非线性移位寄存器

万哲先　代宗铎
刘木兰　冯绪宁　编著

科学出版社

非线性移位寄存器

万哲先　代宗铎
刘木兰　马绪宁　编著

科学出版社
1978

内 容 简 介

本书综述了非线性移位寄存器的主要研究成果，包括对该寄存器的分析和综合以及由它所产生的M序列等方面的结果，也附带介绍了研究它所需要的图论知识和开关函数的极小化方法。

读者对象为从事数学和通信方面工作的有关研究、技术人员以及大专院校有关专业的师生。

非线性移位寄存器

万哲先　代宗铎
刘木兰　冯绪宁　编著

*

科学出版社出版
北京朝阳门内大街137号
中国科学院印刷厂印刷
新华书店北京发行所发行　各地新华书店经售

*

1978年10月第一版　开本：787×1092 1/32
1978年10月第一次印刷　印张：7
印数：0001—26,130　字数：156,000

统一书号：13031·810
本社书号：1158·13—1

定价：0.85元

序　言

近二十年来，由于反馈移位寄存器所产生的一些二元序列有许多重要应用，所以它的研究很受重视．例如，在连续波雷达中可用作测距信号，在遥控系统中可用作遥控信号，在多址通信中可用作地址信号，在数字通信中可用作群同步信号，此外还可用作噪声源以及在保密通信中起加密作用等等．关于线性移位寄存器，由于有有效的代数工具对它进行分析，它的理论已相当完整．至于非线性移位寄存器的理论，目前还很不成熟．这方面的结果，除戈龙布（S. W. Golomb）将他本人和他的一些合作者的几篇工作报告汇编成《移位寄存器序列》[Shift Register Sequences (Holden-Day, San Francisco, U. S. A., 1967)] 一书外，还散见于各杂志和报告中．鉴于我国有关读者迫切要求这方面读物，特将各书刊上已发表的主要研究结果汇编成书，书中也包括我们自己工作中所得到的一些新成果和新证明．本书出版后，希望能得到读者的批评指正．

作　者

1975 年

目　录

第一章 引 论

§1.1 两个例子

例1 考察下面这个 3 级反馈移位寄存器

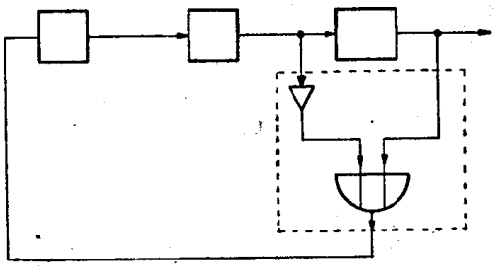


图 1.1

图 1.1 的上方一排 3 个小方框代表 3 个寄存器，把它们从左往右依序叫做第 1 级、第 2 级、第 3 级寄存器. 每个寄存器有两种可能的状态，分别用 0 和 1 来代表，而 0 和 1 可以看作是仅含两个元素的有限域 $\mathbf{F}_2$ 中的元素[1]. 图 1.1 中用虚线框起来那一部分电路是一个有两个输入端和一个输出端的组合电路，它包含一个“非门”和一个“或门”. 符号

1) $\mathbf{F}_2$ 是仅含两个元素的集合，用 0 和 1 来代表这两个元素. 在 $\mathbf{F}_2$ 中规定了如下的加法和乘法两种运算：

$$0+0=1+1=0,\ 0+1=1+0=1,$$
$$0\cdot 0=1\cdot 0=0\cdot 1=0,\ 1\cdot 1=1.$$

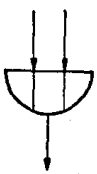
这样 $\mathbf{F}_2$ 就是一个域. 关于域的定义，可参看万哲先，代数和编码(科学出版社，1976)，第一章，§1.

代表一个“非门”，它有一个输入端和一个输出端；当输入端的输入是 x 时，我们通常把它的输出记作 $\bar{x}$，$\bar{x}$ 对 x 的依赖关系是

表 1.1

x	$\bar{x}$
0	1
1	0

图 1.1 中符号



代表一个“或门”，它有两个输入端和一个输出端；当两个输入端的输入分别是 x 和 y 时，它的输出是 $x \vee y$，这里 $x \vee y$ 表示 x 和 y 的逻辑和，它对于 x 和 y 的依赖关系可用表 1.2 来表示。

表 1.2

x	y	$x \vee y$
0	0	0
0	1	1
1	0	1
1	1	1

假定在某一时刻，第 1 级寄存器的状态是 a_3，第 2 级寄存器的状态是 a_2，第 3 级寄存器的状态是 a_1，我们就说这个 3 级反馈移位寄存器在这一时刻的状态是 (a_1, a_2, a_3). 因为 a_1, a_2, a_3 可以独立地取 $\mathbf{F}_2$ 中的元素 0 或 1 为值，所以这个 3

级反馈移位寄存器一共有 $2^3=8$ 个可能的状态，而

$$\mathbf{F}_2^3=\{(a_1,a_2,a_3)\mid a_1,a_2,a_3\in\mathbf{F}_2\}$$

就是它的状态集．假定在某一时刻，这个 3 级反馈移位寄存器的状态是 (a_1,a_2,a_3)．加上一个移位脉冲后，一方面每个寄存器的内容移给它右面的一级，最右面一级的内容就是输出；另一方面将第 2 级的内容 a_2 输送给“非门”，并将“非门”的输出 $\bar{a}_2$ 和第 1 级的内容 a_1 又输送给图 1 下方的“或门”，再将这个“或门”的输出 $a_1\vee\bar{a}_2$ 输送给最左面一级（即第 1 级）寄存器，这一过程就叫反馈．这样这个反馈移位寄存器的状态就变成 $(a_2,a_3,a_1\vee\bar{a}_2)$，而输出是 a_1．我们也说，加上一个移位脉冲后，这个反馈移位寄存器从状态 (a_1,a_2,a_3) 转移到 $(a_2,a_3,a_1\vee\bar{a}_2)$，而输出是 a_1．从状态 (a_1,a_2,a_3) 转移到状态 $(a_2,a_3,a_1\vee\bar{a}_2)$ 的变换

$$(a_1,a_2,a_3)\to(a_2,a_3,a_1\vee\bar{a}_2)$$

叫做这个反馈移位寄存器的*状态转移变换*，它是将状态集 $\mathbf{F}_2^3$ 映到自身之中的一个映射．我们说一个反馈移位寄存器的功能是指任意给定它的状态，加一个移位脉冲后，它转移到哪个状态以及它的输出是什么．由于反馈移位寄存器的输出由它

表 1.3

本状态 (a_1,a_2,a_3)			下一状态 $(a_2,a_3,a_1\vee\bar{a}_1)$		
0	0	0	0	0	1
0	0	1	0	1	1
0	1	0	1	0	0
0	1	1	1	1	0
1	0	0	0	0	1
1	0	1	0	1	1
1	1	0	1	0	1
1	1	1	1	1	1

的状态唯一确定，因此反馈移位寄存器的功能由它的状态转移变换完全确定．上面这个反馈移位寄存器的状态转移变换可用状态转移表 1.3 来表示．注意，表 1.3 中 8 个可能的状态的先后次序是按以下规则排列的：先规定 $0<1$；我们把 (a_1, a_2, a_3) 排在 (b_1, b_2, b_3) 的前面，如果 $a_1<b_1$，或 $a_1=b_1$ 而 $a_2<b_2$ 或 $a_1=b_1$，$a_2=b_2$ 而 $a_3<b_3$．这种排列方法通常叫按字典次序排列．

我们把函数

$$f(x_1, x_2, x_3)=x_1 \vee \bar{x}_2$$

叫做这个反馈移位寄存器的反馈函数，有时也叫反馈逻辑．它表明当这个反馈移位寄存器的状态是 (x_1, x_2, x_3) 时，加一个移位脉冲后，反馈给最左面一级(即第 1 级)寄存器的内容就是 $f(x_1, x_2, x_3)=x_1 \vee \bar{x}_2$．那么这个反馈移位寄存器就从状态 (x_1, x_2, x_3) 转移到状态 $(x_2, x_3, f(x_1, x_2, x_3))=(x_2, x_3, x_1 \vee \bar{x}_2)$．因此这个反馈移位寄存器的功能就由它的反馈函数完全确定，反馈函数 $f(x_1, x_2, x_3)=x_1 \vee \bar{x}_2$ 也可以用它的函数值表 1.4 来表示．反馈函数的函数值表通常叫做它的真值表．

表 1.4

x_1	x_2	x_3	$f(x_1,x_2,x_3)=x_1 \vee \bar{x}_2$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

在数学上表示反馈移位寄存器的功能的另一方法是用状态转移图，简称状态图．图 1.2 是上述 3 级反馈移位寄存器的状态图．图中 8 个小圆圈分别代表它的 8 个可能的状态，

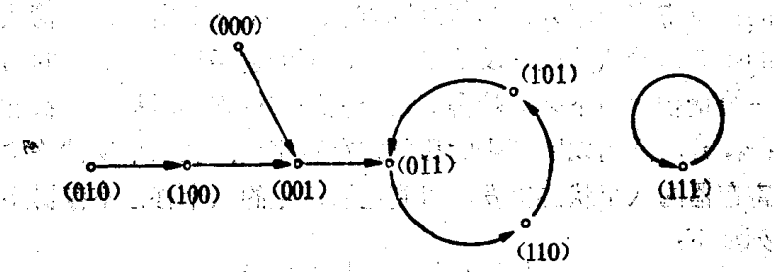


图 1.2

在每个小圆圈的附近标上它所代表的状态．这 8 个小圆圈叫做这个状态图的顶点．图 1.2 中从每个顶点出发恰有一根带箭头的线段(直线段或曲线段)终止于另一顶点．这个带箭头的线段叫做弧，它出发的顶点叫做它的起点，而它终止的顶点叫做它的终点．这样一共有 8 条弧，这 8 条弧都是有方向的，所以这个图是个有向图．这 8 条弧表明这个反馈移位寄存器的状态转移关系，即如果这个反馈移位寄存器的状态是某一顶点，加一个移位脉冲后，这个反馈移位寄存器就转移到以这个状态为起点的弧的终点．因此这个反馈移位寄存器的功能由它的状态图完全确定．注意，这个反馈移位寄存器的状态图里有两个圈，它们的圈长(即圈上的顶点个数)一个等于 3，另一个等于1．其余的 4 个状态都在圈长等于 3 的圈的枝上．

假定这个反馈移位寄存器的初始状态是 (a_0, a_1, a_2)，那么不断地加移位脉冲，这个反馈移位寄存器的输出就是一个二元序列

$$a_0, a_1, a_2, \cdots$$

其中

$$a_n = a_{n-3} \vee \bar{a}_{n-2}, \quad n \geq 3.$$

这个二元序列叫做这个反馈移位寄存器从初始状态(a_0, a_1, a_2)出发所产生的*移位寄存器序列*. 也可以利用状态图来得到这个反馈移位寄存器从任一初始状态 (a_0, a_1, a_2) 出发所产生的移位寄存器序列.这只要从顶点 (a_0, a_1, a_2) 出发，按箭头的指向沿着弧一段一段地走下去，把沿途经过的各状态的第一分量依序写下来，就得到这个反馈移位寄存器从初始状态 (a_0, a_1, a_2) 出发所产生的移位寄存器序列. 从这个反馈移位寄存器的八个状态出发，得到它所产生的八个移位寄存器序列如下：

$$
\begin{array}{l}
1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ \cdots \\
0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ \cdots \\
1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ \cdots \\
1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ \cdots \\
0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ \cdots \\
0\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ \cdots \\
1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ \cdots \\
0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ \cdots
\end{array}
$$

值得注意的是，从圈长等于 1 的圈上的状态(111)出发所产生的序列是周期等于 1 的*周期序列*[1]；从圈长等于 3 的圈上的任一状态出发所产生的序列都是周期等于 3 的周期序列，而且它们都*平移等价*[2]；从其余 4 个状态出发所产生的序列，如果

---

1) 一个二元序列(即元素属于 F_2 的序列)

$$a_0, a_1, a_2, \cdots \quad (a_i \in F_2)$$

叫周期序列，如果有一个正整数 l 存在，使

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

而满足上述条件的最小正整数 l 就叫做它的周期.

2) 两个二元周期序列

$$a_0, a_1, a_2, \cdots$$
$$b_0, b_1, b_2, \cdots$$

叫平移等价，如果有一个非负整数 l 存在，使

$$a_{k+l} = b_k, \quad k = 0, 1, 2, \cdots.$$

适当略去前面几项，也都是周期等于 3 的周期序列，而且与从圈长等于 3 的圈上的某一状态出发所产生的序列一致.

例 2 考察图 1.3 这个 3 级反馈移位寄存器.

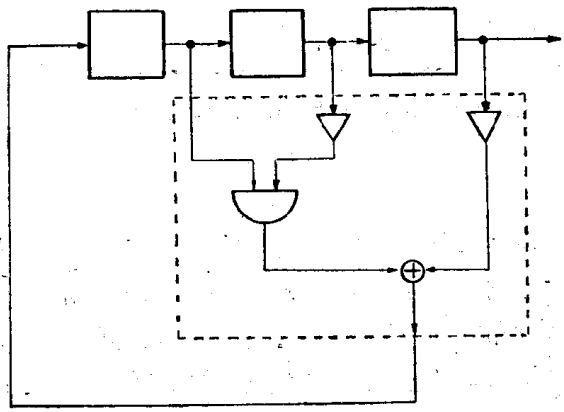
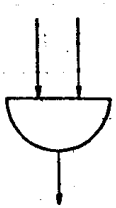


图 1.3

图中框在虚线里的那一部分电路是一个有 3 个输入端，1 个输出端的组合电路；它包含两个“非门”，一个“与门”和一个“模 2 加法器”.符号



代表一个“与门”，它有两个输入端和一个输出端：当两个输入端的输入分别是 x 和 y 时，把它的输出表作 xy，这里 xy 表示 x 和 y 的逻辑积，xy 对于 x 和 y 的依赖关系可用表 1.5 来表示.

表 1.5

x	y	xy
0	0	0
0	1	0
1	0	0
1	1	1

注意，xy 也即是 x 和 y 在 $\mathbf{F}_2$ 中的乘积．符号

代表一个模 2 加法器，它有两个输入端和一个输出端：当两个输入端的输入分别是 x 和 y 时，它的输出就是 $x+y$，这里 $x+y$ 表示 x 和 y 在 $\mathbf{F}_2$ 中的和．模 2 加法器的输出 $x+y$ 对于它的两个输入端的输入 x 和 y 的依赖关系可用表 1.6 来表示．

表 1.6

x	y	$x+y$
0	0	0
0	1	1
1	0	1
1	1	0

表 1.7

x_1	x_2	x_3	$f(x_1, x_2, x_3) = \bar{x}_1 + \bar{x}_2 x_3$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

这个移位寄存器的反馈函数是

$$f(x_1, x_2, x_3) = \bar{x}_1 + \bar{x}_2 x_3,$$

表 1.7 是它的真值表. 这个移位寄存器的状态图见图 1.4. 它的 8 个状态都在一个圈上，这个圈的圈长等于8. 从任一状态出发，这个移位寄存器产生的移位寄存器序列都是周期等于 8 的周期序列，而且它们都平移等价.

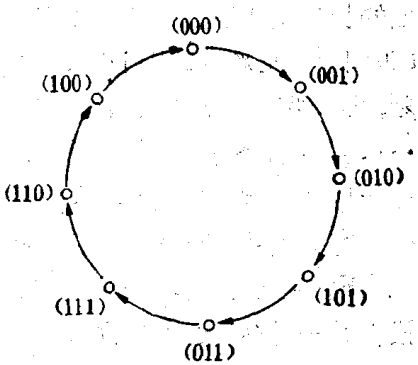


图 1.4

在下一节里将要证明，3 级反馈移位寄存器所能产生的移位寄存器序列的周期一定 $\leqslant 2^3 - 8$，因此本例中的 3 级反馈移位寄存器所产生的移位寄存器序列的周期达到了最大值 8.

§1.2 非线性移位寄存器的一些基本概念

图1.5是一个 n 级反馈移位寄存器(下面总把反馈移位寄存器简称移位寄存器)的框图. 上面一排小方框一共 n 个，代

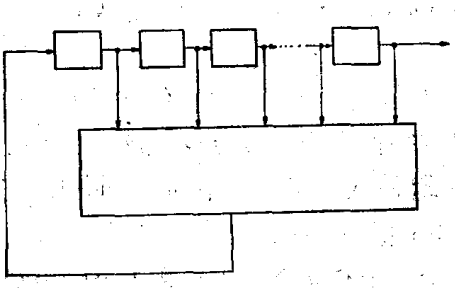


图 1.5

表 n 个寄存器，把它们从左往右依序叫做第 1 级寄存器，第 2 级寄存器，…，第 n 级寄存器．每个寄存器有两种可能的状态，分别用 0 和 1 来代表，而 0 和 1 可以看作是 $\mathbf{F}_2$ 的元素．下面的长方框代表一个有 n 个输入端和一个输出端的组合电路（也叫开关电路，或叫门电路），用 C 来代表它．假定在某一时刻，第 1 级寄存器的状态是 a_n，第 2 级寄存器的状态是 a_{n-1}，…，第 n 级寄存器的状态是 a_1，我们就说这个移位寄存器在这一时刻的状态是 $(a_1, a_2, \cdots, a_n)$．一个 n 级移位寄存器一共有 2^n 个可能的状态，它的状态集是

$$\mathbf{F}_2^n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in \mathbf{F}_2, i = 1, 2, \cdots, n\}.$$

设在某一时刻，这个移位寄存器的状态是 $(a_1, a_2, \cdots, a_n)$，当加上一个移位脉冲后，一方面每个寄存器的状态移给它右面的一级，最右面一级（第 n 级）的状态 a_1 就是输出；另一方面将这 n 个寄存器的状态输送给组合电路 C 的 n 个输入端，并将 C 的输出，设为 a_{n+1}，反馈给最左面一级（即第 1 级）寄存器．因此 C 又叫这个移位寄存器的反馈组合电路．这样，加上一个移位脉冲后，这个移位寄存器就从状态 $(a_1, a_2, \cdots, a_n)$ 转移到状态 $(a_2, a_3, \cdots, a_n, a_{n+1})$，这里 a_{n+1} 由原来的状态 $(a_1, a_2, \cdots, a_n)$ 和组合电路 C 完全确定，而输出是 a_1．从状态 $(a_1, a_2, \cdots, a_n)$ 到状态 $(a_2, \cdots, a_n, a_{n+1})$ 的变换

$$T: (a_1, a_2, \cdots, a_n) \to (a_2, \cdots, a_n, a_{n+1})$$

叫做这个移位寄存器的状态转移变换，它是将这个移位寄存器的状态集 $\mathbf{F}_2^n$ 映入它自身之中的一个映射，它由组合电路 C 所确定．T 也叫做次一状态算子．

在数学上一个有 n 个输入端和 1 个输出端的组合电路 C，可以由一个 n 元开关函数 $f(x_1, x_2, \cdots, x_n)$ 来描述，开关函数也叫布尔函数，它是一个 n 个变元 $x_1, x_2, \cdots, x_n$ 可以

独立地取 0 或 1 这两个可能的值，而函数值 $f(x_1, x_2, \cdots, x_n)$ 也只能是取 0 或 1 为值的函数[1]. 即当图1.5中的组合电路 C 的 n 个输入端从右往左依序是 $x_1, x_2, \cdots, x_n$ 时，它的输出就是 $f(x_1, x_2, \cdots, x_n)$. 描述上述移位寄存器中反馈组合电路的布尔函数又叫这个移位寄存器的反馈函数，有时也叫反馈逻辑. 以 $f(x_1, x_2, \cdots, x_n)$ 为反馈函数的 n 级移位寄存器的状态转移变换往往记作 T_f，而

$$T_f: (a_1, a_2, \cdots, a_n) \to (a_2, \cdots, a_n, f(a_1, a_2, \cdots, a_n)).$$

当 n 较小时，也可以列出这个移位寄存器的状态转移表. 一个 n 级移位寄存器的功能由它的状态转移变换完全确定，而它的状态转移变换又由它的反馈函数完全确定，因此它的功

表1.8 $f_1(x_1, x_2, x_3, x_4)$ 的真值表

x_1	x_2	x_3	x_4	$f_1(x_1, x_2, x_3, x_4)$
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
0	0	1	1	0
0	1	0	0	1
0	1	0	1	0
0	1	1	0	0
0	1	1	1	1
1	0	0	0	1
1	0	0	1	0
1	0	1	0	0
1	0	1	1	1
1	1	0	0	0
1	1	0	1	1
1	1	1	0	1
1	1	1	1	0

表1.9 $f_2(x_1, x_2, x_3, x_4)$ 的真值表

x_1	x_2	x_3	x_4	$f_2(x_1, x_2, x_3, x_4)$
0	0	0	0	1
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	1
0	1	1	1	1
1	0	0	0	1
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	1
1	1	1	1	1

1) 关于开关函数的概念，可参看本书第 §5.1.