移位寄存器序列概论

（上）

二〇〇五年八月

前 言

为了满足我局技术人员专题进修和实际工作的需要，我们编写了这本教材。

本书是参照北京大学的讲义《线性移位寄存器序列》和当前国内有关线性移存器的若干理论文献以及部分我们实际研究的成果综合写成的。全书共分十四章。前六章集中讨论了单回头线性反馈移存器及其序列的基本理论和解决问题的基本方法，作为研究各类线性移存器序列的基础。第七章重点讲述具有代表性的不等距多回头级间模2加线性移存器的主要理论、规律和方法，它是线性移存器的一般形式。第八章至第十一还有选择地介绍了常见的几种类型的级间模2加线性移存器及其特有的规律和结论，以满足实际需要和开阔读者的眼界。第十二章，集中介绍了各种前馈序列的基本理论和若干实际问题的求解方法。最后在第十三章，我们通过线性自动机的介绍，对本书各章的论述进行概括提升，并将线性移存器的学习和探讨引入更广泛的领域。第十四章作为本书的附录，简单介绍了非线性移存器的一般概念等几个问题。

书中的论证基点是在读者掌握了高等代数理论和初等数论、有限域知识的基础上进行的。另外为便于应用，我们在书后给出计算所需的若干数表。

本书中的绝大部分定理都给出了理论证明，只有少数定理由于涉及较多的数学理论或论证十分繁琐，我们只给出结论和举例，并注明参考材料，以便有兴趣的读者参阅和深入研究。因为本书着重实际应用，故对某些概念和结论仅作了一般的介绍。对书中所有的重要概念和结论，我们都给出实际例子进行说明，并在每章后面附有习题，以便读者获得感性认识，便于理解和掌握。

在给出基本理论及其证明的同时，我们也重点给出了若干实际问题的求解方法。为便于手工推算，所举例题的级数一般都不太大，对于级数较大的情况，可借助于电子计算机求解。

由于编者水平所限，时间仓促，书中如有疏漏不当之处，敬请读者指正。

本书是内部材料，请勿外传，注意保存。

八 局

1981. 4. 北京

出版者的话

本书是在五七三一八部队组织编写的“线性移位寄存器”的基础上改编的，“线性移位寄存器”是由司常玉、邓永庆主编，邝新生、戴跃书、周忠德、华宁参加了编写工作，五七三一八部队的有关同志也提了不少宝贵意见。

在此基础上又请邓永庆同志增写了非线性移位寄存器和有关理论证明部份。

本书比较全面地收集、编写了各类常见的移位寄存器序列的初步分析，既有实例，又有理论证明，写得比较通俗，只要具有高等代数和有限域初步知识的人员即可学懂。本书可供广大工作人员学习参考用。

五七三〇三部队司令部

一九八一年八月

目　录

第一章　线性反馈移位寄存器的数学描述

§1. 线性移位寄存器的一般概念

n 级线性反馈移位寄存器的一般示意图如下：

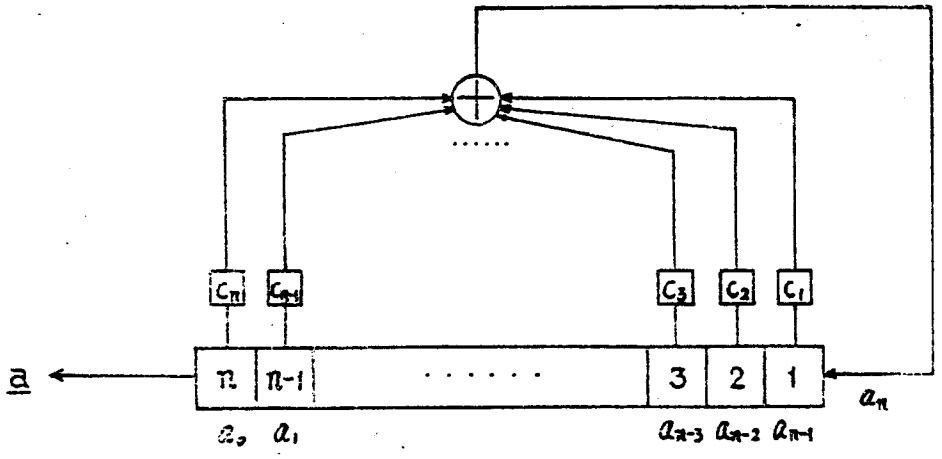

图 1．1

图1．1中1，2，3，…，$n-1$，n 为移位寄存器（可简写为移存器）的各级编号；c_1，c_2，…，c_n，表示各级是否抽头参与反馈，当第 i 级抽头，则 $c_i=1$，若第 i 级不抽头，则 $c_i=0$。在这里，我们所讨论的线性反馈移存器都是第 n 级一定抽头，即 $c_n=1$ 的情况，我们称之为**n级非退化的线性反馈移存器。**

a_0，a_1，…，a_{n-1} 是各级寄存器的内容（或称各级寄存器的**状态符号**），$a_i=0$ 或 1，$i=0$，1，2，…；它的排列顺序和各级编号相反。

向量 $\alpha^0=(a_0,a_1,\cdots,a_{n-1})$ 称为移存器**第 0 时刻的状态**，也称为移存器的**初始状态**（简称**初态**）。第 i 时刻的状态记为 $\alpha^i=(a_i,a_{i+1},\cdots,a_{i+n-1})$。显然，$n$ 级移存器共有2 个不同的状态。

a_n，a_{n+1}，…，a_{n+i} 分别称为第 0 时刻，第 1 时刻，…，第 i 时刻的**反馈符号。**

如果 a_{i+n} 可以表成 a_{i+n} 的前 n 级符号的线性组合，即有

$$a_{i+n}=c_1a_{n-1+i}+c_2a_{n-2+i}+\cdots+c_na_i,\qquad i=0,\ 1,\ 2,\ \cdots$$

则称此移存器为**线性反馈移存器。**

如果反馈符号 a_{i+n} 不能表成 a_{i+n} 前 n 级符号的线性组合，则称此移存器为**非线性反馈**

移存器。

在此说明一点：一般地，我们也将第七、八、九、十、十一等章所讲的线性移存器称为**多回头级间模2加线性反馈移存器**，图1.1所示的移存器称为**单回头线性反馈移存器**；我们习惯上说的线性反馈移存器就是指的这种移存器。后文不再每次说明。由于任何一条由线性移存器所产生的序列，都等价于一条线性反馈移存器序列，因此，对线性反馈移存器及其序列的研究在线性移存器的研究中具有重要的意义。

显然，由反馈符号的线性表出式：

$$a_{i+n}=c_1a_{n-1+i}+c_2a_{n-2+i}+\cdots+c_na_i,\quad i=0,\ 1,\ 2,\ \cdots, \qquad (1)$$

完全刻划了一个线性移存器的功能，（1）式通常称为线性移存器的**反馈函数**（或**反馈逻辑、反馈线路、线性网络**等等）。

这样，线性移存器经过不断地反馈，移位，在第 n 级寄存器就输出一个序列，记为：$\underline{a}=(a_0,a_1,a_2,\cdots,a_n,a_{n+1},a_{n+2},\cdots)$

$\underline{a}$ 即称为**线性反馈移存器序列。**

在数学上，我们有：

定义 无限序列 $\underline{a}=(a_0,a_1,a_2,\cdots)$

称为一个**线性递推序列**，如果 $a_0,a_1,a_2,\cdots$ 适合一个线性递推关系式：

$$a_{i+n}=\sum_{j=0}^{n-1}c_ja_{i+j}\qquad i=0,\ 1,\ 2,\ \cdots$$

例： F_2 上序列 $\underline{a}=(0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\cdots\cdots)$

$\because \underline{a}$ 适合关系式：$a_{i+3}=a_i+a_{i+1},\ i=0,\ 1,\ 2,\ \cdots$

$\therefore \underline{a}$ 是一个线性递推序列，又可记为*LR*序列。

显然，线性递推序列不过是线性移存器序列的一个数学说法。所以，我们将线性移存器序列

$\underline{a}=(a_0,a_1,a_2,\cdots\cdots)$，又称为**线性递推序列。**

线性反馈移存器序列又可简写为 **LFSR序列。***LFSR*是英文 *Linear Feedback Shift Register*（线性反馈移存器）的缩写。

目前，我们所研究的移存器可以大致分为以下几种类型，（见下页表1.1）：

实际上，移位寄存器只是一般时序线路的一种特殊线路，自动机就是这种时序线路的一个数学抽象。我们准备在第十三章中对线性自动机作一些初步介绍。本书主要介绍线性移存器和它的前馈门电路。作为本书的续篇，在第十四章里对非线性移位寄存器的一般概念作些初步介绍。

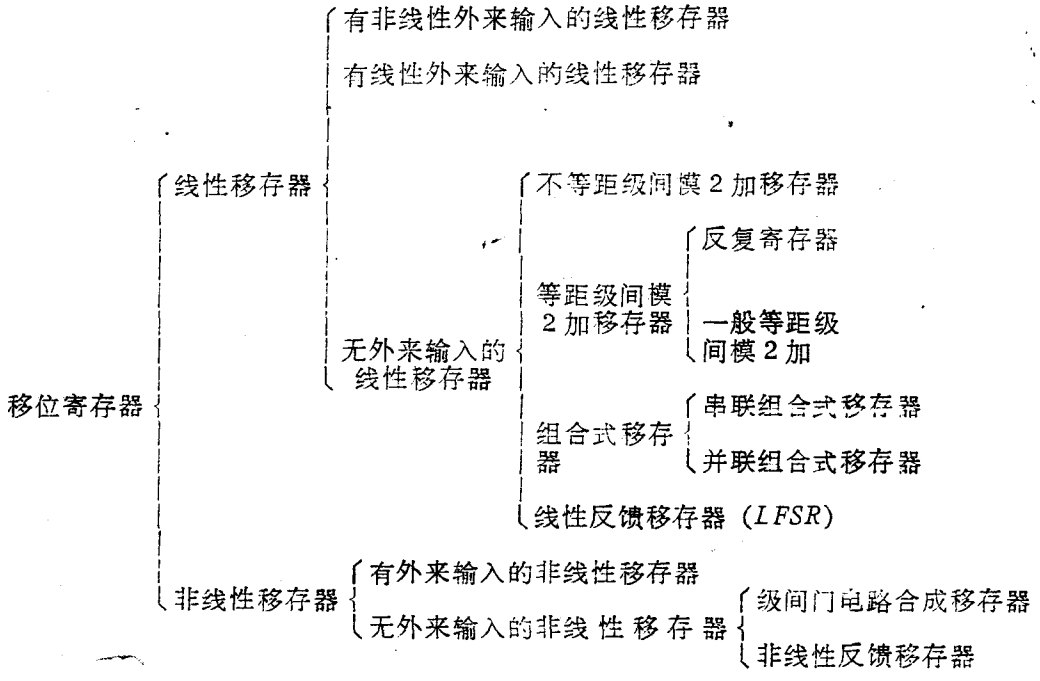

表1．2

§2．状态转移变换

§2．1　状态转移变换

n 级线性反馈移存器每一时刻的内部状态，都可以看成是 F_2 上一个 n 维向量。这样，移存器的全体状态就是 F_2 上的全体 n 维向量，构成了 F_2 上的 **n 维向量空间**，记作 V。

移存器由一个时刻的状态变到下一时刻状态，可以看作是线性空间 V 的一个变换，叫做**状态转移变换**。对线性反馈移存器来说，由于后一状态的各级符号可以表示成前一状态各级符号的线性组合，因此状态转移变换是**线性变换**。

例：4 级线性反馈移存器如图：

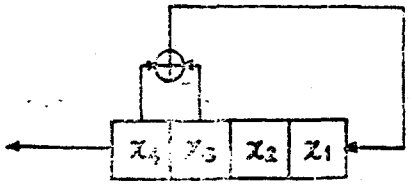

图1．2

设：前一状态为 $\alpha^i=(x_4x_3x_2x_1)$，则下一状态为

$$\alpha^{i+1}=\underline{A}(\alpha^i)=\underline{A}(x_4x_3x_2x_1)$$

由 $\underline{A}(x_4)=x_3$

$\underline{A}(x_3)=x_2$

$\underline{A}(x_2)=x_1$

$\underline{A}(x_1)=x_3+x_4$

$\Rightarrow \underline{A}(x_4, x_3, x_2, x_1)=(x_3, x_2, x_1, x_3+x_4)$。

$\underline{A}$即是由状态α^i变到α^{i+1}的状态转移变换。

§2.2 状态转移矩阵

我们知道，线性变换可以用一组基下的矩阵来表示。对 n 级线性反馈移存器来说，可以任选 n 个线性无关的状态 ε_1，ε_2，…，ε_n做为一组基，设它们在状态转移变换 $\underline{A}$下的象为 $\underline{A}\varepsilon_1$，$\underline{A}\varepsilon_2$，…，$\underline{A}\varepsilon_n$，

定义矩阵

$$A=\begin{pmatrix}\varepsilon_1\\ \varepsilon_2\\ \vdots\\ \varepsilon_n\end{pmatrix}^{-1}\begin{pmatrix}\underline{A}\varepsilon_1\\ \underline{A}\varepsilon_2\\ \vdots\\ \underline{A}\varepsilon_n\end{pmatrix}$$

为移存器的**状态转移矩阵**。

注意，根据A的定义，在不同基下所得到的状态转移矩阵A是固定不变的。

例：4级线性反馈移存器为图1.2所示，设它每次走一步的状态转移变换为 $\underline{A}$，下面一组状态构成 $\underline{A}$的一组单位基：

$$\varepsilon_1=(1\ 0\ 0\ 0)$$
$$\varepsilon_2=(0\ 1\ 0\ 0)$$
$$\varepsilon_3=(0\ 0\ 1\ 0)$$
$$\varepsilon_4=(0\ 0\ 0\ 1)$$

它们在 $\underline{A}$下的象为：

$$\underline{A}(\varepsilon_1)=(0\ 0\ 0\ 1)$$
$$\underline{A}(\varepsilon_2)=(1\ 0\ 0\ 1)$$
$$\underline{A}(\varepsilon_3)=(0\ 1\ 0\ 0)$$
$$\underline{A}(\varepsilon_4)=(0\ 0\ 1\ 0)$$

于是状态转移矩阵

$$A=\begin{pmatrix}\varepsilon_1\\ \varepsilon_2\\ \varepsilon_3\\ \varepsilon_4\end{pmatrix}^{-1}\cdot\begin{pmatrix}\underline{A}\,\varepsilon_1\\ \underline{A}\,\varepsilon_2\\ \underline{A}\,\varepsilon_3\\ \underline{A}\,\varepsilon_4\end{pmatrix}=E^{-1}\cdot\begin{pmatrix}0&0&0&1\\1&0&0&1\\0&1&0&0\\0&0&1&0\end{pmatrix}=\begin{pmatrix}0&0&0&1\\1&0&0&1\\0&1&0&0\\0&0&1&0\end{pmatrix}。$$

状态转移矩阵A的作用是：

$\alpha^i\cdot A=\alpha^{i+1}$　　或　　$\alpha^0\cdot A^i=\alpha^i$。（其中$\alpha^i$表示第 i 拍状态）

§2．3　表出式及其转移矩阵

例：4 级线性反馈移存器如下图：

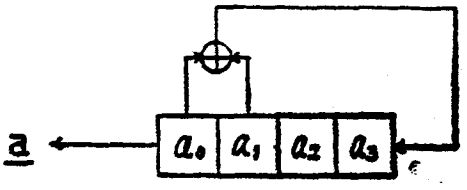

图 1．3

它的输出序列为　$\underline{a}=(a_0,a_1,a_2,a_3,a_4,\cdots\cdots)$，初态 $\alpha^0=(a_0,a_1,a_2,a_3)$，

线性递推关系为　$a_{i+4}=a_{i+1}+a$，　$i=0,\ 1,\ 2,\ \cdots$。

根据线性递推关系，序列$\underline{a}$中的任意一个符号a_i都可以被$\underline{a}$的初态中的符号 a_0，a_1，a_2，a_3线性表出，表出系数写成向量的形式，即为该符号被初态的**表出式**，又称为该符号在初态下的**坐标**。

如：

$$\begin{aligned}
a_0&=1\cdot a_0+0\cdot a_1+0\cdot a_2+0a_3 &\Rightarrow\quad &(1\ 0\ 0\ 0)=\sigma^0\\
a_1&=0\cdot a_0+1\cdot a_1+0\cdot a_2+0a_3 &\Rightarrow\quad &(0\ 1\ 0\ 0)=\sigma^1\\
a_2&=0\cdot a_0+0\cdot a_1+1\cdot a_2+0a_3 &\Rightarrow\quad &(0\ 0\ 1\ 0)=\sigma^2\\
a_3&=0\cdot a_0+0\cdot a_1+0\cdot a_2+1a_3 &\Rightarrow\quad &(0\ 0\ 0\ 1)=\sigma^3\\
a_4&=1\cdot a_0+1\cdot a_1+0\cdot a_2+0a_3 &\Rightarrow\quad &(1\ 1\ 0\ 0)=\sigma^4\\
a_5&=0\cdot a_0+1\cdot a_1+1\cdot a_2+0a_3 &\Rightarrow\quad &(0\ 1\ 1\ 0)=\sigma^5\\
&\vdots &\quad &\vdots
\end{aligned}$$

σ^i即为 a_i 在初态 $\alpha^0=(a_0a_1a_2a_3)$ 下的表出式。由于每个表出式都可以写成 n 维向量的形式，因此，全体表出式也构成一个F_2上的 **n 维线性空间**，记为U。我们把由表出式σ^i变到σ^{i+1}的变换叫做**表出式转移变换$\underline{A}'$**，即

$$\underline{A}'\ (\sigma^i)=\sigma^{i+1},$$

设：σ^0，σ^1，σ^2，σ^3，…，σ^{n-1}，是U的一组基。

我们**定义**$n\times n$矩阵A'

$$A'=\begin{pmatrix}\sigma^0\\ \sigma^1\\ \sigma^2\\ \sigma^3\\ \vdots\\ \sigma^{n-1}\end{pmatrix}^{-1}\cdot\begin{pmatrix}\overline{A'\sigma^0}\\ \overline{A'\sigma^1}\\ \overline{A'\sigma^2}\\ \overline{A'\sigma^3}\\ \vdots\\ \overline{A'\sigma^{n-1}}\end{pmatrix}$$

为移存器的序列符号的**表出式转移矩阵**。

如上例：$$A'=\begin{pmatrix}\sigma^0\\ \sigma^1\\ \sigma^2\\ \sigma^3\end{pmatrix}^{-1}\cdot\begin{pmatrix}\overline{A'\sigma^0}\\ \overline{A'\sigma^1}\\ \overline{A'\sigma^2}\\ \overline{A'\sigma^3}\end{pmatrix}=\begin{pmatrix}0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 1&1&0&0\end{pmatrix}$$

可以看出，序列符号的表出式转移矩阵就是状态转移矩阵A的转置。

同理，我们可以推出状态表出式及其转移矩阵：

设α^0，α^1，α^2，…，α^{n-1}是由n级线性反馈移存器的初态α^0推出的连续n个状态，那么由α^0派生的任意一拍状态α^i都可以被α^0，α^1，…，α^{n-1}线性表出，表出系数写成向量形式，就叫做α^i的**状态表出式**。

全体状态的表出式也构成一个**n维线性空间**，记为U。

如上例：
$$\alpha^0=1\cdot\alpha^0+0\cdot\alpha^1+0\cdot\alpha^2+0\cdot\alpha^3\Rightarrow(1\ 0\ 0\ 0)=\sigma^0$$
$$\alpha^1=0\cdot\alpha^0+1\cdot\alpha^1+0\cdot\alpha^2+0\cdot\alpha^3\Rightarrow(0\ 1\ 0\ 0)=\sigma^1$$
$$\alpha^2=0\cdot\alpha^0+0\cdot\alpha^1+1\cdot\alpha^2+0\cdot\alpha^3\Rightarrow(0\ 0\ 1\ 0)=\sigma^2$$
$$\alpha^3=0\cdot\alpha^0+0\cdot\alpha^1+0\cdot\alpha^2+1\cdot\alpha^3\Rightarrow(0\ 0\ 0\ 1)=\sigma^3$$
$$\alpha^4=1\cdot\alpha^0+1\cdot\alpha^1+0\cdot\alpha^2+0\cdot\alpha^3\Rightarrow(1\ 1\ 0\ 0)=\sigma^4$$

σ^i即为状态α^i在α^0，α^1，α^2，α^3下的状态表出式（或称坐标）。

对于线性反馈移存器来说，由于状态α^i就等于序列$\underline{a}$中从a_i开始的连续n个符号形成的向量，故状态之间的表出关系完全对等于序列符号之间的表出关系。因此，线性反馈移存器的状态表出式转移矩阵与序列符号**表出式转移矩阵**是相同的。

表出式转移矩阵的作用是：
$$\sigma^i\cdot A'=\sigma^{i+1}$$
$$\sigma^0(A')^i=\sigma^i$$

如果把α^i写成列向量，那么显然有：$A\alpha^i=\alpha^{i+1}$；$A^i\alpha^0=\alpha^i$。（A为状态转移矩阵）。

§2．4　状态的循环不变子空间

设有5级线性反馈移存器如图：

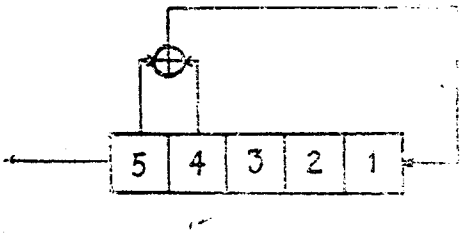

图 1．4

它的全体状态构成F_2上5维线性空间V，设其状态转移变换为$\underline{A}$，则有$\underline{A}\alpha^i=\alpha^{i+1}$。

下面一组状态构成V的一个子集合W_1：

$W_1=\{\alpha^1=(1\ 1\ 1\ 0\ 1)$，$\alpha^2=(1\ 1\ 0\ 1\ 0)$，$\alpha^3=(1\ 0\ 1\ 0\ 0)$，
$\alpha^4=(0\ 1\ 0\ 0\ 1)$，$\alpha^5=(1\ 0\ 0\ 1\ 1)$，$\alpha^6=(0\ 0\ 1\ 1\ 1)$，
$\alpha^7=(0\ 1\ 1\ 1\ 0)$，$\alpha^0=(0\ 0\ 0\ 0\ 0)\}$

W_1具有以下特点：

(i) W_1对V的加法和数乘封闭，秩=3，因此它是V的一个3维**子空间**。

(ii) 对W_1中所有的元素α^i，都有$\underline{A}(\alpha^i)\in W_1$，因此$W_1$是$V$的一个**不变子空间**。

(iii) W_1中所有元素，都可以表示成α，$\underline{A}(\alpha)$，$\underline{A}^2(\alpha)$，即α，α^2，α^3的线性组合，因此W_1是V的一个由α生成的3维**循环不变子空间**。

同理，$W_2=\{\beta^1=(1\ 1\ 0\ 1\ 1)$，$\beta^2=(1\ 0\ 1\ 1\ 0)$，
$\beta^3=(0\ 1\ 1\ 0\ 1)$，$\beta^0=(0\ 0\ 0\ 0\ 0)\}$

是V的一个2维循环不变子空间。

由于V中所有状态都可以表为如下形式：

$\alpha^i\oplus\beta^j$（其中$\alpha^i\in W_1$，$\beta^j\in W_2$），

且　维W_1+维W_2=3+2=5=维V，所以，V可以写成W_1、W_2的直和：

$V=W_1\dot{+}W_2$。

§3．线性反馈移存器及其状态与序列的多项式描述

§3．1　特征多项式

由上节已知，线性反馈移存器的变换功能可以用状态转移矩阵来表示。这个矩阵的特征多项式，就称为线性反馈移存器的**特征多项式**。

设：状态转移矩阵为A，则特征多项式为

$f(x)=|X\cdot E+A|$。

特征多项式描述了状态和序列的递推关系。设特征多项式

$f(x)=x^n+c_1x^{n-1}+\cdots+c_{n-1}x+1$，状态转移矩阵为$A$，则：

$f(A)=A^n+C_1A^{n-1}+\cdots+C_{n-1}A+E=0$

由此可推出：$A^n=C_1A^{n-1}+\cdots+C_{n-1}A+E$。

对移存器的状态来说，由于　$\alpha^i\cdot A^k=\alpha^{i+k}$，

故有　$\alpha^i\cdot A^n=\alpha^i(C_1A^{n-1}+\cdots+C_{n-1}A+E)$

$\Rightarrow\alpha^{n+i}=C_1\alpha^{n-1+i}+\cdots+C_{n-1}\alpha^{i+1}+\alpha^i$

这就是状态之间的递推关系。

设　线性反馈移存器的输出序列为

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

由于，状态α^i就是序列$\underline{a}$中从a_i开始的连续n个符号，即

$\alpha^i=(a_i,a_{i+1},\cdots\cdots,a_{i+n-1})$，因此状态$\alpha^i$，$\alpha^{i+1},\cdots,\alpha^{i+n}$之间的递推关系式完全对应于序列符号$a_i$，$a_{i+1}$，…，$a_{i+n}$之间的递推关系。

即由$\alpha^{i+n}=C_1\alpha^{i+n-1}+\cdots+C_{n-1}\alpha^{i+1}+\alpha^i$

可得$a_{i+n}=C_1a_{i+n-1}+\cdots+C_{n-1}a_{i+1}+a_i$。

因此，可以说，特征多项式各项的系数，就描述了状态和序列的递推关系。

例：如下面5级线性反馈移存器：

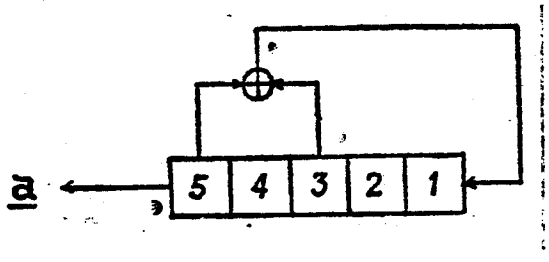

图1．5

它的状态转移矩阵

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

特征多项式　$f(x)=|XE+A|=x^5+x^2+1$

$\because$　$f(A)=A^5+A^2+E=0$

$\therefore$　$\alpha^iA^5+\alpha^iA^2+\alpha^i=0$

$\Rightarrow$　$\alpha^{i+5}+\alpha^{i+2}+\alpha^i=0$

故状态递推关系为：　$\alpha^{i+5}=\alpha^{i+2}+\alpha^i$

$\Rightarrow$　序列$\underline{a}$的递推关系：　$a_{i+5}=a_{i+2}+a_i$