+\lambda^{108}+\lambda^{107}+\lambda+1$.

GF(2)上本原多项式表

1	0				6	1	0		
2	1	0			7	1	0		
3	1	0			8	6	5	1	0
4	1	0			9	4	0		
5	2	0			10	3	0		
11	2	0			31	3	0		
12	7	4	3	0	32	28	27	1	0
13	4	3	1	0	33	13	0		
14	12	11	1	0	34	15	14	1	0
15	1	0			35	2	0		
16	5	3	2	0	36	11	0		
17	3	0			37	12	10	2	0

（续表）

18	7	0			38	6	5	1	0
19	6	5	1	0	39	4	0		
20	3	0			40	21	19	2	0
21	2	0			41	3	0		
22	1	0			42	23	22	1	0
23	5	0			43	6	5	1	0
24	4	3	1	0	44	27	26	1	0
25	3	0			45	4	3	1	0
26	8	7	1	0	46	21	20	1	0
27	8	7	1	0	47	5	0		
28	3	0			48	28	27	1	0
29	2	0			49	9	0		
30	16	15	1	0	50	27	26	1	0
51	16	15	1	0	71	6	0		
52	3	0			72	53	47	6	0
53	16	15	1	0	73	25	0		
54	37	36	1	0	74	16	15	1	0
55	24	0			75	11	10	1	0
56	22	21	1	0	76	36	35	1	0
57	7	0			77	31	30	1	0
58	19	0			78	20	19	1	0
59	22	21	1	0	79	9	0		
60	1	0			80	38	37	1	0
61	16	15	1	0	81	4	0		
62	57	56	1	0	82	38	35	3	0
63	1	0			83	46	45	1	0
64	4	3	1	0	84	13	0		
65	18	0			85	28	27	1	0
66	10	9	1	0	86	13	12	1	0
67	10	9	1	0	87	13	0		
68	9	0			88	72	71	1	0
69	29	27	2	0	89	38	0		
70	16	15	1	0	90	19	18	1	0

（续表）

91	84	83	1	0	111	10	0		
92	13	12	1	0	112	45	43	2	0
93	2	0			113	9	0		
94	21	0			114	82	81	1	0
95	11	0			115	15	14	1	0
96	49	47	2	0	116	71	70	1	0
97	6	0			117	20	18	2	0
98	11	0			118	33	0		
99	47	45	2	0	119	8	0		
100	37	0			120	118	111	7	0
101	7	6	1	0	121	18	0		
102	77	76	1	0	122	60	59	1	0
103	9	0			123	2	0		
104	11	10	1	0	124	37	0		
105	16	0			125	108	107	1	0
106	15	0			126	37	36	1	0
107	65	63	2	0	127	1	0		
108	31	0			128	29	27	2	0
109	7	6	1	0	129	5	0		
110	13	12	1	0	130	8	0		
131	48	47	1	0	150	53	0		
132	29	0			151	3	0		
133	52	51	1	0	152	66	65	1	0
134	57	0			153	1	0		
135	11	0			154	129	127	2	0
136	126	125	1	0	155	32	31	1	0
137	21	0			156	116	115	1	0
138	8	7	1	0	157	27	26	1	0
139	8	5	3	0	158	27	26	1	0
140	29	0			159	31	0		
141	32	31	1	0	160	19	18	1	0
142	21	0			161	18	0		
143	21	20	1	0	162	88	87	1	0

（续表）

144	70	69	1	0	163	60	59	1	0
145	52	0			164	14	13	1	0
146	60	59	1	0	165	31	30	1	0
147	38	37	1	0	166	39	38	1	0
148	27	0			167	6	0		
149	110	109	1	0	168	17	15	2	0

这个表是

Wayne Stahnke. Primitive Binary Polynomials

Mathematics of Computation, vol. 27. no. 124, 1973

中作出的。

名 词 索 引

(按汉语拼音的字母顺序排列)