移位寄存器序列

尹文霖 编著

四川人民出版社

移位寄存器序列

尹文霖　编著

四川人民出版社

一九八二年·成都

移位寄存器序列 尹文霖 编著

四川人民出版社出版 （成都盐道街三号）

四川省新华书店发行 四川新华印刷厂印刷

开本 787×1092 毫米 1/32 印张 6.25 插页 4 字数 134千

1982年10月第一版 1982年10月第一次印刷

印数：1—5,780册

书号：15118·63 定价：1.05 元

前　言

移位寄存器序列，在现代通讯中，有很多重要应用。原稿系应有关单位要求，在四川大学讲授其数学内容时的讲义。它的先行课程是线代数与有限域。

移位寄存器的基本问题是分析——给定一个移位寄存器讨论它所产生的诸序列的某些特性——与综合——给定序列的某些特性求产生此种序列的移位寄存器（亦即求出其开关线路或曰反馈逻辑）。本书第一章建立基本概念并分析一个任意给定的移位寄存器产生的全部序列。第二章分析一个任意给定序列的某些特性。第三章讨论一类重要的特殊序列——双值自相关序列，建立其与差集的联系，并不加证明地征引了若干关于差集的已知结果。第四章讨论一类重要的特殊的移位寄存器——线性移位寄存器——的分析与综合问题。第五章对图论作一简介。第六章通过状态图间彼此的相互关系对状态图作进一步的分析。第七章讨论一类重要序列——最长移位寄存器序列。第八章给出几个一般的综合办法。

在编写本书过程中，曾得到段学复、万哲先、聂灵沼、丁石荪诸位教授和有关单位的大力支持，多次赠予有关资料，给予鼓励。李德琅同志曾参与讲授初稿的编写工作，并多次提供宝贵意见。例如线性移位寄存器的极小多项式的表示式〔第四章（6）式〕，就是他在1974年首先提出的。

在此，一并表示感谢。由于本人知识、业务水平有限，书中难免个人管见。不足之处，望读者批评指正。

作　者

一九八一年十月

符 号 说 明

F_2——二元域，亦记作F；

$F[x]/h(x)$——F上的多项式对模h(x)的剩余类环；

$[r]$——不超过r的最大整数；

$(a_1, a_2, \cdots, a_n)$——n位向量。在不必明确诸分量的场合，常简记作a。无穷序列亦以黑体字表之；

(a, b)——作为非向量的整数出现时，表示a与b的最大公因数；

$[a, b]$——a与b的最小公倍数；

$(f(x), g(x))$——f(x)与g(x)的最高公因式；

$\{f(x), g(x)\}$——f(x)与g(x)的最低公倍式；

$a \mid b$——a除得尽b；

$a \nmid b$——a除不尽b；

$a \equiv b \pmod m$——$m \mid (a-b)$；

$a \not\equiv b \pmod m$——$m \nmid (a-b)$；

$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n$；

$\sum_{d \mid M} a_d$——d过M的因子求和。如 $\sum_{d \mid 6} a_d = a_1 + a_2 + a_3 + a_6$；

$\prod_{i=1}^{n} a_i = a_1 a_2 \cdots a_n$；

$\prod_{d \mid M} a_d$——d过M的因子求积；

$v(a)$——序列a的周期。在不需要指明序列的场合常简记作v。

$p(f)$——多项式$f(x)\neq x$的指数。即合于$x^p\equiv 1 \pmod{f(x)}$的最小自然数p。在不需要指明多项式的场合简记作p。

Ind $f(x)$——不可约多项式$f(x)$的指标。即$(2^n-1)/p$，式中n为$f(x)$的次数，p为$f(x)$的指数；

$e_v(q)$——q对模v的指数。即合$q^m\equiv 1 \pmod{v}$的最小自然数m。在不必明确模v的场合，常简记作$e(q)$；

$\varphi(n)$——不超过n而与n互素的自然数的个数；

$\varphi(f(x))$——次数不超过$f(x)$的次数且与$f(x)$互素的多项式的个数；

$G_f=G(f)=G(f(x))$——以$f(x)$为反馈逻辑的移位寄存器的状态图；

$N_f=N(f)=N(f(x))$——$G(f)$中的圈数；

$Z(n)$——n级纯循环移位寄存器状态图的圈数；

$Z^*(n)$——n级补循环移位寄存器状态图的圈数。

目　录

第一章　状态图分析

移位寄存器的全部功能与其状态图是相互决定的。本章主要介绍有关基本概念，并初步讨论一个给定的移位寄存器状态图的枝和圈数。

1．移位寄存器序列

反馈移位寄存器（简称**移位寄存器**）是个如图1.1.1所

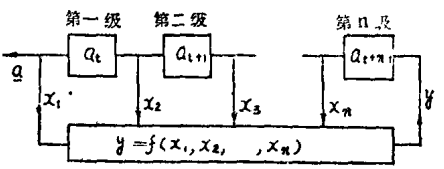

图1.1.1　n级反馈移位寄存器框图

示的脉冲电动设备。图中各小正方形表寄存器，都是具有1（开、有等）、0（关、无等）两种可能**状态**（视作二元域F_2中两个元素）的有一个输入和一个输出的记忆元件。在时钟脉冲到达时，元件所处状态即为输出，同时接受一个输入作为新状态，而寄存器又忆记着它直至下一个脉冲到达，故状态与时刻有关。图示时刻t，第i级寄存器处于状态a_{t+i-1}，$i=1,2,\cdots,n$，我们称向量

$$S(t)=(a_t,a_{t+1},\cdots,a_{t+n-1})$$

为整个**移位寄存器在时刻t的状态**，可简称**状态**，亦记作$S_t(a)$。又图中$f(x_1, x_2, \cdots, x_n)$是有n个输入（即$x_1, \cdots, x_n$）及一个输出y的**反馈开关线路**（亦称**反馈逻辑**），故f即取值于F_2上的一个n元函数。在时刻$t+1$，$x_i = a_{t+i-1}$，$i = 1, \cdots, n$，移位寄存器的状态为

$$S(t+1) = \left(a_{t+1}, a_{t+2}, \cdots, a_{t+n-1}, f(a_t, a_{t+1} \cdots, a_{t+n-1})\right)$$

又取第一级寄存器的输出作为整个移位寄存器的**输出**。并在任意给定**初态**$S_0(a) = (a_0, a_1, \cdots, a_{n-1})$后，随着时钟脉冲逐次到达，便得到唯一确定的一个输出序列，即

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

称为**移位寄存器序列**。这个序列完全由递归关系（即反馈逻辑的序列表示法）

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

与初态决定。

我们常只讨论**非退化反馈移位寄存器**（除非另有声明），如图1.1.1所示，第n级所接受反馈y之值与第一级状态有关（简称第一级参加反馈），因为这是最常见，最重要的一种移位寄存器。实际上，退化指y值与第一级无关，即相当于级数减少。确切地说，退化移位寄存器产生的序列，除最初几个数元外，与某个非退化的移位寄存器产生的序列全同。

例1. 3级纯循环移位寄存器，记作 PCR_3，即反馈逻辑 $f(x_1, x_2, x_3) = x_1$，如图1.1.2。

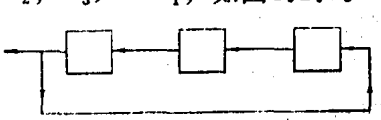

图1.1.2 PCR_3 即 $f(x_1, x_2, x_3) = x_1$

其初态与相应的序列如下表：

$S_0(a)$	
0 0 0	000000000000…… = (0)
0 0 1	001001001001…… = (001)
0 1 0	010010010010…… = (010)
0 1 1	011011011011…… = (011)
1 0 0	100100100100…… = (100)
1 0 1	101101101101…… = (101)
1 1 0	110110110110…… = (110)
1 1 1	111111111111…… = (1)

表中用括号表示重复出现（下同）。

例2． $f(x_1, x_2, x_3) = 1 + x_1$ 或 x_1x_2，其框图分别见图1.1.3(A)及(B)，前者称为3级补循环移位寄存器，简记为 CCR_3。

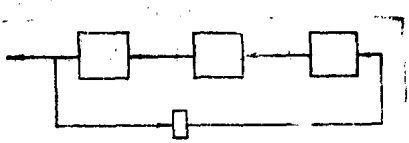

图 1.1.3(A) CCR_3 $f(x_1, x_2, x_3) = 1 + x_1$

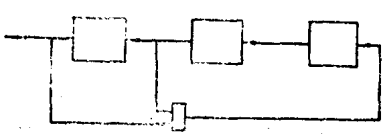

图1.1.3(B) $f(x_1, x_2, x_3) = x_1x_2$。

其初态与相应的移位寄存器序列如下表：

$S_0(a)$	$a(CCR_3)$	$a(f=x_1x_2)$
0 0 0	(000111)	(0)
0 0 1	(001110)	001 (0)
0 1 0	(01)	01 (0)
0 1 1	(011100)	01101(0)
1 0 0	(100011)	1 (0)
1 0 1	(10)	101 (0)
1 1 0	(110001)	1101 (0)
1 1 1	(111000)	(1)

我们看到：移位寄存器序列可以是周期的，也可以是非周期的。但无论如何，最后总要出现周期重复的现象。这是因为 n 级移位寄存器的不同状态恰有 2^n 种，而一旦某一状态出现，它的所有的后继状态，均一一确定。即有

定理 1．给定 n 级移位寄存器，则 2^n 个初态产生 2^n 个不同的移位寄存器序列，且每个序列都要产生数元个数$\leqslant 2^n$的周期重复段。

2．真值表、小项表示、多项式表示。

本节介绍开关函数的三种表示法。所谓**开关函数**就是一个自变量和函数值均在F中的函数，换句话说，就是 2^n个n位有序0、1数组x（称为**点**）作成的集合（称为**点空间**）

$$V_n=\left\{x_i \quad x=(x_1,\cdots,x_n),\ x_i\varepsilon F\right\}$$

到 F_2 内（或上）的一个映射：

$$x=(x_1,\cdots,x_n)\to y,\ y\varepsilon F_2,\ x\varepsilon V.$$

记作

$$y=f(x_1,\ \cdots,\ x_n)\quad 或\quad y=f(x)。$$

实际上，一个反馈逻辑就是一个反馈开关函数。

显然，n维点空间共有2^n个点2^{2^n}个不同的开关函数（每点可取两值），而一个移位寄存器的功能被一个开关函数唯一确定；反之，一个移位寄存器的功能又唯一确定一个开关函数。

2.1. **真值表** 刻划开关函数最直接的办法就是列表，即对每个点x列出对应的函数值。称为真值表。

为了查表方便，通常采用字典排法，即视x为n位二进数，再按大小，一位一位依次往下排；亦即从左到右，先0后1，一位一位往下排。

例。 PCR_3、CCR_3、$f(x_1,x_2,x_3)=x_1x_2$ 的真值表

	f_{PCR}	f_{CCR}	$f=x_1x_2$
000	0	1	0
001	0	1	0
010	0	1	0
011	0	1	0
100	1	0	0
101	1	0	0
110	1	0	1
111	1	0	1

真值表中函数值取值1的次数称为该函数的**重量**，记为w(f)，即：

$$W(f)=\sum_{f(x)=1,x\in V_n} 1$$

如上表，则有 $w(f_{PCR_3})=4=W(f_{CCR_3})$，而 $w(x_1x_2)=2$

2.2. **小项表示** 点的特征函数乘以该点上的函数值的（模2）和是刻划开关函数的第二种办法。所谓一个点的**特征函数**就是在该点取值1，其余（V_n中）点上均取值0的函数。

令 $x^0=1+x$，称为函数的**补函数**（在一般的布尔代数中常用符号 $\bar{x}$ 来表示，（简称为x**取补**）。故对，$c\in F_2$，穷举四种可能得到：

$$x^c=\begin{cases}1, & x=c,\\ 0, & x\neq c,\end{cases}$$

又对 $c=(c_1, c_2,\cdots, c_n)\in V_n$，令

$$\chi(c)=x_1^{c_1}x_2^{c_2}\cdots x_n^{c_n}=\begin{cases}1, & x=c,\\ 0, & x\neq c.\end{cases}$$

就是点c的特征函数（称为一个**小项**）。于是：

$$f(x)=f(x_1, x_2,\cdots,x_n)$$

$$=\sum_{c_1=0}^{1}\cdots\sum_{c_n=0}^{1}f(c_1,\cdots,c_n)\,x^{c_1}\cdots x^{c_n}=$$

$$=\sum_{c\in V_n}f(c)\chi(c)=\sum_{f(c)=1}\chi(c)$$

就是开关函数$f(x_1, \cdots, x_n)$的小项表示，由函数值 $y=f(c_1\cdots, c_n)$的唯一性，立知小项表示的唯一性。

例. $f_{PCR_3}=x_1\bar{x}_2\bar{x}_3+x_1\bar{x}_2x_3+x_1x_2\bar{x}_3+x_1x_2x_3$

2.3. **多项式示表** 将$f(x)$的小项表示展开(分配律)、化简（交换，给合律），得到诸变元的单项式之和，称为$f(x)$的多项式表示。即：

$$f(x_1,\cdots,x_n)=a_0+\sum_{i=1}^{n}a_ix_i+\sum_{i>j}a_{ij}x_ix_j+\sum_{i>j>k}a_{ijk}x_ix_jx_k+\cdots+a_{12\ldots n}x_1x_2\cdots x_n$$

式中诸a为0或1。

一个n元开关函数的多项式表示共含2^n个项，因而共有2^{2^n}个不同的多项式表示，与不同的开关函数的个数一致，因而一个开关函数的多项式表示是唯一的。

我们指出，小项表示在物理上（或逻辑上）意味着开关函数可用与，非，加三种门电路来实现，而多项式表示意味着可用与，1，加来实现。

例. $\bar{x}_1\bar{x}_2\bar{x}_3+\bar{x}_1\bar{x}_2x_3+\bar{x}_1x_2\bar{x}_3+\bar{x}_1x_2x_3+x_1\bar{x}_2\bar{x}_3+x_1\bar{x}_2x_3=1+x_1x_2$

参见2.1.节x_1x_2的真值表。

当多项式表示是$x_1, \cdots, x_n$的线性齐次多项式，即

$$f(x_1, \cdots, x_n)=c_1x_1+c_2x_2+\cdots+c_nx_n,$$

式中诸c为0或1时，称以f为反馈逻辑的n位移

位寄存器为**线性的**，否则就叫n位**非线性移位寄存器**，显然，线性移位寄存器在逻辑上可仅用加法器实现。

在线性的场合，n级移位寄存器的真值表可用公式（如前所述仅考虑非退化的场合）

$$x_{n+1}=\sum_{i=1}^{n}c_i x_i, \qquad c_i=1$$

表达，亦可写作

$$\sum_{i=1}^{n+1}c_i x_i=0, \qquad c_1 c_{n+1}=1.$$

常称之为**线性递归关系**。为讨论方便起见，有时令 $a_i=x_{i+1}$，$h_i=c_{n+1-i}$，$i=0,1,\cdots,n$，上式化作

$$\sum_{i=0}^{n}h_i a_{n-i}=0, \qquad h_0 h_n=1$$

其框图见图1.2。

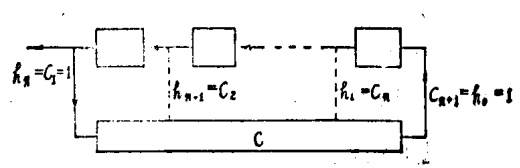

图1.2. 线性移位寄存器

图中C是模2累加器，而诸寄存器与C连通否视h_i，$i=1,\cdots,n$，取值1或0而定。

3. 状态（转移）图

表示移位寄存寄功能的另一种方法是：在平面上用2^n个点表示n位移位器存器的2^n种状态，并用箭头标明其相互联系，即在时钟脉冲作用下，一个状态怎样转变到另一个状态。例如PCR_3，共有$2^3 = 8$种状态。从状态（000）出发，下一状态还是（000），于是从点(000)划箭头回到它自己，这样的图叫一个**环**，如图1.3.1（a）；同样从点(001)出发，下一个状态是(010)，就用前者作箭尾，后者作箭头所向把它们联起来。如此继续下去，经过三次后，又回到(001)，于是得到一个圈。如在图1.3.1（b)。在8种状态中余下的状态里任选一个仿上进行，至8种状态全画出为止。这样得到的图称为PCR_3的**状态转移图**，简称**状态图**。它由彼此不相交的四个圈组成。

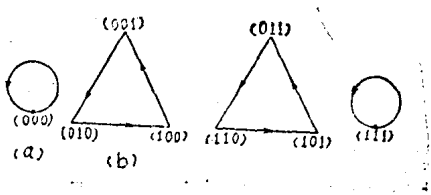

图1.3.1 PCR_3的状态图

我们看到状态图是移位寄存器状态x在移位脉冲作用下，转移到后继状态x′如下表的图像表示。