

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。第八章至第十一章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，扈新生、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
§ 1. 线性移位寄存器的一般概念	1
§ 2. 状态转移变换	3
§ 2. 1 状态转移变换	3
§ 2. 2 状态转移矩阵	4
§ 2. 3 表出式转移矩阵	5
§ 2. 4 状态的循环不变子空间	6
§ 3. 线性反馈移存器及其状态与序列的多项式描述	7
§ 3. 1 特征多项式	7
§ 3. 2 抽头多项式	9
§ 3. 3 序列的左移变换、极小多项式	10
§ 3. 4 状态的极小多项式和表出多项式	11
§ 3. 5 特征多项式的特点与线性移存器性质的对应	14
§ 4. 生成函数	15
§ 5. 迹表示法	20
第二章 线性反馈移位寄存器的周期特性	27
§ 1. 移存器序列的周期	27
§ 2. 状态图 Σ 、中腿数和圈长的计算方法	31
§ 3. 有关的理论证明	35
第三章 m 序列	41
§ 1. m 序列与本原多项式	41
§ 2. m 序列的移加特性	42
§ 3. m 序列的伪随机性	44
§ 4. m 序列的采样特性 (选取特性)	48
§ 5. 绝对零起点 m 序列	51
第四章 线性反馈移位寄存器的综合	56
§ 1. 求序列极小多项式方法 (一) 解方程法	56
§ 2. 求序列极小多项式方法 (二) 迭代算法	58
§ 3. 求序列极小多项式方法 (三) 连分式法	62
§ 4. 状态极小多项式	64
§ 5. 已知序列中的某些符号求初态	65
§ 6. 已知含错序列求初态	67

第五章 状态和位置的互求	74
§ 1. 由位置求状态的方法	75
§ 1. 1 不可约多项式的位置求状态	76
§ 1. 2 可约多项式的位置求状态	79
§ 1. 3 已知第 k 步的状态 α^k 求初态 α^0	81
§ 2. 由状态求位置的方法	83
方法 1. 长除运算	83
方法 2. 一般方法	84
方法 3. 计算参数组	89
方法 4. 解同余方程组	93
方法 5. 计算机方法	95
第六章 线性移存器序列的分解与合成	99
§ 1. 线性移存器序列的分解特性	99
§ 2. 线性移存器序列的合成	108
§ 3. 有关合成序列的几个反推问题	119
§ 3. 1 已知合成序列及抽头求初始状态	119
§ 3. 2 已知抽头和 r 步后的合成序列求初态	122
§ 3. 3 已知线性合成序列及初始状态, 求模 2 加抽头	125
§ 3. 4 已知外来输入和反馈序列, 求反馈抽头	128
第七章 不等距级间模 2 加移位寄存器	134
§ 1. 不等距级间模 2 加寄存器的数学描述	134
§ 1. 1 状态转移矩阵	134
§ 1. 2 特征多项式和极小多项式	137
§ 1. 3 状态的极小多项式及其周期	139
§ 1. 4 各级输出序列的极小多项式和周期	144
§ 1. 5 C_A 状态和输出序列的极小多项式的求法	146
§ 2. 不等距级间模 2 加寄存器的状态图	149
§ 2. 1 一般概念	149
§ 2. 2 非奇异矩阵的状态图	150
§ 2. 3 幂零矩阵的状态图	153
§ 2. 4 奇异矩阵的状态图	155
§ 3. 状态与序列的关系	156
§ 3. 1 状态与序列的表出关系	156
§ 3. 2 极小多项式之间的联系	162
§ 3. 3 序列状态转移矩阵	166
§ 3. 4 输出序列之和及寄存器对输出序列的等价	171

§ 3. 5	序列之间的线性表出	176
§ 3. 6	输出序列之间的零相关	178
§ 4.	不等距级间模 2 加移寄存器的综合	182
§ 4. 1	已知输出序列的若干符号求初态	182
§ 4. 2	求不等距级间模 2 加的抽头逻辑	184
第八章	等距 1 部分级间模 2 加移寄存器	197
§ 1.	等距 1 部分级间模 2 加的数学描述	197
§ 1. 1	定义	197
§ 1. 2	状态转移矩阵	198
§ 1. 3	特征多项式和极小多项式	198
§ 1. 4	状态的极小多项式	200
§ 1. 5	各级序列的理论多项式和极小多项式	203
§ 2.	输出序列的平移等价及其起点差	204
第九章	全距 1 级间模 2 加移位寄存器	215
§ 1.	数学描述	215
§ 1. 1	特征多项式和极小多项式	215
§ 1. 2	矩阵 A 与循环矩阵 B	216
§ 1. 3	状态的多项式变换	217
§ 2.	状态分析	218
§ 2. 1	状态的极小多项式	218
§ 2. 2	状态图	219
§ 2. 3	圈上状态的周期	221
§ 2. 4	当 n 为奇数时, (λ, m) 的计算方法	223
§ 2. 5	当 n 为偶数时, (λ, m) 的计算方法	228
§ 3.	序列特点	230
§ 3. 1	表出式	230
§ 3. 2	输出序列的平移等价类与起点差	232
第十章	K 型移存器	241
§ 1.	K 型移存器的一般概念及其性质	241
§ 2.	$K-m$ 序列	243
§ 2. 1	$K-m$ 序列的基本概念, 存在性及其个数	244
§ 2. 2	拼合圈	246
§ 3.	t 圈与小 m 序列	250
§ 3. 1	K 圈、拼合圈与 t 圈的关系	250
§ 3. 2	小代表圈的几个特点	251
§ 3. 3	t 级 m 序列的绝对 0 起点	255

§ 3. 4 绝对 0 起点的确定	256
第十一章 对称组合式移位寄存器	260
§ 1. 移存器的并联与串联	260
§ 1. 1 并联组合	260
§ 1. 2 串联组合	263
§ 2. 对称组合式移存器的数学描述	265
§ 3. 状态与序列	270
§ 3. 1 状态特点	270
§ 3. 2 序列特点	273
§ 4. 2^l 对称组合式移存器	278
第十二章 前馈序列	289
§ 1. 引言、二元序列的根表示法	289
§ 2. 二端与门 m 前馈序列的分析	296
§ 3. 三端以上 m 前馈网络的分析	313
3. 1 三端与门网络的分析	313
3. 2 r 端与门网络的分析	322
§ 4. 非 m 前馈序列的分析	323
§ 5. 由 $F_r(x)$ 求 $f(x)$	332
§ 6. 前馈门电路中的与门降端	341
§ 6. 1 与门降端的条件	341
§ 6. 2 求降端初态的方法	342
§ 7. 前馈序列的线性表示	355
§ 8. 前馈序列的反推	359
§ 8. 1 求初态	359
§ 8. 2 求前馈网络	362
§ 9. m 前馈序列的分解	365
§ 9. 1 σ 变换	365
§ 9. 2 $\sigma(c)$ 被输入 m 序列线性表出	366
§ 9. 3 用 σ 变换解前 m 前馈序列的方法	370
§ 9. 4 m 前馈序列与陪集选取特点	373
§ 9. 5 用陪集选取分解 m 前馈序列的方法	377
第十三章 线性自动机的基本概念	388
§ 1. 线性自动机的定义	388
§ 2. 自动机的等价、同构与相似	392
§ 3. 线性自动机的极小化	397
§ 4. 线性自动机的标准形	405

第十四章 非线性移位寄存器介绍	412
§ 1. 非线性移位寄存器的数学描述	412
§ 1. 1 非线性移位寄存器的概念	412
§ 1. 2 π 元函数的功能刻划	414
§ 1. 3 有向图和德布鲁因—哥德图	420
§ 1. 3. 1 有向图	420
§ 1. 3. 2 德布鲁因—哥德图 (<i>De Bruijn—Good</i> 图)	421
§ 1. 3. 3 n 级 $D-G$ 图的极大图	422
§ 2. 非奇异非线性移存器的分析	424
§ 2. 1 非奇异移存器的定义	424
§ 2. 2 n 级非奇异移存器状态图的拆圈和并圈	426
§ 2. 3 纯轮换移存器和补轮换移存器的分析	429
§ 2. 3. 1 墨比乌斯函数和墨比乌斯反馈公式	429
§ 2. 3. 2 纯轮换移存器	431
§ 2. 3. 3 补轮换移存器	434
§ 2. 4 非奇异移存器的状态图中图的个数的上界和奇偶性	438
§ 3. M 序列	440
§ 3. 1 关于 M 序列的一般概念	440
§ 3. 2 求全部 n 级 M 序列及其反馈函数的一个方法—剪接法	442
§ 3. 2. 1 状态图的相等	442
§ 3. 2. 2 连线及其交点的赋值	443
§ 3. 2. 3 最大圈的剪接	443
§ 3. 2. 4 新反馈逻辑的标记	446
§ 3. 2. 5 多次联合剪接	446
§ 3. 2. 6 举例	449
§ 3. 3 产生 M 序列的反馈函数所适合的一些必要条件	450
§ 3. 4 M 序列的伪随机性	452
§ 4. 非线性移位寄存器的综合	455
§ 4. 1 第一种类型的问题	455
§ 4. 2 第二种类型的问题	456
§ 4. 3 第三种类型的问题	459
§ 4. 4 间接方法	462
§ 4. 5 π 项转换法	463
§ 4. 6 一种求初态的方法	466
§ 5. 非线性反馈移存器的串联	468

§ 5. 1	非线性反馈移寄存器的生成多项式	468
§ 5. 2	生成多项式的三种变换	470
§ 5. 3	非线性生成多项式的乘法运算法则	472
§ 5. 4	不具有最后反馈的非线性多项式的乘法运算与移寄存器的串联	473
§ 5. 5	包含最后反馈的生成多项式的乘积与移寄存器的串联	477
§ 6.	生成多项式的组合性质和对称形式	481
§ 6. 1	组合多项式的性质	481
§ 6. 2	多项式的对称形式	483
附:	常用数表	487
附表 I	2^n 数表 ($0 < n \leq 50$)	437
附表 I	C_n^r 数表 ($m = n \leq 20$)	488
附表 II	A_n 数表 ($m = n \leq 20$)	489
附表 IV	素数表 ($0 < p \leq 10000$)	491
附表 V	$2^n - 1$ 素因数分解表 ($0 < n \leq 100$)	496
附表 VI	F_2 上本原多项式表 (次数 ≤ 100)	499
附表 VII	$2^n - 1$ 陪集分解表 ($2 \leq n \leq 9$)	501
附表 VIII	F_2 上不可约多项式表 ($0 < \text{次数} \leq 14$)	507

§ 1. 线性移位寄存器的一般概念

图1.1中1, 2, 3, ..., $n-1$, n 为移位寄存器(可简称为移存器)的各级编号; $c_1, c_2, \dots, c_n$,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。

向量 $\alpha^0 = (a_0, a_1, \dots, a_{n-1})$ 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 $\alpha^i = (a_i, a_{i+1}, \dots, a_{i+n-1})$ 。显然， n 级移存器共有 2^n 个不同的状态。

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

$$a_{i+n} = c_1 a_{n-1+i} + c_2 a_{n-2+i} + \dots + c_n a_i, \quad i = 0, 1, 2, \dots$$

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：

$$a_{i+n} = c_1 a_{i+n-1} + c_2 a_{i+n-2} + \cdots + c_n a_i, \quad i = 0, 1, 2, \dots, \quad (1)$$

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：
 $\underline{a} = (a_0, a_1, a_2, \dots, a_n, a_{n+1}, a_{n+2}, \dots)$

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

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

$$a_{i+n} = \sum_{j=0}^{n-1} c_j a_{i+j} \quad i = 0, 1, 2, \dots$$

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

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

$\therefore \underline{a}$ 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

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

线性反馈移存器序列又可简称为 **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。

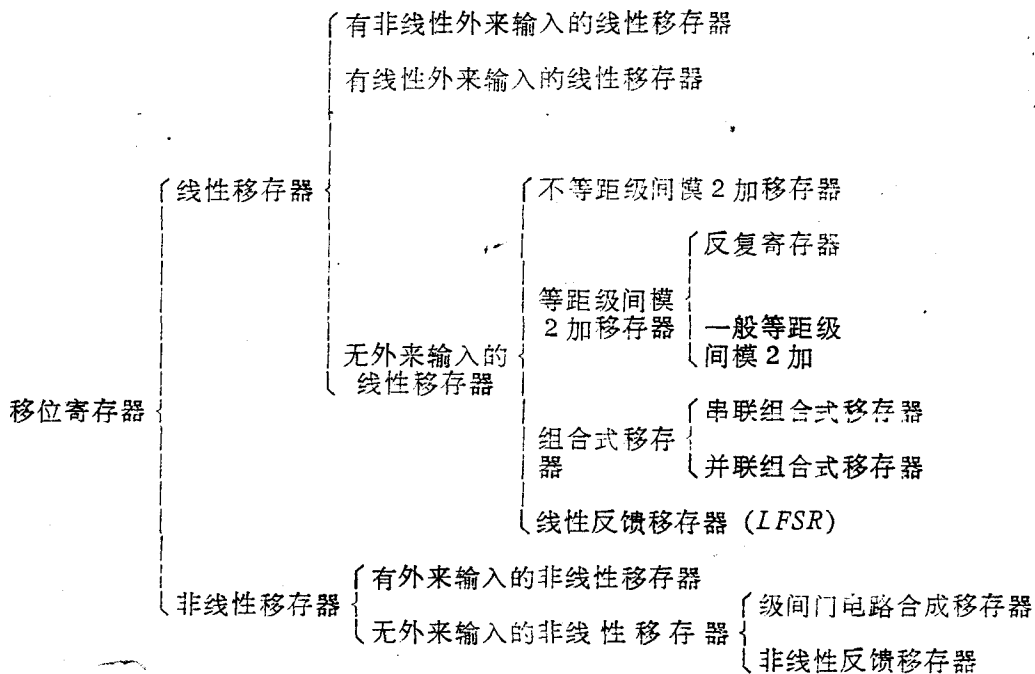


表 1. 2

§ 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：

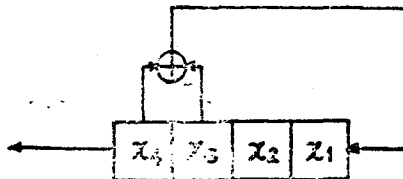


图 1. 2

设：前一状态为 $\alpha^i = (x_4 x_3 x_2 x_1)$ ，则下一状态为

$$\alpha^{i+1} = \underline{A}(\alpha^i) = \underline{A}(x_4 x_3 x_2 x_1)$$

$$\text{由 } \underline{A}(x_4) = x_3$$

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

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

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

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

$\underline{A}$ 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 $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$ 做为的一组基，设它们在状态转移变换 $\underline{A}$ 下的象为 $\underline{A}\varepsilon_1, \underline{A}\varepsilon_2, \dots, \underline{A}\varepsilon_n$ ，

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

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

状态转移矩阵 A 的作用是:

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

§2.3 表出式及其转移矩阵

例: 4 级线性反馈移存器如下图:

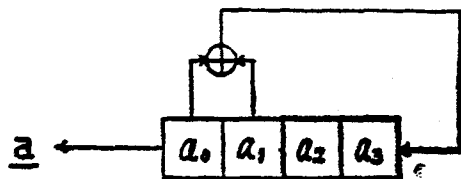


图 1.3

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

线性递推关系为 $a_{i+4} = a_{i+1} + a_i, i = 0, 1, 2, \dots$.

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。

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

σ^i 即为 a_i 在初态 $\alpha^0 = (a_0, a_1, a_2, a_3)$ 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: $\sigma^0, \sigma^1, \sigma^2, \sigma^3, \dots, \sigma^{n-1}$, 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。

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

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 $\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{n-1}$ 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 $\alpha^0, \alpha^1, \dots, \alpha^{n-1}$ 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。

全体状态表出式也构成一个 n 维线性空间, 记为 U 。

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

$$\alpha^1 = 0 \cdot \alpha^0 + 1 \cdot \alpha^1 + 0 \cdot \alpha^2 + 0 \cdot \alpha^3 \Rightarrow (0 \ 1 \ 0 \ 0) = \sigma^1$$

$$\alpha^2 = 0 \cdot \alpha^0 + 0 \cdot \alpha^1 + 1 \cdot \alpha^2 + 0 \cdot \alpha^3 \Rightarrow (0 \ 0 \ 1 \ 0) = \sigma^2$$

$$\alpha^3 = 0 \cdot \alpha^0 + 0 \cdot \alpha^1 + 0 \cdot \alpha^2 + 1 \cdot \alpha^3 \Rightarrow (0 \ 0 \ 0 \ 1) = \sigma^3$$

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

σ^i 即为状态 α^i 在 $\alpha^0, \alpha^1, \alpha^2, \alpha^3$ 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 σ^i 写成列向量, 那么显然有: $A \sigma^i = \sigma^{i+1}$; $A' \alpha^0 = \sigma^i$ 。 (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:

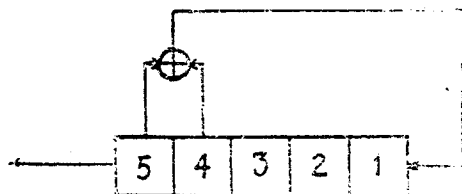


图 1. 4

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 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：

$$\alpha^i \oplus \beta^j \quad (\text{其中 } \alpha^i \in W_1, \beta^j \in W_2),$$

且 $\dim W_1 + \dim W_2 = 3 + 2 = 5 = \dim V$ ，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

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

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

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

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

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

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

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

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

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

$$\alpha^i = (a_i, a_{i+1}, \dots, a_{i+n-1}), \text{ 因此状态 } \alpha^i, \alpha^{i+1}, \dots, \alpha^{i+n} \text{ 之间的递推关系式完全}$$

对应于序列符号 $a_i, a_{i+1}, \dots, a_{i+n}$ 之间的递推关系。

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

$$\text{可得 } a_{i+n} = C_1a_{i+n-1} + \dots + C_{n-1}a_{i+1} + a_i.$$

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:

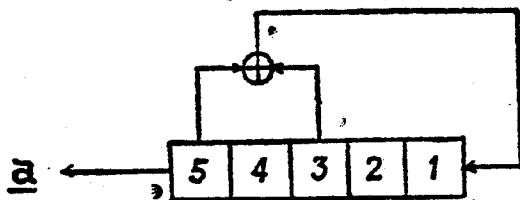


图 1. 5

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 $f(x) = |XE + A| = x^5 + x^2 + 1$

$$\therefore f(A) = A^5 + A^2 + E = 0$$

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

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

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

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